

Effiziente Einführung von Datenschutz und IT-Security

mit freundlicher Empfehlung des Autors
Axel Saffran

Sonderdruck aus IT-Security,
Ausgabe 6/2007

mit freundlicher Genehmigung des IT-Verlags
<http://www.it-verlag.de>



Einführungsmodelle für gesetzkonforme Unternehmenssicherheit

Effiziente Einführung von IT-Security

Ein Vorgehensmodell zur wirtschaftlichen und transparenten Einführung. „Datenschutz, oh, ja, ich weiß, da sollten wir dringend was machen“, so oder ähnlich lautet die Antwort vieler Geschäftsführer, IT-Leiter oder IT-Administratoren, wenn sie zum Stand der Umsetzung des gesetzlich vorgeschriebenen Datenschutzes in ihrem Unternehmen gefragt werden.



Die eher ablehnende Haltung einiger Unternehmen gegenüber transparenten vorschriftsmäßigen Datenschutzmaßnahmen sind kein Einzelfall. So gaben im Rahmen des Checkpoint-Securityindexes zu Beginn des letzten Jahres 45 % der Unternehmen mit 101 bis 250 Mitarbeitern an, noch keinen Datenschutzbeauftragten bestellt zu haben. In Betrieben mit über 500 Mitarbeitern fehlt dieser immerhin noch bei 30 % der Befragten.

Dies ist eigentlich unverständlich, da zunehmend von Kunden, Lieferanten und Partnern gelebter Datenschutz als Voraussetzung für eine neue Partnerschaft oder die Fortführung der Geschäftsbeziehung gefordert wird. Und muss man dann Datenschutz erst einführen, geht der Auftrag oft an den Mitbewerber. Und über den möglichen Imageverlust bei einem Datenschutzvorfall und

die persönliche Haftung der Geschäftsführung möchte man erst gar nicht nachdenken.

Ungeliebter Datenschutz

Aber woher kommt dann diese distanzierte Haltung der betroffenen Unternehmen? Datenschutz und insbesondere seine Einführung stehen in dem Ruf, kostenintensiv und risikobehaftet zu sein. Die Unternehmensleitung treibt oft die Angst um, dass viele Prozesse geändert werden müssen, große Investitionen folgen, schlicht, dass „kein Stein auf dem anderen bleibt“.

Aus diesen Gründen verfahren viele Unternehmen im Bereich des Datenschutzes nach dem Grundsatz „erstmal nichts machen und bloß nicht unangenehm auffallen“, hoffen, dass man selbst nicht in das Raster der Aufsichtsbehörde für den Da-

tenschutz fällt. Gleichzeitig wird auf die recht niedrigen personellen Ressourcen dieser Behörden gesetzt.

Manche Unternehmen sind schon einen Schritt weiter gegangen und haben einen Mitarbeiter zu einer Datenschutz-Schulung entsendet und alsbald zum Datenschutzbeauftragten bestellt. Der Mitarbeiter kommt „vollgepackt mit Paragraphen“ aus der Schulung zurück und weiß so gar nicht, wo er anfangen soll. Eine effiziente und wirtschaftliche Vorgehensweise zur Einführung kann, schon aus Zeitgründen, in den Basisschulungen nicht vermittelt werden.

Dieser Artikel stellt ein praxiserprobtes Vorgehensmodell zur Einführung des Datenschutzes in Unternehmen vor, das beginnend von den ersten Ergebnissen bis zur Einführung vollständige Prozess-Transparenz bietet. Das Modell basiert auf drei, wirtschaftlich unabhängigen

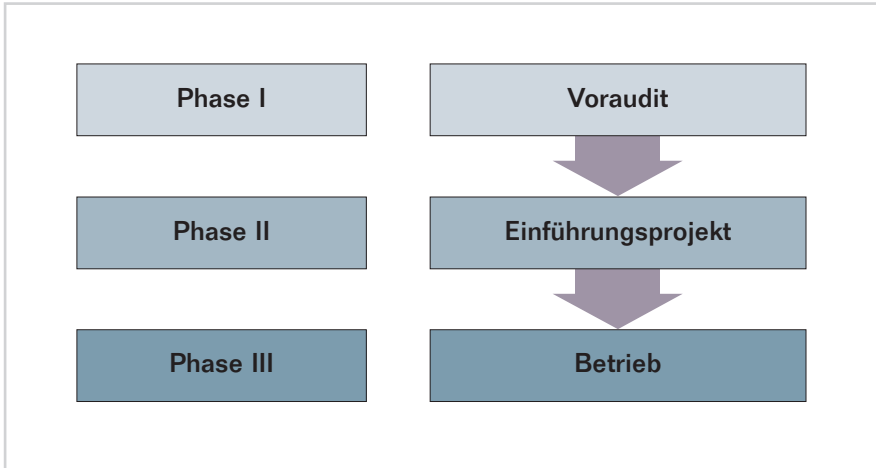


Abbildung 1: Überblick Vorgehensmodell

Phasen: Audit, Einführungsprojekt und Betrieb.

