© BSI - AdobeStock.com

So setzten Sie Informationssicherheit um

PRIVACYXPERTS

Inhaltsverzeichnis

Das sind die wesentlichen Prozessschritte 1

Nutzen Sie diese Standards als Basis Ihrer Maßnahmen 2

Das beinhaltet eine Schutzbedarfsfeststellung 8

Holen Sie alle Beteiligten ins Boot 14

Das sind die wesentlichen Prozessschritte

Informationssicherheit beschreibt Prozesse und Verfahren, die zur Wahrung der Schutzziele Ihres Unternehmens vorhanden sein müssen. Hierzu zählen die folgenden wesentlichen Prozessschritte:

ÜBERSICHT: Prozessschritte Informationssicherheit	
Prozess	**Maßnahme**
Strukturanalyse	Erhebung aller relevanten IT-Systeme
Schutzbedarfs-feststellung	Einstufung der eingesetzten Anwendungen, IT-Systeme, Infrastruktur (Räume, Netzwerk) hinsichtlich ihres Schutzbedarfs
Soll-Ist-Vergleich	Überprüfung der aktuellen Sicherheitsmaßnahmen durch ein Audit (Ist) und Abgleich der Ergebnisse mit den Unternehmenszielen (Soll)
Risikoanalyse	Identifikation und Bewertung der erhobenen Risiken
Risikobehandlung/ Maßnahmenplan	Erstellung eines Maßnahmenplanes zur Risikominimierung oder Risikobeseitigung
Dokumentation	Dokumentation aller Prozessschritte und Ergebnisse in einer aussagekräftigen Form

Diese Prozesse stehen in der Regel im Verantwortungsbereich des IT-Sicherheitsoder Informationssicherheitsbeauftragten (ISB) des Unternehmens. Als Datenschutzbeauftragter sollten Sie mit diesem eng zusammenarbeiten, weil Sie die Ergebnisse aus dessen Schutzbedarfsfeststellung und Risikoanalyse für die Erfüllung Ihre Aufgaben als Datenschutzbeauftragter benötigen.

Sollte es in Ihrem Unternehmen keinen ISB geben, müssen Sie sich mit Ihrer Geschäftsleitung in Verbindung setzen und darauf hinwirken, dass eine solche Funktion eingerichtet wird.

Nutzen Sie diese Standards als Basis Ihrer Maßnahmen

1. ISO 27001:2013 – So hilft Ihnen der Standard bei Ihrer Arbeit

Die ISO 27001:2013 ist der internationale Standard zum Informationssicherheits-Management. Sie beschreibt Prozesse und Maßnahmen zur Gewährleistung der Informationssicherheit und zur Etablierung eines Informationssicherheits-Managementsystems (ISMS). Als Datenschutzbeauftragter können Sie von diesem Standard in vielerlei Hinsicht profitieren. Gibt er Ihnen doch die Möglichkeit, Ihre Anforderungen an die Datensicherheit mit einem internationalen Standard zu begründen.

2. ISO 27001:2013 – Das sind die Schwerpunkte

Insbesondere im Hinblick auf die Anforderungen aus der Datenschutz-Grundverordnung (DS-GVO) und der darin geforderten Datenschutzfolgenabschätzung (DSFA) müssen Sie prüfen, ob die technischen und organisatorischen Maßnahmen geeignet sind, die personenbezogenen Daten zu schützen. Hier sollten Sie sich an geeigneten internationalen Sicherheitsstandards wie der ISO 27001:2013 orientieren.

Geeignete Maßnahmen sind in den Kapiteln 4 bis 8 der ISO 27001:2013 zu den nachfolgenden Themen beschrieben:

- Aufbau und Umsetzung eines ISMS und eines Risikomanagements
- Verantwortung des Managements (IT-Sicherheitsleitlinie, Ressourcen usw.)
- Durchführung regelmäßiger Audits zur Überwachung der Wirksamkeit des ISMS
- Aufbau von Messgrößen und Kennzahlen zur Messbarkeit des Sicherheitsniveaus
- Korrektur und Verbesserungsmaßnahmen

