Datenschutz nach DSGVO und Informationssicherheitsmanagement nach IT-Grundschutz

Ressourcen optimieren, Kosten reduzieren und Ergebnisse sichern

Nur das integrierte Vorgehen führt zum nachhaltigen gemeinsamen Erfolg.

Informationssicherheit nach IT-Grundschutz und Datenschutz sind wichtige Themenbereiche in Organisationen. Beide Compliance-Themen sind abhängig voneinander und haben Gemeinsamkeiten. Aufgrund der Komplexität der Aufgabenstellung ist eine toolgestützte integrierte Umsetzung sinnvoll. Die Autoren erläutern in diesem Artikel die Vorteile und den Nutzen dieser Herangehensweise.

Von Ellen Wüpper und Werner Wüpper, WMC GmbH

Der BSI IT-Grundschutz ist national anerkannt und eine besonders bei öffentlichen Auftraggebern in Deutschland weit verbreitete Methode für die Planung, Umsetzung und Überprüfung von Informationssicherheit. Im Kern steht die Umsetzung eines Informationssicherheitsmanagementsystems (ISMS) entsprechend den Anforderungen der ISO-27001-Norm auf Basis der Vorgehensweise nach IT-Grundschutz. Der Schwerpunkt liegt hier auf technischen, infrastrukturellen, organisatorischen und personellen Schutzmaßnahmen im Ermessen der jeweiligen Organisation.

Die DSGVO ist die Richtlinie zum Datenschutz in der europäischen Union, welche die Regeln zur Verarbeitung personenbezogener Daten EU-weit vereinheitlichen soll. Die sieben wesentlichen Grundsätze dabei sind: Rechtmäßigkeit (Verarbeitung nach Treu und Glauben, Transparenz), Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit der relevanten Daten und die Rechenschaftspflicht. Der Schwerpunkt hier liegt auf der Umsetzung strenger gesetzlicher Regelungen.

Für beide Compliance-Standards gemeinsam gilt, dass Organisationen die Vertraulichkeit, Integrität und Verfügbarkeit sensibler Daten gewährleisten müssen. Weiter sind die Themenbereiche durch gesetzlich definierte Schutzziele miteinander verknüpft: Der Datenschutz ist elementarer Bestandteil der IT-Sicherheit nach IT-Grundschutz und die Umsetzung des IT-Grundschutz-Standards kann ohne den Schutz personenbezogener Daten nicht gewährleistet werden. Es liegt auf der Hand, dass die Verbindung der beiden Compliance-Standards sinnvoll ist. IT-Grundschutz und Datenschutz führen integriert betrachtet im Ergebnis zu mehr Informationssicherheit bei gleichzeitiger Optimierung von Ressourcen und Kosten.

Der Weg zum Ziel

Um ein nachhaltiges Konzept für ein integriertes Vorgehen zu den komplexen Themen IT-Grundschutz und Datenschutz nach DSGVO zu entwickeln, empfiehlt sich ein der jeweiligen Institution angepasstes, methodisches Vorgehen und die Berücksichtigung

- der jeweiligen Ausgangslage,
- der Gemeinsamkeiten und
- der möglichen Benefits aus der Verbindung der beiden Standards.

Ausgangslage

Bei der Analyse der Ausgangslage ergeben sich für den Datenschutz folgende Punkte aus der DSGVO:

- Grundsätze für die Verarbeitung personenbezogener Daten Art. 5 DSGVO
- Rechtmäßigkeit der Verarbeitung personenbezogener Daten Art. 6 DSGVO
- Bedingungen für die Einwilligung Art. 7 DSGVO
- Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft Art. 8 DSGVO
- Verarbeitung besonderer Kategorien personenbezogener Daten Art. 9 DSGVO

—— Verarbeitung von personenbezogenen Daten über strafrechtliche Verfolgung Art. 10 DSGVO
—— Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist Art. 11 DSGVO
—— Umsetzung der weiteren Artikel

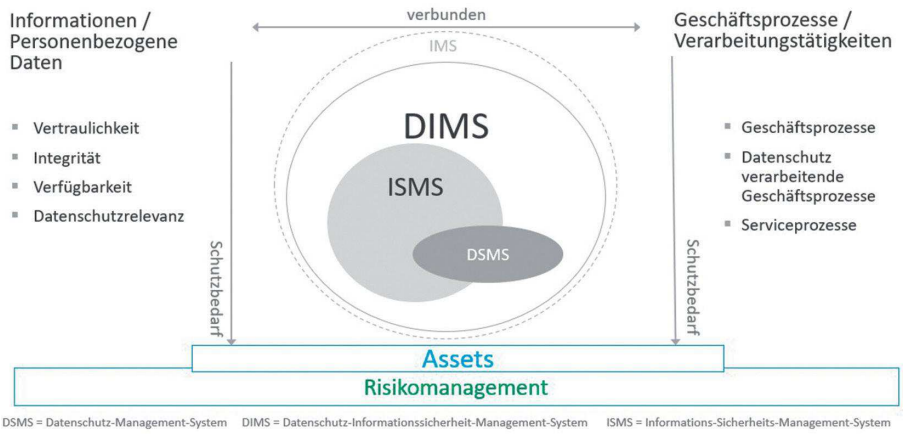
Insgesamt definiert die DSGVO verbindliche gesetzliche Vorgaben. Allerdings geht sie nicht auf Umsetzungsdetails ein beziehungsweise gibt hierzu wenig konkrete Regelungen vor. Anders als bei der IT-Sicherheit nach IT-Grundschutz: Hier gibt es kaum gesetzliche Vorgaben und das Handeln liegt im Ermessen und Interesse der Organisation. Allerdings geht der Standard auf zahlreiche Umsetzungsdetails ein. Bei der Analyse der Ausgangslage für die IT-Sicherheit nach IT-Grundschutz ergeben sich folgende Punkte:

—— Anerkannte Methode und akzeptiertes Vorgehen zur Strukturanalyse, Schutzbedarfsfeststellung, Modellierung, Grundschutz-Check, Analyse von Risiken und Umsetzung erforderlicher Maßnahmen zur Risikobegegnung
—— Unterstützung durch Standards wie ISO 27001 und „Stand der Technik“
—— Abdeckung der Vorsorgeverpflichtungen
—— Reifegradermittlung
—— Möglichkeit der Zertifizierung

Die Basis ist hier ein auf dem Stand der Technik basierender Bausteinkatalog.

Gemeinsamkeiten

Im nächsten Schritt sind die gemeinsamen Ziele und Abhängigkeiten der Standards zu ermitteln: An erster Stelle steht die Umsetzung von Maßnahmen zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit zum Schutz von Daten und Menschen. Weiter geht es



Das Datenschutz-Informationssicherheits-Management-System

in beiden Standards um die Risikoreduzierung auch im Hinblick auf Haftungsreduzierungen. Zudem stehen sie in Abhängigkeit zueinander: IT-Sicherheit ohne Datenschutz ist nicht zielführend. Letztlich haben beide Compliance-Standards ähnliche Vorgehensweisen und Mechanismen.

Trotz vieler Gemeinsamkeiten muss man jedoch auch die individuellen Belange beider Standards vollumfänglich berücksichtigen.

Benefits durch Toolunterstützung

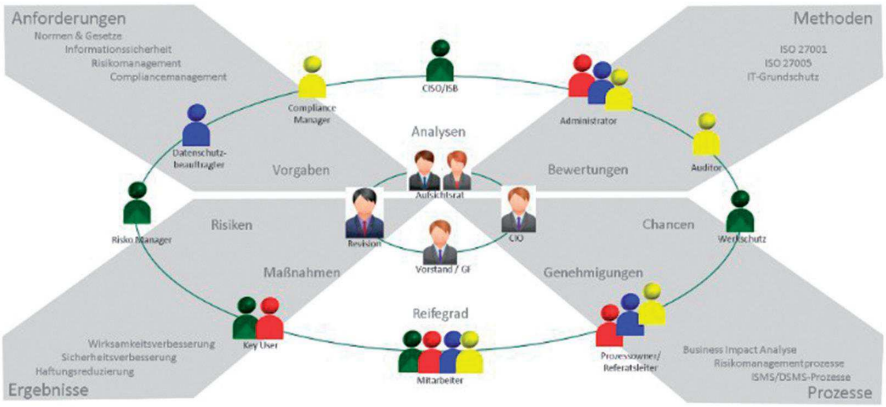
Zum Erreichen von Synergien bei IT-Grundschutz und Datenschutz wird ausdrücklich ein toolgestütztes Vorgehen empfohlen, da sich die Nachhaltigkeit deutlich mit der Nutzung eines integrierten Managementsystems auf Datenbankbasis erhöht. Moderne Systeme bieten die Möglichkeit des Vorgehens nach dem IT-Grundschutz und den Anforderungen der ISO 27001 ebenso wie die integrierte Abbildung aller Datenschutzanforderungen. Mit Bordmitteln, wie beispielsweise Excel, können diese komplexen Prozesse längst nicht mehr zielführend und nachhaltig dargestellt werden.

Wenn beide Themengebiete auf die gleiche vorhandene Datenbasis zugreifen können, muss der Prozess vom Prozessverantwortlichen nur einmal erfasst werden. Die Prozesse sind somit die Basis für die Verarbeitungstätigkeit im Datenschutz und für die Kritikalitätsbewertung in der Informationssicherheit. In der Praxis wird oftmals das Verzeichnis der Verarbeitungstätigkeiten vom Datenschutzbeauftragten (DSB) unabhängig von der Prozessdarstellung des Informationssicherheitsbeauftragten (ISB) erstellt. Das erzeugt Redundanzen und erhöht die Fehlerquote.

Beteiligte Rollen entlasten

In der Praxis sind idealerweise unterschiedliche Rollen an den Aufgaben zur Umsetzung von Informationssicherheit und Datenschutz sowie den zugehörigen Erfassungs-, Bewertungs- und Reportingaufgaben beteiligt.