Phase I: Audit

Das hier vorgestellte Muster zur Datenschutz-Einführung beginnt mit einem Datenschutz-Audit. Im Rahmen von maximal vier bis fünf Arbeitstagen analysiert der interne betriebliche Datenschutzbeauftragte und/oder ein externer Berater das Unternehmen systematisch auf Datenschutzwachstellen, gemeinsam mit den Verantwortlichen der Fachabteilungen. Ziel des Audits ist die Identifizierung datenschutzrelevanter Unternehmensteile, Infrastruktureinrichtungen, Geschäftsprozesse, Betriebsvereinbarungen, Anwendungen, Datenbanken, IT-Systeme (Hardware, Software, Infrastruktur, ..), usw.

Vor Beginn des Audits sollten dem Auditor (der interne DSB oder der externen Berater) datenschutzrelevante Unterlagen zur Vorbereitung zur Verfügung gestellt werden. Dies dient, und das sollte den Gesprächspartnern im Vorfeld (z.B. im Rahmen der frühzeitigen Einladung) mitgeteilt werden, einer effizienten, kürzeren und somit wirtschaftlicheren Durchführung der eigentlichen Befragungen. Wichtige und notwendige Unterlagen sind beispielsweise die aktuelle IT-Dokumentation und sämtliche datenschutzrelevante Betriebsvereinbarungen oder Arbeitsanweisungen (Internet-/eMail-Nutzung, Zeiterfassung, ...).

Zur Durchführung des eigentlichen Audits empfiehlt sich die Organisation von mehreren „Fachgesprächen“ zwischen den Leitern der Fachabteilungen IT, Personal, Buchhaltung, Controlling, Vertrieb und dem Datenschutzbeauftragten oder dem externen Berater. Diese Gespräche sollten aus Effizienzgründen zeitnah, d.h. innerhalb zwei aufeinanderfolgenden Tagen durchgeführt werden, auch um das Thema und das Interesse der Beteiligten warm zuhalten.

Wie jedes Projekt sollte auch das Datenschutz-Audit mit einem kleinen Kick-Off-Veranstaltung starten, in der die in den nächsten Tagen befragten

Personen mit dem Thema vertraut gemacht und für das Thema anhand täglicher Lebenssituationen sensibilisiert werden. Außerdem sollten die Gesprächspartner auf die Inhalte der Diskussionen vorbereitet werden und ihnen die Angst vor problematischen Fragen genommen werden. Der Tenor sollte ein „wir möchten Ihnen helfen, und wenn Sie es aus fehlendem Wissen bisher etwas falsch gemacht haben, ist dies kein Problem, wir unterstützen Sie dabei, es in der Zukunft richtig zu machen“ sein. Wichtig ist die Teilnahme der Geschäftsführung an diesem Kick-Off, da somit den Anwesenden die Wichtigkeit oder auch Brisanz des Themas klar gemacht wird. Das steigert oft die Bereitwilligkeit und somit die Effizienz der Mitarbeiter zur Zusammenarbeit.

Wichtig für die Akzeptanz und damit für den Erfolg dieser „Befragungen“ ist eine gute Gesprächsatmosphäre. Schon von Beginn an sollte deshalb nicht von Befragung, sondern von „Fachgesprächen“ oder „Diskussionen“ gesprochen werden. Sinnvoll ist auch, den Betriebsrat gleich mit ins Boot zu nehmen. Je nach Firmengröße sollte ein Betriebsratsmitglied bei allen Befragungen anwesend sein. Spätere Diskus-