In Anhang A finden Sie als Datenschutzbeauftragter normative Maßnahmenziele und Maßnahmen zu den folgenden Themenbereichen:
- Sicherheitsleitlinie (Inhalte und Aufbau)
- Organisation der Informationssicherheit (IT-Sicherheitsbeauftragter usw.)
- Management der Werte im Unternehmen (Strukturanalyse, Schutzbedarf)
- Personelle Sicherheit
- Physische Sicherheit
- Betriebsund Kommunikationsmanagement
- Zugangskontrolle
- Beschaffung, Entwicklung und Wartung von IT-Systemen
- Umgang mit Sicherheitsvorfällen
- Sicherstellung des Geschäftsbetriebs (Business Continuity Management)
- Einhaltung von Vorgaben (Compliance)

Wichtig für den Datenschutzbeauftragten: Als Datenschutzbeauftragter können Sie Ihrer Verantwortung am besten nachkommen, wenn Sie Ihre Daten sicherheitsmaßnahmen mit der Einhaltung gängiger Sicherheitsstandards begründen. Zunächst verweist Art. 32 DSGVO dabei auf eine „Berücksichtigung des Stands der Technik", um geeignete Schutzmaßnahmen zu gewährleisten. Wobei sich der „Stand der Technik" auch aus den Anforderungen der ISO 2700:2013 ableitet. Auch das Bundesamt für Sicherheit in der Informations technik (BSI) bezieht sich auf die ISO 27001:2013.

3. ISO 27002 – Hier finden Sie konkrete Maßnahmenempfehlungen

Die ISO 27002 kann als Ausgangspunkt für die Entwicklung organisationsspezifischer Leitlinien angesehen werden. Möglicherweise sind nicht alle der in diesem Leitfaden angegeben Sicherheitsmaßnahmen und Orientierungshilfen für Ihr Unternehmen anwendbar.

Für die Prüfung von Sicherheitsmaßnahmen insbesondere im Rahmen von Auftragsverarbeitungen, können diese Maßnahmen für Sie jedoch sehr hilfreich sein, folgen diese doch konsequent einem Best Practice-Ansatz.

Sie finden in der ISO 27002 unter anderem konkrete Maßnahmenempfehlungen zu den folgenden Themen:
- Sicherheitsleitlinien
- Organisation der Informationssicherheit

- Informationsklassifizierung
- Zugriffskontrolle
- Kryptografie
- Zutrittsschutz
- Betriebssicherheit (Malwareschutz, Backup, Protokollierung, Schwachstellenmanagement usw.)
- Sicherheit in der Kommunikation (Netzwerksicherheit usw.)

Wichtig für den Datenschutzbeauftragten: Als Datenschutzbeauftragte/r können Sie die ISO 27001 verwenden, um die Funktionsfähigkeit eines Sicher heitsmanagements zu prüfen. Ein solches Sicherheits management ist die Basis dafür, dass die konkreten Maßnahmen aus der ISO 27002 überhaupt wirksam umgesetzt werden können. Die beiden Standards er gänzen sich also und sind für Sie als Datenschutzbe auftragten wertvolle Arbeitshilfen und Nachschlage werke, die Sie nutzen sollten.

Zertifizierung nach ISO 27001 möglich
Derzeit basieren die meisten Rahmenwerke zur IT-Sicherheit auf dieser Norm. Es ist auch möglich, sich als Unternehmen nach der ISO 27001 zertifizieren zu lassen. Als Datenschutzbeauftragte/r müssen Sie wissen, dass ein solches Zertifikat im Wesentlichen den Reifegrad des Informationssicherheits-Managements und der Sicherheitsmechanismen und nicht den Stand der Datensicherheit beschreibt.

Die ISO 27001 beschreibt demnach Prozesse und Anforderungen – aber nicht, wie man diese Anforderungen tatsächlich zur Wahrung der IT-Sicherheit umsetzen muss. Sie werden in der ISO z. B. keine Beschreibung dazu finden, wie Sie einen Server sicher betreiben können.

4. BSI IT-Grundschutz – So profitieren Sie von den Neuerungen

Das BSI beschreibt in seinen IT-Grundschutzkatalogen konkrete Sicherheitsmaßnahmen zur Umsetzung der Anforderungen aus der ISO 27001. Unternehmen können sich auf der Basis des IT-Grundschutzes nach der ISO 27001 zertifizieren lassen. Das BSI zertifiziert auch entsprechende Auditoren.

