Datenschutz: Verhältnismäßigkeit von technischen und organisatorischen Maßnahmen

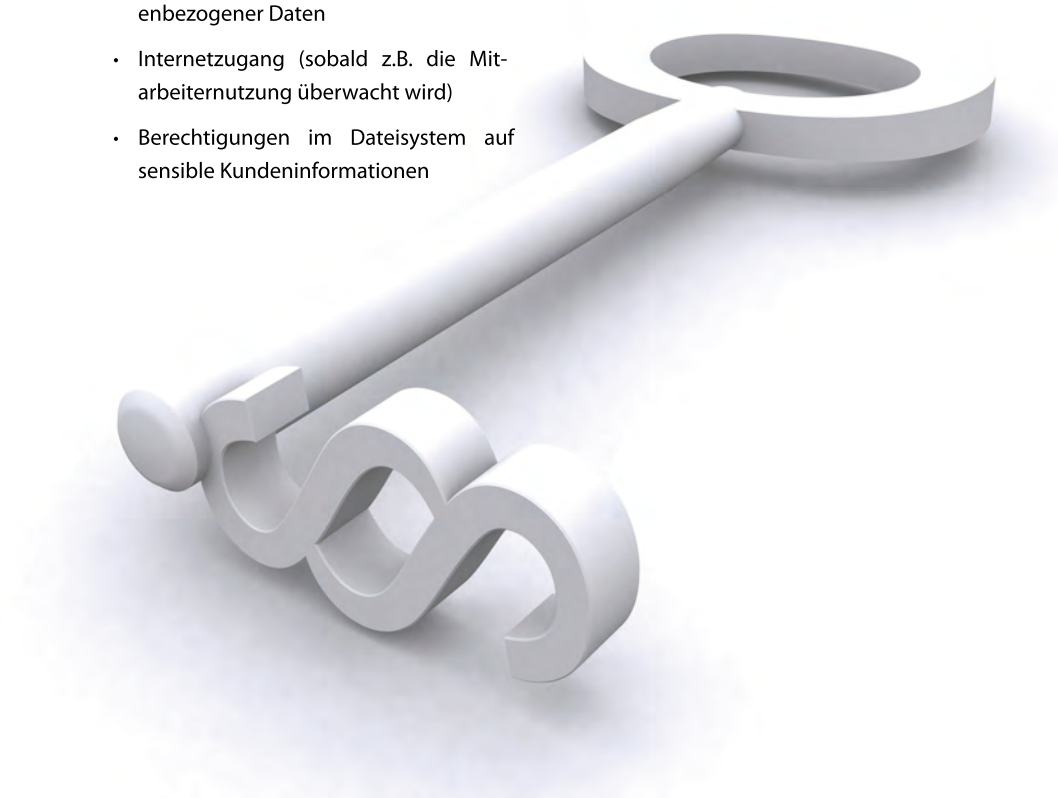
Das BDSG klassifiziert im Anhang von §9 die Maßnahmen zur Minderung von Datenschutzrisiken. Dabei erhalten Unternehmen einen gewissen Spielraum, um einen angemessenen Aufwand zu betreiben. Die Entscheidung, welche Maßnahmen erforderlich sind und welche nicht, ist jedoch nicht leicht und sollte fundiert getroffen werden.

IT Wissen ist gefragt

§9 des Bundesdatenschutzgesetzes fordert von Unternehmen die Umsetzung von technischen und organisatorischen Maßnahmen zum Schutz von personenbezogenen Daten.

Nach Aufnahme der datenschutzrelevanten Prozesse (Verfahren) ergeben sich die vom Gesetz betroffenen Stellen bzw. Risiken. Dazu zählen beispielsweise:

- Datenbank mit abgespeicherten Daten von Privatkunden
- E-Mail Verkehr zum Austausch personenbezogener Daten
- Internetzugang (sobald z.B. die Mitarbeiternutzung überwacht wird)
- Berechtigungen im Dateisystem auf sensible Kundeninformationen



Schon diese kleine Auflistung macht klar, dass ein Großteil der IT Systemkomponenten mit persönlichen Daten zu tun haben und somit abgesichert werden müssen. Konkretisiert werden diese Anforderungen im Anhang zum Satz 1 des §9 BDSG. Dabei ist das Wort „Anhang" jedoch für den Nicht-Juristen eher irreführend, denn gerade in diesen Regelungen sind die zentralen Umsetzungsrichtlinien des Datenschutzes für IT Systeme geregelt.