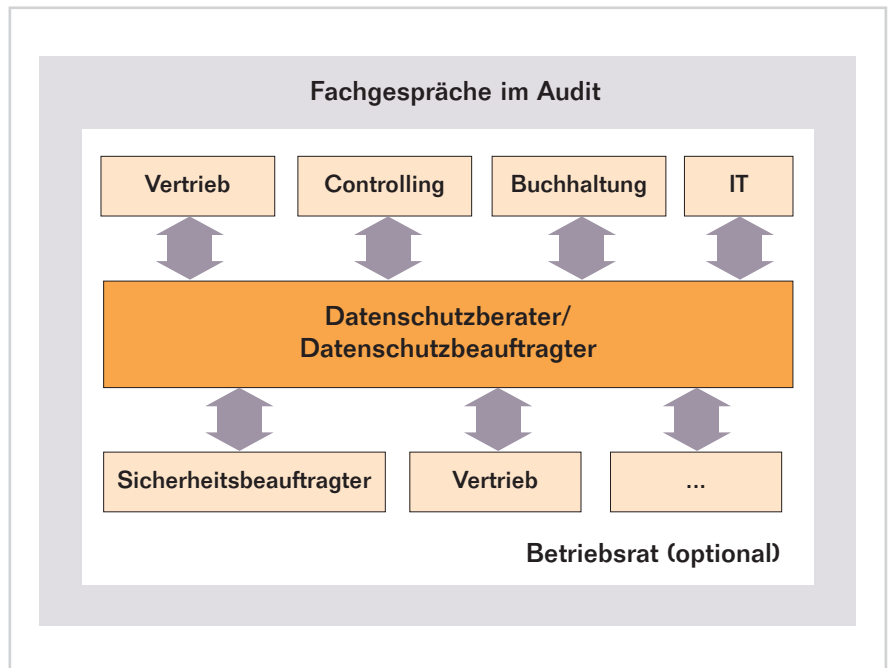


Abbildung 2: Fachgespräche

sionen, beispielsweise bei notwendigen Änderungen von Betriebsvereinbarungen, werden dadurch erheblich vereinfacht.

Fachgespräche

Die Fachgespräche an sich sollten anhand eines vorbereiteten, detaillierten Fragebogens durchgeführt werden. Einerseits um die Gespräche strukturiert zu führen, andererseits

kontrolle, Trennungsgebot) untersucht werden.

Der Detaillierungsgrad sollte hoch sein. So sollten beispielsweise bei den genutzten Passwortkonventionen sowohl die Konventionen (Ausschluss Trivialkennworte, Klein-/Großbuchstaben, Zahl, Sonderzeichen, Gültigkeitsdauer in Tagen: ... , Anzahl der Generationen ?) als auch deren Umsetzung erfragt werden, technisch (zum Beispiel Gruppen-

nehmen „Personalakten“ liegen können (Beispiele: in den Fachabteilungen, im Bereich der Arbeitssicherheit/des Betriebsarztes, in Veröffentlichungen (Mitarbeiterzeitungen, ...), in technischen Systemen (Personalinformationssystem, Dokumentenmanagementsystem, ...), usw.). Mit der Vertriebsabteilung beispielsweise sollte der Umgang mit Freifeldern im CRM-System besprochen werden, da hier oftmals datenschutzrechtlich als



„Beim Thema Datenschutz fürchten viele Unternehmen hohe Investitionen und Prozessänderungen mit Folgerisiken.“

zu Dokumentationszwecken. Der Fragebogen sollte die wichtigsten, häufigsten Datenschutzschwachstellen in Unternehmen abdecken. Beginnend bei allgemeinen organisatorischen Fragestellungen (Verpflichtung/Schulung der Mitarbeiter, IT-Sicherheit, Notfallvorsorge, Datensicherung) sollten die vom Bundesdatenschutzgesetz geforderten technisch-organisatorischen Maßnahmen (Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Auftragskontrolle, Verfügbarkeits-

richtlinien) oder organisatorisch (im Rahmen einer Arbeitsanweisung). Abschließend muss natürlich noch festgestellt werden, wie bei Verstoß gegen diese Konventionen technisch oder organisatorisch reagiert wird.

Sensitive Bereiche

Zusätzlich sollten besonders sensitive Bereiche durch separate Fragestellungen berücksichtigt werden. So sollte mit der Personalabteilung diskutiert werden, wo überall im Unter-

problematisch einzustufende Bemerkungen eingetragen werden, um den Kunden „optimal betreuen zu können“ (Beispiele aus der Praxis: „Kunde ist Fliegenfischer“, „Her Müller mag Rotwein“, „Frau Maier hat drei hübsche Töchter“, „Kunde ist leicht cholerisch“).