Im Gegensatz zur ISO finden Sie in den IT-Grundschutzkatalogen konkrete Handlungsempfehlungen zur Umsetzung der Sicherheitsanforderungen. Allerdings müssen Sie beachten, dass diese Handlungsempfehlungen IT-Kenntnisse erfordern und oftmals so umfangreich und detailliert sind, dass Sie als Datenschutzbeauftragte/r ohne tiefere ITKenntnisse kaum einen Mehrwert aus dieser Vielzahl von Informationen ziehen können.

Das BSI hat alle Standards und die Bestandteile des IT-Grundschutzes im Jahr 2017 aktualisiert. Ziel war es, grundlegende Sicherheitsmaßnahmen schneller umsetzen zu können. Eines der neuen Kerndokumente ist der BSI Standard 200-2 IT-Grundschutz Methodik, der den bisherigen BSI Standard 100-2 ablöst. In dem neuen Standard wird konsequent zwischen Sicherheitsanforderungen und Umsetzungshinweisen mit konkreten Tipps zum Erreichen des jeweiligen Sicherheitsniveaus unterschieden. Aus dem IT-GrundschutzKatalog wurde das IT-Grundschutz-Kompendium. Damit kann eine schnelle Basisabsicherung als Grundlage für ein wirksames Informationssicherheits-Managementsystem (ISMS) erreicht werden.

BSI Grundschutz – Das ist die neue Struktur

Das neue IT-Grundschutz-Kompendium besteht aus der übergeordneten Schicht ISMS und den Sicherheitsüberprüfungen sowie der Schicht „Detektion und Reaktion“ (DER), die das Erkennen und Behandeln von Sicherheitsvorfällen enthält. Dazwischen liegen die Prozessbausteine „Organisation und Personal“ (ORP), „Konzepte und Vorgehensweisen“ (CON) sowie „Betrieb“ (OPS). Darauf folgen die Systembausteine „Anwendungen“ (APP), „IT-Systeme“ (SYS), „Netze“ (NET), „Infrastruktur“ (INF) und „Industrielle-IT“ (IND) mit zum Teil sehr konkreten Maßnahmenempfehlungen.

Das versteht das BSI unter Basisund Kernabsicherung

In den einzelnen Kapiteln des neuen IT-GrundschutzKompendiums wird nun der Weg zu einem vollständigen ISMS beschrieben. Hierbei können unterschiedliche Wege beschritten werden. Erste Ziele können das Erreichen einer Basisabsicherung bzw. einer Kernabsicherung sein. Wobei die Kernabsicherung im Wesentlichen die bewährte Vorgehensweise des bisherigen BSI Standards 100-2 ohne die „ergänzende Sicherheitsanalyse“ umfasst.

Mit der Basisabsicherung kann schnell ein Mindestsicherheitsniveau im Unternehmen erreicht werden. Vor dem Hintergrund, dass die Umsetzung

eines vollständigen ISMS die kurzfristige Umsetzung konkreter Sicherheitsmaßnahmen zunächst verzögert, wird bei dieser Basisabsicherung auf umfangreiche Dokumentationen und Analysen verzichtet. Hier werden zentrale Sicherheitsanforderungen wie das Patchmanagement, Passwortrichtlinien usw. behandelt. Die Kernabsicherung umfasst die Absicherung der Kronjuwelen eines Unternehmens, bei deren Verletzung der Sicherheitsziele Vertraulichkeit, Verfügbarkeit und Integrität existenzbedrohende Schäden auftreten würden. Auch bei der Kernabsicherung wird das Ziel verfolgt, eine möglichst schnelle Umsetzung der Sicherheitsmaßnahmen zu ermöglichen. Sind die Maßnahmen für eine Basisund Kernabsicherung vollständig umgesetzt, ist ein sachgerechtes ISMS im Unternehmen etabliert.

MEIN TIPP: Setzen Sie sich mit Ihrer IT-Abteilung in Verbindung und überzeugen Sie die Kollegen zunächst, mit der Basisabsicherung zu beginnen. Die dort beschriebenen Maßnahmen sind leicht verständlich und schnell umsetzbar. So erreichen Sie mit überschaubarem Aufwand ein gutes Sicherheitsniveau.

Zu den Bestandteilen der Basisabsicherung zählen:
- Initialisierung eines Informationssicherheitsprozesses
- Definition einer Sicherheitsleitlinie und Sicherheitsorganisation
- Eine Übersicht der IT-Systeme und Anwendungen (Strukturanalyse)

Die Kernabsicherung umfasst im Wesentlichen Maßnahmen zur Ermittlung und Absicherung der Kronjuwelen in Ihrem Unternehmen. Wobei die Kernabsicherung zwar vom Geltungsbereich auf die kritischsten Systeme beschränkt ist, aber vom Umfang der Maßnahmen gesehen aufwändiger ist.