Durch die Integration von Datenschutz und IT-Grundschutz in einem System können die beteiligten Ressourcen in die jeweiligen Aufgaben einbezogen und optimiert werden. Andernfalls werden die Ressourcen durch ein getrenntes Vorgehen doppelt belastet und Daten doppelt erfasst. Eine Belastung über Gebühr führt häufig zu sinkender Akzeptanz bei den Fachverantwortlichen und erhöhten Fehlerquoten. Nur wenn eine prozessorientierte Vorgehensweise in der Organisation etabliert wird und auch für die verantwortlichen Anwender ein erkenn-



Rollen und Verantwortlichkeiten

barer Mehrwert entsteht, werden Erhebungen und Bewertungen gern durchgeführt, und die Akzeptanz für den Prozess steigt. Umso wichtiger wird eine Softwareunterstützung für die regelmäßige Erfassung und Bewertung der komplexen Anforderungen. Ohne eine datenbankorientierte Unterstützung können diese nicht qualitativ hochwertig umgesetzt werden, da die Bewertungskriterien der Disziplinen sich überschneiden, aber dennoch die jeweiligen für das Fachgebiet erforderlichen zusätzlichen Themenerweiterungen benötigt werden. Diese Verbindung zwischen den Themenbereichen und die gleichzeitige Erweiterung um bereichsindividuelle Features ermöglicht komfortabel nur ein integriertes Tool. Dennoch sind grundsätzlich auch Schnittstellen zwischen bestehenden Tools denkbar, um zumindest die Doppelerfassung von Daten zu unterbinden.

Es ist besonders anzumerken, dass auch Revisoren, Auditoren, Qualitätsverantwortliche, IKS-Verantwortliche et cetera mit in die Anwendung einbezogen werden sollten. Damit wird eine noch höhere Akzeptanz unter allen Anwendern erzeugt.

Festgelegtes, einheitliches methodisches Vorgehen

Die Umsetzung der Anforderungen der Informationssicherheit nach IT-Grundschutz und des Datenschutzes nach der EU-DSGVO erfolgt in der Praxis häufig nur durch den ISB und den DSB. Bei Nutzung einer Toolunterstützung werden im Gegensatz zu diesem Vorgehen alle Prozessbeteiligten in den Prozess einbezogen und mit einer einheitlich festgelegten Bewertungsmethode unterstützt. Anpassungen werden nur nach einem festgelegten Veränderungsprozess vorgenommen. Damit werden vergleichbare Ergebnisse und Reports über alle Organisationseinheiten erzielt.

Schnellere Einführung und Betrieb

Die Anforderungen an ein Datenschutz- und Informationssicherheitsmanagementsystem sind komplex und bewertungsintensiv. Über die in einem Tool verfügbaren und festgelegten Methoden und den mitgelieferten Content wird eine schnelle Einführung gewährleistet. Durch die Abbildung der Aufbau- und der Ablauforganisation mit allen erforderlichen Daten- und Bewertungsanforderungen kennt jeder Prozessbeteiligte seine Aufgaben und wird permanent an offene Aufgabenstellungen erinnert. Damit ist eine wesentliche Zeitersparnis verbunden.

Bessere Unterstützung der Fachverantwortlichen

Die regelmäßige Neu- und Veränderungserfassung beziehungsweise Neubewertung der für den Prozess erforderlichen Daten (Prozesse, Informationen und Assets etc.) kann mit Toolunterstützung benutzerfreundlich über die Verwendung von Workflows umgesetzt werden. Dieser Vorteil führt zu einer deutlichen Steigerung der Nutzerakzeptanz. Ferner ist ein Fachverantwortlicher oftmals nur einmal jährlich mit der Bewertung seiner Prozesse beauftragt. Vorteil einer intuitiven Führung für die jeweilige Aufgabenstellung im gesamten Workflowprozess ist hier die sich dadurch reduzierende Schulungsaufwendung.

Haftungs- und Risikoreduzierung

Die Umsetzung der Anforderungen der Informationssicherheit nach IT-Grundschutz und des Datenschutzes nach der EU-DSGVO dient nicht nur zur Haftungsreduzierung, sondern auch im Wesentlichen zur Reduzierung der operationellen Risiken. Durch die toolgestützte methodische Risikobewertung der den Prozess unterstützenden Assets werden die Risiken erkannt und durch Maßnahmen reduziert. Gleichzeitig stehen alle Datenschutz- und Informationssicherheitsvorfälle bei der Bewertung zur Verfügung.

Fazit

Datenschutz und Informationssicherheit nach IT-Grundschutz leisten einen wichtigen Beitrag zur Compliance und Risikoreduzierung in einer Organisation. Mit einem methodischen und integrierten Vorgehen werden die Aktivitäten vergleichbar, revisionssicher dokumentiert und nachhaltig entwickelbar. Da beide Themenbereiche komplex sind, Gemeinsamkeiten haben und sich gegenseitig unterstützen können, ist eine toolgestützte gemeinsame Datenbasis ohne Redundanzen nicht nur „nice to have“, sondern bringt Unterstützung, Erleichterung, Prozess-, Ressourcen- und Kostenoptimierung.