Nach den zwei Interviewtagen hat der Auditor schon einen guten Überblick über die Situation im Unternehmen. Im Idealfall zieht dieser sich dann für weitere zwei Tage zurück, um die Ergebnisse zu analy-

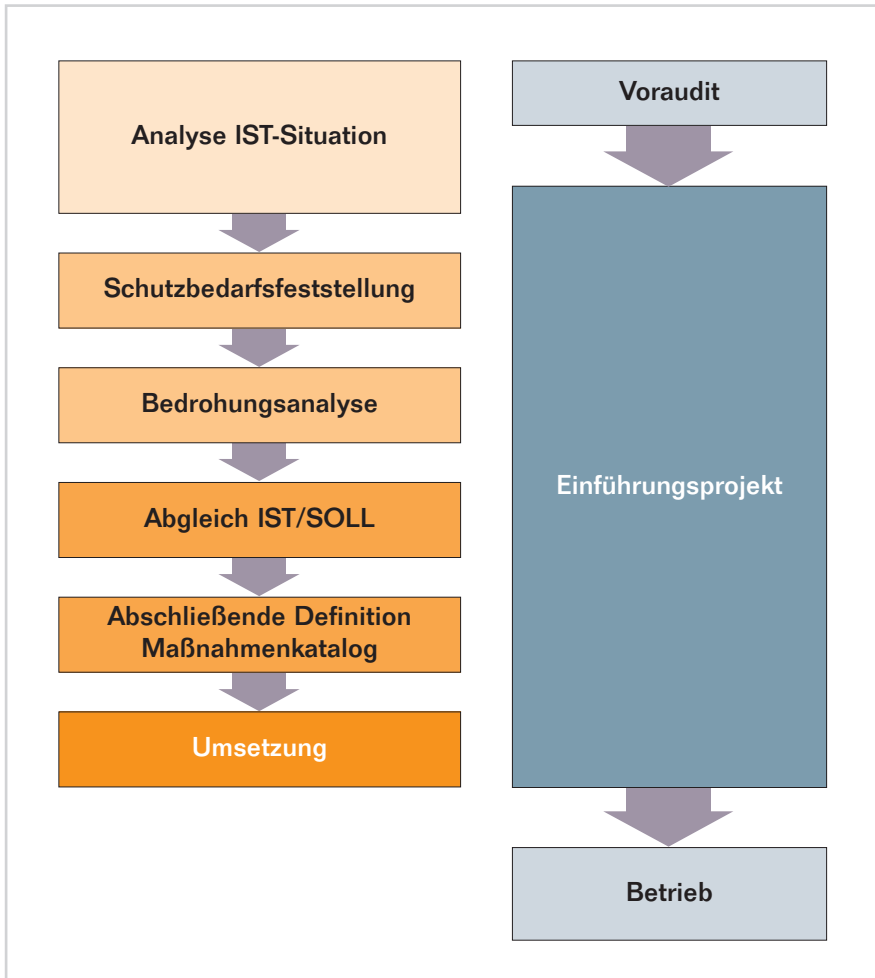


Abbildung 3: Einführungsprojekt

sieren, schwierige Fragestellungen genauer zu untersuchen und die gewonnenen Erkenntnisse in einem Ergebnisdokument zusammenzufassen. Eigentlich immer ergeben sich in den Diskussionen Nachfragen, die dann per mail oder in weiterführenden Gesprächen geklärt werden.

Das Ergebnisdokument sollte auf maximal 20 – 25 Seiten die Resultate der Befragungen in leicht lesbarer Form darstellen. Bewährt hat sich eine Struktur beginnend mit einer vorangestellten maximal dreiseitigen Management-Summary, eine Beschreibung der Vorgehensweise und einer Darstellung der Ergebnisse. Die Ergebnisdarstellung kann unterteilt werden in die Abschnitte „Basisdatenschutz“, „Technische und organisatorische Maßnahmen“ und „Personelle Maßnahmen“. Im Abschnitt Basisdatenschutz wird auf die aktuelle Situation bezüglich der grundlegen-

den Dokumente (Verpflichtungen, ...), der Auftragsdatenverarbeiter, des Verfahrensverzeichnis usw. eingegangen. Das Kapitel „Technische und organisatorische Maßnahmen“ befasst sich mit der IT im weitesten Sinne, den Arbeitsanweisungen, den Betriebsvereinbarungen, usw. Der Abschnitt „Personelle Maßnahmen“ führt Optimierungsmöglichkeiten im Bereich des IT Knowhows, der Mitarbeiterschulungen, o.ä. auf.

Ergebnisdokument

Abgeschlossen werden sollte das Ergebnisdokument mit einem Maßnahmenkatalog. Dieser kann, nach einer nur zweitägigen Untersuchung des Unternehmens zwangsläufig nur einen vorläufigen Charakter haben. Erfahrungsgemäß jedoch werden durch das Audit schwerwiegende und somit meist investitionsträchtige Mängel be-

reits aufgedeckt, so dass später auftauchende, zusätzlich notwendige Maßnahmen hinsichtlich der Kosten oder Änderungen der Organisation relativ übersichtlich bleiben. Zusammenfassend erhält die Unternehmensführung durch das Ergebnisdokument einen Überblick, welche Erstmaßnahmen getroffen werden sollten und mit welchen Umstellungen voraussichtlich zu rechnen sein wird.