Wichtig für den Datenschutzbeauftragten: Das BSI hat mit dem neuen IT-Grundschutz-Kompendium ein modulares Vorgehensmodell zur Etablierung eines ISMS geschaffen, das die Verantwortlichen in Ihrem Unternehmen in die Lage versetzt, das Sicherheitsniveau effektiv zu verbessern – wobei gerade die Bausteine in den Schichten (APP, SYS, INF usw.) für Sie als Datenschutzbeauftragte/n interessant sind. Diese Bausteine enthalten auf wenigen Seiten sehr konkrete und direkt umsetzbare Maßnahmen.

5. COBIT

COBIT (Control Objectives for Information and Related Technology) ist das international anerkannte Framework zur ITGovernance und gliedert die Aufgaben der IT in Prozesse und Kontrollziele. COBIT definiert hierbei nicht vorrangig, wie die Anforderungen umzusetzen sind, sondern primär, was genau umzusetzen ist. Cobit bestimmt den Reifegrad des Managementprozesses. Mit Cobit können z. B. die folgenden Fragestellungen beantwortet werden:
Werden IT-Services entsprechend den Prioritäten des Unternehmens erbracht?

- Können Anwender die IT-Systeme produktiv und sicher nutzen?
- Ist eine angemessene Vertraulichkeit, Integrität und Verfügbarkeit gegeben?
- Für jede dieser Fragen gibt es wiederum eine Vielzahl von Kontrollfragen, die aber immer auf den jeweiligen Prozess abstellen.

Für Sie als Datenschutzbeauftragte/n kann Cobit in erster Linie eine Übersicht der relevanten IT-Prozesse und der entsprechenden Kontrollfragen für Audits liefern.

6. ITIL

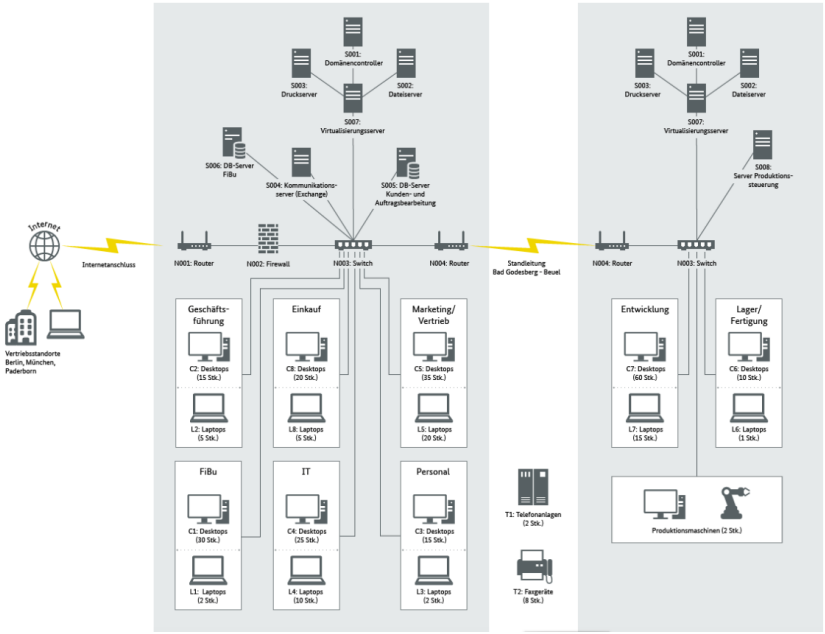
Die IT Infrastructure Library (ITIL) ist eine Sammlung von Best Practices in einer Reihe von Publikationen zur Umsetzung eines IT-Service-Managements (ITSM). In dem Regelund Definitionswerk werden die für den Betrieb einer IT-Infrastruktur notwendigen Prozesse, die Aufbauorganisation und die Werkzeuge beschrieben. Die ITIL orientiert sich an dem durch den IT-Betrieb zu erbringenden wirtschaftlichen Mehrwert für den Kunden. Dabei werden die Planung, Erbringung, Unterstützung und Effizienz-Optimierung von ITServiceleistungen im Hinblick auf ihren Nutzen als relevante Faktoren zur Erreichung der Geschäftsziele eines Unternehmens betrachtet. Als Datenschutzbeauftragte/r können Sie von ITIL in erster Linie dann profitieren, wenn die IT in Ihrem Unternehmen die Prozesse nach ITIL ausgerichtet hat. Dann haben Sie eine Chance, strukturierte und dokumentierte Verfahren vorzufinden und diese auch prüfen zu können. Insbesondere das Incidentund Problem-Management (Behandlung von Störungen und Fehlern) und das Changemanagement (Behandlung von Änderungen) sind auch für die Datensicherheit von wesentlicher Bedeutung.