Mit Abgabe des Ergebnisdokuments ist der erste Abschnitt des Vorgehensmodells abgeschlossen. Abhängig von den Resultaten steht es der Unternehmensführung frei, wie weiter mit dem Thema „Datenschutz“ umgegangen werden soll. Im Wesentlichen ergeben sich die folgenden Alternativen:

Falls das Voraudit durch einen externen Berater durchgeführt wurde und man diesem vertraut oder von seiner Kompetenz überzeugt wurde, ist es sinnvoll, auch das Einführungsprojekt durch diesen durchführen zu lassen. Er sollte dann auch in der Lage sein, ein detailliertes Angebot abzugeben.

Natürlich kann auch, insbesondere bei unproblematischen Fragestellungen oder aus wirtschaftlichen Erwägungen, die Einführung durch internes Personal durchgeführt werden, mit der optionalen Möglichkeit punktuell den externen Berater hinzuzuziehen.

Phase II: Einführungsprojekt

Basierend auf dem Ergebnisdokument ist eine grobe wirtschaftliche Einschätzung der notwendigen Maßnahmen möglich und es kann ein realistisches Einführungsprojekt für die Einführung des Datenschutzes als Phase zwei des Vorgehensmodells geplant werden. Im Einführungsprojekt liegen die inhaltlichen Schwerpunkte insbesondere in der Anpassung des Unternehmens an die gesetzlichen Anforderungen und die Herstellung von Rechtssicherheit.

Für das Einführungsprojekt sollte neben dem Projektleiter ein Kernteam definiert werden. Diesem

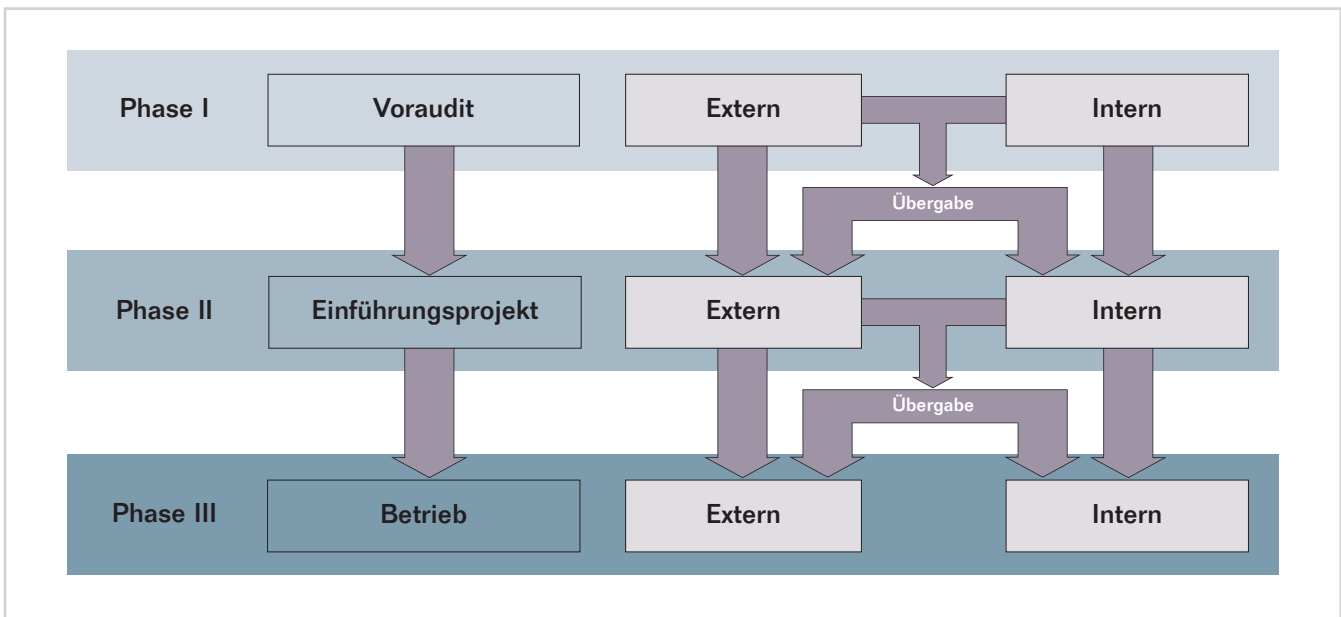


Abbildung 4: Zusammenarbeit Externe und Interne Datenschutzberater

gehören, neben dem Datenschutzbeauftragten, der Leiter der Informationstechnik und Endanwender an. Abhängig von den jeweilig zu bearbeitenden Aufgaben sollte das Kernteam bei Bedarf um weitere Personen mit unterschiedlicher Fachkompetenz ergänzt werden, beispielsweise aus der IT, den Fachabteilungen, externe oder interne Juristen und Entscheider im weitesten Sinne (Geschäftsführung und Betriebsrat).