Das beinhaltet eine Schutzbedarfsfeststellung

1. Strukturanalyse

Die Strukturanalyse gibt Ihnen als Datenschutzbeauftragtem einen Überblick über die in Ihrem Unternehmen eingesetzten IT-Systeme, Netzwerkund Kommunikationsverbindungen. Die Strukturanalyse ergänzt damit Ihr Verzeichnis um diese wesentlichen Aspekte. Ein Teil der Strukturanalyse ist der „gruppierte Netzplan". Dieser Netzplan soll es Ihnen ermöglichen, einen Überblick über die Netzwerkstruktur zu erhalten. Hierbei steht nicht die Technik, sondern die logische Struktur des Netzwerkes im Vordergrund.

Einen solchen Netzplan sollten Sie sich von Ihrer IT-Abteilung erstellen lassen. Legen Sie hierbei den Schwerpunkt auf solche IT-Systeme, die nach Ihrem Verzeichnis personenbezogene Daten verarbeiten.



Beispiel: „Gruppierter Netzplan"

MEIN TIPP: Legen Sie Ihrer IT-Abteilung eine Liste der Anwendungen, die personenbezogene Daten enthalten, vor und lassen Sie sich für diese Anwendungen die entsprechenden IT-Systeme, Räume und Kommunikationsverbindungen eintragen. Für diese Informationen (Räume, IT-Systeme, Anwendungen) soll Ihnen die IT-Abteilung einen „gruppierten Netzplan" erstellen.

Beispiel: Erfassungsbogen für die Strukturanalyse

IT-Anwendungen

Kürzel	IT-Anwendung	Beschreibung	Datenhaltung (Kürzel IT-System)	IT-Systeme (Kürzel)	Netzwerksysteme (Kürzel)	Verantwortlich	Dienstleister	personenbezogene Daten	Integrität	Vertraulichkeit	Verfügbarkeit
A01	Lohn und Gehalt	Anwendung für Personalwesen	Kürzel IT-System	S01	Kürzel Netzwerksystem	Leiter Personal	Interne IT-Abteilung	x	sh	h	h

ITund Netzwerksysteme (Sxx)

Kürzel	Name	Beschreibung	Anzahl	Plattform	Raum/Ort (Kürzel)	Verantwortlich	Externe Verbindung (Kürzel)	Dienstleister	Integrität	Vertraulichkeit	Verfügbarkeit
S01	SAP	DatenbankServer	1	Windows 2008	R01	Leiter Personal	KE01	D01	sh	h	h

Netzwerkverbindungen (Nxx)

Kürzel	Verbindung	Beschreibung	Externe Verbindung	Integrität	Vertraulichkeit	Verfügbarkeit
N01	Anbindung Dienstleister	Standleitung	x	sh	h	h

Räume (Rxx)

Kürzel	Bezeichnung	Beschreibung	Ort	Verantwortlich	Hochwasserschutz	USV/ NSV	Klimaanlage	Brandschutz	Videoüberwachung	Zutrittsregelungen	Zugangskontrolle	Integrität	Vertraulichkeit	Verfügbarkeit
R01	Serverraum	Zentraler Serverraum Hauptgebäude	Zentrale	IT-Abteilung	ja	ja	ja	ja	ja	ja	ja	sh	h	h

Dienstleister (Dxx)

Kürzel	Beschreibung	Vertragsnummer	Vertragsdatum	Laufzeit	Verantwortlich
D01	Servicevertrag mit dem IT-Dienstleister	14663	01.01.2012	unbegrenzt	IT-Abteilung

Mit diesen Erfassungsbögen haben Sie als Datenschutzbeauftragte/r einen sehr guten Überblick über alle relevanten IT-Systeme. Diese Strukturanalyse ist auch die Basis für Ihr Verzeichnis.