Erste Schritte

Als erster Schritt des Einführungsprojektes wird zunächst das Ergebnis des Vorausdits verfeinert. Hierzu wird eine Schutzbedarfsfeststellung durchgeführt. Hier werden die zu schützenden „Objekte“ zunächst noch einmal detailliert gesammelt. Ziel sollte eine abschließende Aufstellung aller Daten, Verfahren und die damit verbundenen Systeme, Netze, Räume, Gebäude und Personen sein. Diese Objekte werden kategorisiert und ihnen werden jeweils Schutzstufen zugeordnet.

Diese Schutzstufen orientieren sich an klassischen Bewertungsmustern wie öffentlich (z.B. Angaben, die auch im Telefonbuch oder Melderegister stehen), intern (z.B.

Dienst- bzw. Schichtpläne, Position und Einsatzgebiete, Urlaubsplan, Telefonliste etc.), vertraulich (z.B. einzelne Vorkommnisse aus der Tätigkeit, Entlohnung etc.) oder streng

vertraulich (z.B. Beurteilungen, private Angaben, Gesundheit, Pfändungen). Spezielle Beachtung müssen „besondere Daten“ nach § 3 Abs. 9 Bundesdatenschutzgesetz finden:

Intern oder Extern

Grundsätzlich stellt sich die Frage, ob die Dateneinführung (und die spätere Besetzung des Datenschutzbeauftragten) mit internen Kräften durchgeführt oder ob externe Beratung eingekauft werden soll. Beide Varianten haben Vor- und Nachteile.

Für den internen Weg spricht die detaillierte Kenntnis des (internen) Mitarbeiters der Betriebsabläufe, außerdem kennt er eventuell vorhandene „Pappenheimer“. Außerdem mag die Nutzung der vorhandenen internen Ressource eine höhere Wirtschaftlichkeit versprechen, da vorhandene personelle Ressourcen genutzt werden. Nachteilig sind der „erhöhte“ Kündigungsschutz des internen DSBs, die „laufenden Kosten“ (Schulungen, Fachliteratur, ...) und mögliche Interessenkollisionen. Oftmals scheidet die Bestellung eines

internen DSB jedoch schlicht an der fehlenden „passenden“ Person, die Fachkompetenzen aus dem Bereich der IT, des Datenschutzrechts und organisatorischer Fragen mitbringen muss.

Dem gegenüber steht der externe Berater. Seine Vorteile liegen in der geringeren Gefahr der Betriebsblindheit und der oftmals größeren Akzeptanz („der Prophet im eigenen Land ...“). Vorteilhaft stellt sich auch die Haftungssituation, die mögliche Nutzung von Synergieeffekten durch die größere Erfahrung auch aus anderen Unternehmen und geringere Interessenkollisionen dar. Und eigentlich wollen sich viele Unternehmen nicht um das Thema Datenschutz selbst kümmern, Konzentration auf Kernkompetenzen ist hier das Stichwort. Oft hat sich ein Mittelweg, insbesondere aus wirtschaftlichen Gründen, als ideal erwiesen. Im Unternehmen wird ein „Datenschutzkoordinator“ aufgebaut, der als Ansprechpartner für Datenschutzfragen gilt und diese an den externen Datenschutzbeauftragten weiterleitet.