Die Verbindungen zwischen den einzelnen Systemen werden über die jeweiligen Kürzel hergestellt.

Wichtig für die Geschäftsleitung: Mit dem Netzplan und diesen Übersichten haben Sie eine vollständige Übersicht über Ihre IT-Infrastruktur, bis hin zu den Verträgen mit Ihren Dienstleistern. So können Sie nicht nur die IT-Risiken, sondern auch Ihre Investitionen besser im Auge behalten. Insbesondere für die Kosten-Nutzen-Analyse von IT-Sicherheitsmaßnahmen kann das für Sie sehr hilfreich sein.

2. Schutzbedarfsfeststellung für Ihre IT-Infrastruktur: So gehen Sie konkret vor

In der Strukturanalyse wurde die IT-Infrastruktur erhoben. In der Schutzbedarfsfeststellung wird nun der Schutzbedarf für diese IT-Infrastruktur ermittelt. Dabei wird zunächst der Schutzbedarf für die Anwendungen berechnet. Für alle weiteren Elemente (IT-Systeme, Netzwerke, Räume usw.) gilt das Vererbungsprinzip.

Hier wird der Schutzbedarf der Anwendung auf das IT-System, der Schutzbedarf des IT-Systems auf die genutzte Netzwerkverbindung und den Raum (Serverraum, Büro usw.) sowie den eventuell involvierten IT-Dienstleister übertragen. Gehen Sie nach dem Maximalprinzip vor.

Nutzen z. B. mehrere Anwendungen den gleichen Server, wird nach diesem Maximalprinzip der Schutzbedarf der Anwendung mit den höchsten Werten an den entsprechenden Server „vererbt“.

Schutzbedarfskategorien

Um den Schutzbedarf ermitteln zu können, müssen Sie zunächst die Schutzbedarfskategorien für Ihre Erhebung definieren. In der Praxis haben sich die folgenden Kategorien bewährt:

Normal	n	Die Schadensauswirkungen sind begrenzt und überschaubar.
Hoch	h	Die Schadensauswirkungen können beträchtlich sein.
Sehr hoch	sh	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Beispiel: Schutzbedarfskategorien	
Beeinträchtigung der Aufgabenerfüllung	
Normal Hoch Sehr hoch	Die Beeinträchtigung würde von den Betroffenen als tolerabel/nicht tolerabel/ existenzbedrohend eingeschätzt werden. Die tolerierbare Ausfallzeit beträgt z. B. maximal 12/1 bis 12 Stunden/weniger als 1 Stunde.
Verstoß gegen Gesetze/Vorschriften/Verträge	
Normal Hoch Sehr hoch	Verstöße gegen Vorschriften und Gesetze haben geringfügige/erhebliche/ geschäftsschädigende Konsequenzen. Vertragsverletzungen haben geringe/hohe/ existenzbedrohende Konventionalstrafen zur Folge.
Beeinträchtigung der Aufgabenerfüllung	
Normal Hoch Sehr hoch	Eine Beeinträchtigung der persönlichen Unversehrtheit kann wahrscheinlich/nicht absolut/nicht ausgeschlossen werden.
Negative Außenwirkung	
Normal Hoch Sehr hoch	Es ist eine geringe bzw. nur interne/breite/überregionale Ansehens- oder Vertrauensbeeinträchtigung zu erwarten.
Finanzielle Auswirkungen	
Normal Hoch Sehr hoch	Es entstehen dem Unternehmen finanzielle Schäden in Höhe von weniger als 1 % /1 % bis 10 %/mehr als 10 % eines durchschnittlichen monatlichen Umsatzes.

Schadenszenarien

Die Schutzbedarfskategorien müssen hinsichtlich des Verlustes von Vertraulichkeit, Verfügbarkeit und Integrität konkretisiert werden. Die Schäden sollten Sie in folgende Schadenszenarien einteilen:

Beeinträchtigung der Aufgabenerfüllung
- Verstoß gegen Gesetze/Vorschriften/Verträge
- Beeinträchtigung der persönlichen Unversehrtheit
- Negative Außenwirkung
- Finanzielle Auswirkungen

Wichtig für die Geschäftsleitung: Wenn Sie diese Kategorien mit Eurobeträgen unterlegen können, ist das für die Bewertung der Schadenshöhen sehr hilfreich. Ihr Risikocontrolling müsste Ihnen wertvolle Hinweise geben können.