Inhaltliche Schwerpunkte des Einführungsprozesses

- Anpassung des Unternehmens an die rechtlichen Anforderungen des BDSG (Bundesdatenschutzgesetz) und an die EU-Richtlinie 95/46 EG und weiterer Gesetze mit datenschutzrelevanten Inhalten.
- Grundsätzliche Herstellung von Rechtssicherheit, Betriebssicherheit und Arbeitssicherheit aus datenschutzrechtlicher Sicht.
- Outsourcing – Funktionsübertragung und Auftragsdatenverarbeitung (Entsorgung, Abrechnung durch Externe (Inkasso / Personaldaten, etc.), Archivierung, Marketing, Wartung und Fernwartung (EDV, TK-Anlage, ...))
- Elektronische Archivierung (z.B.: steuerlich relevanter Unterlagen)
- Datenschutzrechtliche Anforderungen bei diversen Kommunikationsformen
- Technisch – organisatorische Maßnahmen
- Erarbeitung verschiedener Anweisungen (Ausarbeitung einer Basis-Datenschutz-Policy, Betrieblicher Datenschutz und Schweigepflicht, Behandlung von Postein- und -ausgang, Archivordnung, Marketingdaten, Übermittlung von Daten an staatliche Einrichtungen (Fiskus, ...), Meldepflicht von Dateien mit personenbezogenen Daten, Auskünfte an Staatsanwaltschaften und Polizei, ...)
- Arbeitnehmerdatenschutz
- Sonstiges
 - Datenübermittlung innerhalb unternehmenseigener Einrichtungen und an Externe in Deutschland innerhalb der EU und in Drittstaaten
 - Einsichtsrechte in Personalakten
 - Mitarbeiterschulungen
 - Erstellung „Datenschutz-Handbuch“

„Angaben über rassische/ ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben“.

Anschließend erfolgt eine Bedrohungsanalyse, in der Schwachstellen und Risiken, soweit dies nicht schon im Rahmen des Voraudits durchgeführt wurde, identifiziert werden. Mögliche, häufig vorkommende Schwachstellen sind beispielsweise unzureichender Einbruchschutz, Brandschutz, Schutz vor Wasserschäden, Virenschutz, usw. Erstaunlicherweise tauchen, trotz der erheblichen Haftungsrisiken für die Geschäftsführer, auch die Themen Backup / Backupstrategie / Auslagerung von Datenträgern immer wieder als Schwachstellen bei Datenschutzeinführungen auf. Basierend auf den gefundenen Schwachstellen und den jeweils den Objekten zugeordneten Schutzstufen wird das vorhandene

Risiko identifiziert und Ziele einer Risikoreduktion definiert.

Datenschutzziele

Parallel werden Datenschutzziele und -leitlinien für das Unternehmen definiert (Sollzustand), diese mit dem IST-Zustand abgeglichen und mögliche Maßnahmen zur Erreichung dieser Ziele und Leitlinien erstellt. Diese Maßnahmen werden nach Wirksamkeit und Kosten beurteilt und der Maßnahmenkatalog, der bereits im Audit erstellt wurde, entsprechend ergänzt.

Diese Ergänzung des ersten Maßnahmenkatalogs aus dem Audit durch die dargestellten Schritte (Schutzbedarfsfeststellung, Bedrohungs- und Schwachstellenanalyse, Datenschutzziele/-leitlinien) hat sich in vielen Datenschutzeinführungsprojekten als sehr sinnvoll erwiesen. Wie bereits erwähnt, wird durch das vorangestellte

Audit ein Großteil der vorhandenen Schwachstellen identifiziert. Ein vollständiger Schutz der Unternehmensdaten kann nur über die beschriebene Vorgehensweise erreicht werden, da nur so der notwendige Detaillierungsgrad erreicht werden kann. Die hierzu notwendigen Aufwände (intern und extern) variieren natürlich stark und sind abhängig von Unternehmensgröße, Branche, Struktur und Komplexität der IT-Landschaft, usw.

Mit dem abschließenden Maßnahmenkatalog kann nun die eigentliche Umsetzung starten. Die Rollen in der Umsetzung sind durch die Kompetenzen definiert, das Projektteam oder der DSB nimmt die erledigten Aufgaben ab und führt die Qualitätskontrolle durch.

Mit Abschluss des Einführungsprojekts ist die zweite Phase des Vorgehensmodells abgeschlossen und, das ist die gute Nachricht für das Unternehmen, das Unternehmen erfüllt nun die rechtlichen Anforderungen des Datenschutzes.

Abhängig von der Durchführung des Einführungsprojekts ergeben sich mehrere Möglichkeiten zur weiteren Vorgehensweise. Wurden die Arbeiten im Bereich des eigentlichen Datenschutzes (Erstellung Verzeichnisses, Mitarbeiterschulungen, ...) durch einen externen Dienstleister geleistet, bietet sich als erste Alternative seine Bestellung als externer Datenschutzbeauftragter an. Alternativ kann ein interner Mitarbeiter zum DSB bestellt werden, dann muss nun eine ausführliche und intensive Übergabe des Datenschutzes durch den Externen erfolgen.

In jedem Fall folgt der eigentlichen Einführung die dritte Phase unseres Vorgehensmodells, der Betrieb.