So führen Sie die Interviews durch
Nachdem Sie die Schutzbedarfskategorien festgelegt haben, müssen Sie mit den für die Anwendung Verantwortlichen die eigentliche Schutzbedarfsfeststellung durchführen. In der Praxis haben sich hierfür Interviews bewährt. Am besten führen Sie diese Interviews mit Formularen durch. Sie finden unter dem Link auf der letzten Seite entsprechende Formulare, mit denen Sie direkt loslegen können.

Wichtig für die Geschäftsleitung: Die Schutzbedarfsfeststellung ist die Basis für alle weiteren Schritte im IT-Risikomanagement. Nur so können Sie Transparenz in Ihre IT-Risiken schaffen und die Kosten für IT-Sicherheitsmaßnahmen sinnvoll steuern. Denn wenn Sie sich auch in der IT-Sicherheit auf die wesentlichen Risiken mit einem hohen Schutzbedarf beschränken, können Sie auch Ihre Kosten senken.

Mit der Schutzbedarfsfeststellung können Sie erkennen, welche Anwendungen und Systeme Ihre erhöhte Aufmerksamkeit als Datenschutzbeauftragte/r erhalten müssen. Sie sollten Ihre weiteren Maßnahmen auf die Systeme mit einem erhöhten Schutzbedarf ausrichten.

MEIN TIPP: Übertragen Sie den Schutzbedarf in eine Tabelle und werten Sie die Ergebnisse aus. Diese Liste sollten Sie Ihrer Geschäftsleitung vorlegen. So können Sie transparent zeigen, welche schützenswerten Daten und IT-Systeme in Ihrem Unternehmen vorhanden sind.

Muster: Tabelle Schutzbedarfsübersicht Häufigkeit (Schutzbedarf Anwendungen)			
Schutzbedarf	**Integrität**	**Vertraulichkeit**	**Verfügbarkeit**
Hoch	10	20	50
Sehr hoch	5	10	20
Normal	2	3	8

Dargestellt wird die Anzahl der Anwendungen, die in die jeweiligen Schutzbedarfskategorien eingeordnet wurden. In diesem Beispiel sind im Unternehmen 35 Anwendungen mit einem „sehr hohen" Schutzbedarf vorhanden, wovon 20 einen sehr hohen Schutzbedarf an die Verfügbarkeit, 10 an die Vertraulichkeit und 5 an die Integrität haben.

Schutzbedarfsliste			
Anwendung	**Integrität**	**Vertraulichkeit**	**Verfügbarkeit**
(A01) SA	Sehr hoch	Hoch	Hoch
(A02) Videoüberwachung	Hoch	Sehr hoch	Hoch
(A03) Zeiterfassung	Hoch	Hoch	Sehr hoch

Mit einer solchen Übersicht können Sie die Geschäftsleitung davon überzeugen, dass Ihre Maßnahmen für die Anwendungen mit erhöhtem Schutzbedarf angemessen und erforderlich sind.

Weitere Prozessschritte wie der Soll-Ist-Vergleich, die Risikoanalyse, die Risikobehandlung und die Maßnahmenplanung werden im Informationssicherheitsmanagement (ISM) des Unternehmens durchgeführt. Als Datenschutzbeauftragter sollten Sie sich die Risikoanalysen und insbesondere die Maßnahmen aushändigen lassen und mit den Ergebnissen Ihrer Datenschutzfolgenabschätzungen abgleichen. Abweichungen der Risikoanalysen oder der identifizierten Maßnahmen sollten Sie mit dem ISB abstimmen.

Holen Sie alle Beteiligten ins Boot

Sämtliche Maßnahmen – von der Strukturanalyse über die Schutzbedarfsfeststellung bis hin zum Maßnahmenplan – können Sie als Datenschutzbeauftragte/r nicht allein durchführen. Sie sind auf die Unterstützung verschiedenster Bereiche in Ihrem Unternehmen angewiesen. Sie benötigen Informationen vonseiten des Risikocontrollings, der IT-Abteilung und allen Fachbereichen, die mit IT-Systemen arbeiten. Sie müssen also als Datenschutzbeauftragte/r alle Beteiligten „ins Boot holen" und davon überzeugen, dass Ihr Projekt einem gemeinsamen Ziel dient. Das geht am einfachsten, wenn bei diesem Projekt für alle etwas „herausspringt", also eine Win-win-Situation entsteht. Den wesentlichsten Nutzen für die Beteiligten aus diesem Projekt können Sie der Liste auf der nachfolgenden Seite entnehmen.

Mit dieser Aufstellung zur Datensicherheit können Sie als Datenschutzbeauftragte/r in die Diskussion mit den beteiligten Bereichen gehen.

Stellen Sie die Vorteile für die jeweiligen Bereiche heraus und überzeugen Sie durch Argumente.

MEIN TIPP: Gehen Sie offensiv in die Diskussion. Ohne Unterstützung seitens der Fachbereiche können Sie insbesondere die Schutzbedarfsfeststellung nicht durchführen. Lassen Sie sich nicht auf Diskussionen ein, dass keiner Zeit für solche Maßnahmen hat. Die Praxis hat gezeigt, dass Sie für eine Schutzbedarfsfeststellung pro Fachbereich maximal 2 Stunden benötigen. So viel Zeit muss jeder Fachbereich haben. Nutzen Sie effektiv die Vorlagen aus diesem Praxisleitfaden.

ÜBERSICHT: Win-win-Situation Projekt „Datensicherheit“			
Maßnahme	**Ziel**	**Beteiligter Bereich**	**Nutzen/Bereich**
Struktur-analyse	Erhebung der IT-Infrastruktur	IT-Abteilung	• Aussagekräftige Übersicht über Systeme und Investitionen, Basis für Notfallpläne, Budgetplanung, Versicherungen usw. • IT-Abteilung, Geschäftsleitung, Risikocontrolling/OpRisk
Schutz-bedarfsfest-stellung	Erhebung des Schutz-bedarfs	bDSB IT-Abteilung Fachbereiche	• Beschränkung der Datensicherheits-maßnahmen auf „wesentliche“ Komponenten: Basis für Notfallpläne (Verfügbarkeit), Risikocontrolling (OpRisk), Investitionen unter Kosten-Nutzen-Aspekten möglich, eventuelle Kostensenkungen durch Anpassung interner Maßnahmen und Maßnahmen bei IT-Dienstleistern. Fachbereiche erhalten Transparenz zu ihren Anforderungen und der Umsetzung in der IT. • IT-Abteilung, Geschäftsleitung, Risikocontrolling/OpRisk, Fachbereiche
Risiko-analyse	Analyse der IT- und Datenschutz-risiken	bDSB IT-Abteilung	• Schaffung von Transparenz über die wesentlichen ITund Datenschutzrisiken. Basis für risikoorientierte Behandlung von Anforderungen aus den Fachbereichen an die IT oder Geschäftsleitung. Schaffung von Objektivität bei der Beurteilung von IT-Sicherheitsanforderungen und -maßnahmen. • IT-Abteilung, Geschäftsleitung, Risikocontrolling/OpRisk, Fachbereiche
Maßnahmen-plan	Ausarbeitung eines Maß-nahmenplans auf der Basis der Risiko-analyse	bDSB IT-Abteilung Fachbereich Geschäfts-leitung	• Risikoorientierte Schutzmaßnahmen verbessern das Schutzniveau und bieten die Chance von Kosteneinsparungen (Kosten-Nutzen-Risiko). • IT-Abteilung, Geschäftsleitung, Risikocontrolling/OpRisk Fachbereiche

© Egor – AdobeStock.com

PRIVACYXPERTS

ein Unternehmensbereich des VNR Verlags für die Deutsche Wirtschaft AG,
Theodor-Heuss-Str. 2–4, 53095 Bonn
Telefon: 02 28/9 55 01 50, Fax: 02 28/3 69 64 80
Internet: www.privacyxperts.de
E-Mail: kundendienst@privacyxperts.de

Vorstand: Richard Rentrop

Verantwortlicher i.S.d.P: Michael Jodda, Theodor-Heuss-Str. 2-4, 53095 Bonn

Autor: Andreas Würtz

Satz: Holger Hellendahl, Neuss

Alle Angaben wurden mit äußerster Sorgfalt ermittelt und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Eine Gewähr kann deshalb nicht übernommen werden.

© 2020 by VNR Verlag für die Deutsche Wirtschaft AG, Bonn, Bukarest, Manchester, Warschau