Phase III: Betrieb

Die dritte Phase des Vorgehensmodells umfasst den kontinuierlichen „Betrieb“ des Datenschutzes im Unternehmen. Datenschutz ist permanenten Wandlungen unterworfen,

einerseits durch gesetzliche Änderungen, aber auch beispielsweise durch Einführung neuer IT-Systeme, deren datenschutzrechtliche Relevanz geprüft werden muss. Hier ist es sinnvoll, den Datenschutzbeauftragten in die IT-Planungs- und Beschaffungsprozesse zu integrieren, so dass er über neue Vorhaben informiert ist, frühzeitig reagieren und beratend tätig sein kann.

Auch müssen Aufzeichnungen und Nachweise über Schulungen/Verpflichtungen erstellt werden. Desweiteren sind die umgesetzten Änderungen im Unternehmen (sowohl seitens der IT als auch in der Organisation) einer ständigen Überwachung, Kontrolle und Dokumentation durch den Datenschutzbeauftragten zu unterziehen. Idealerweise wird diese Tätigkeit durch regelmäßige kleinere Audits (im Rahmen von zwei Tagen pro Jahr) ergänzt.

Diese Arbeit wird durch den (internen oder externen) betrieblichen Datenschutzbeauftragten in

Zusammenarbeit mit den Fachabteilungen geleistet.

Zusammenfassung

Datenschutz wird zunehmend zum wichtigen Wettbewerbsfaktor, immer mehr Unternehmen erwarten von ihren Kunden, Lieferanten und Partnern „gelebten Datenschutz“. Trotzdem sträuben sich viele Unternehmen davor, Datenschutz einzuführen, da sie befürchten, dass dies erhebliche Störungen des Betriebsablaufs mit sich bringt. Richtig ist, dass die Einführung im Ergebnis immer Umstellungen oder auch Einschränkungen mit sich bringt, sowohl für den „normalen“ Mitarbeiter, als auch für die Administratoren. Jedoch zeigt die Praxis, dass diese Änderungen überschaubar bleiben, denn Datenschutz sollte immer angemessen sein, da Datenschutz selten zum Kerngeschäft des Unternehmens gehört.

Das vorgestellte Vorgehensmodell zeigt einen Weg auf, um Datenschutz

in einem Unternehmen effizient, transparent und wirtschaftlich zu integrieren. Es zeichnet sich durch die Unabhängigkeit der drei Phasen Audit, Einführungsprojekt und Betrieb aus. Je nach Ressourcenverfügbarkeit, Knowhow im Unternehmen und Investitionsbereitschaft kann jede Phase durch internes und / oder externes Personal bewältigt werden. Durch diese Auftrennung wird inhaltliche und wirtschaftliche Transparenz gegenüber Mitarbeitern und Unternehmensführung geschaffen. Jede Phase kann separat beauftragt und abhängig von den wirtschaftlichen Möglichkeiten durchgeführt werden. Auch die stufenweise Entwicklung des Maßnahmenkatalogs, die Beurteilung der Maßnahmen nach Wirksamkeit und Kosten und die darauf basierende Definition der umzusetzenden Maßnahmen sorgt für eine effiziente und wirtschaftliche Realisierung.

Axel Saffran

Unsere Leistungen

- Vor-Ort-Check up Ihres Unternehmens hinsichtlich Datenschutz und Datensicherheit
- Anpassung des Unternehmens an die rechtlichen Anforderungen des BDSG (Bundesdatenschutzgesetz) und an die EU-Richtlinie 95/46 EG und weiterer Gesetze mit datenschutzrelevanten Inhalten
- Erstellung Verarbeitungsverzeichnis und Verfahrensverzeichnis
- Prüfung der Technisch-Organisatorischen Maßnahmen
- Bereitstellung eines externen Datenschutzbeauftragten nach §4f BDSG
- Mitarbeiterschulungen zu den Themen Datenschutz, Datensicherheit und Schweigepflicht
- Umfassender Telefon- und e-Mail-Support
- Wir halten Sie auf dem Laufenden – mindestens zweimal im Jahr erhalten Sie einen Newsletter mit aktuellen Informationen zum Thema
- Kurze Reaktionszeiten bei sämtlichen Fragestellungen zum Thema Datenschutz und IT-Sicherheit
- Kompetente, unabhängige Beratung zu den Themen IT, Datenschutz und Datensicherheit



Axel Saffran
Dipl.-Informatiker
Datenschutzauditor (TÜV)
Wattwillerstraße 13
79241 Ihringen
Fon: +49-(0)7668-902515
Fax: +49-(0)7668-902516
info@saffran.net
www.saffran.net

Datenschutz – wir kümmern uns