Gemäß diesem Gesetz wird bei einem Datenschutzbeauftragten ein hohes Maß an IT Know How gefordert, so dass man für diese Arbeit eine gewisse Affinität zur IT benötigt. Nicht selten werden gerade aus diesem Grund Mitarbeiter mit IT Vergangenheit zum Datenschutzbeauftragten ernannt – wobei hier darauf zu achten ist, dass ein Mitarbeiter nicht Datenschutzbeauftragter und Systemadministrator zugleich sein sollte, um Interessenskonflikte zu vermeiden.

Übersicht über die erforderlichen Maßnahmen zum Schutz der Daten nach Anlage zu §9 Satz 1 BDSG:

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren *(Zutrittskontrolle)*
2. Nutzung der DV-Anlagen verhindern *(Zugangskontrolle)*
3. Zugriff nur für berechtigten Personen *(Zugriffskontrolle)*
4. Sicherstellung einer korrekten Übermittlung von Daten *(Weitergabekontrolle)*
5. Möglichkeit der Nachverfolgbarkeit von Eingaben in Softwareprodukte *(Eingabekontrolle)*
6. Im Auftrag Dritter verarbeitete Daten nur gemäß den Anweisungen verarbeiten *(Auftragskontrolle)*
7. Schutz vor Zerstörung oder Verlust von Daten *(Verfügbarkeitskontrolle)*
8. Zweckbindung der Verarbeitung und keine Vermischung von Daten *(Trennungsgebot)*

Einen Überblick über die im Gesetz erwähnten technischen und organisatorischen Maßnahmen finden Sie in der Infobox. Diese Maßnahmen sind je nach Unternehmen und des Umfangs der Verwendung von personenbezogenen Daten mehr oder weniger mit Aufwand verbunden.

Doch wie viel Aufwand ist denn angemessen? Muss ein Unternehmen mit 5 Mitarbeitern 50.000 € ausgeben, um mit den neuesten und hochwertigsten technologischen Mitteln das System zu sichern?

Für diese Fragen gibt es keine eindeutige Antwort – und gerade deswegen hat der Gesetzesgeber in §9 Satz 2 BDSG diesen Graubereich auch erwähnt:

„Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhält-

nis zu dem angestrebten Schutzzweck steht."

Diese Aussage lässt viele Interpretationen zu und daher ist es wichtig, im Falle einer Prüfung sowie bei Nachfragen erklären zu können, warum nun eine Maßnahme getroffen wurde oder nicht. Hier kommt die Risikoanalyse ins Spiel. Wie bei jedem Sicherheitskonzept geht auch hier den konkreten Umsetzungsanweisungen eine Analyse der Prozesse voraus. Es sind alle datenschutzrelevanten Verfahren / Prozesse aufzunehmen und zu bewerten.

festlegen und gewichten. Ändern Sie diese Konfiguration nur bei groben Fehleinschätzungen.

Ebenfalls subjektiv ist auch Punkt 4, also die Festlegung, ab welchem Risikowert Maßnahmen getroffen werden sollen. Verinnerlichen Sie sich dabei das sogenannte Pareto-Prinzip. Dieses sagt aufgrund von statistischen Untersuchen aus, dass 80% eines Projektes durch 20% des Gesamtaufwandes durchgeführt werden können. Die restlichen 20% erfordern demnach 80% des Aufwandes.

„Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."

Risikoanalyse und -bewertung

Die Erfassung der Verfahren und deren Risikobewertung können sehr lange dauern, denn sie bilden die Grundlage für alle späteren Maßnahmen. Ohne die Risikoanalyse und –bewertung bauen die spätere Datenschutzrichtlinie und die Umsetzung von Maßnahmen auf nichts auf und Sie haben keine Möglichkeit sich zu rechtfertigen.

Gehen Sie bei der Risikoanalyse wie folgt vor:

1. Aufnahme der datenschutzrelevanten Verfahren
2. Identifizierung der Risiken, die unter Anhang §9 BDSG fallen
3. Bewertung der Risiken nach gewissen Kriterien
4. Entscheiden, welche Risiken Maßnahmen erfordern und welche Risiken hinnehmbar sind

Die Bewertung der Risiken nach Punkt 3 ist eine sehr individuelle Sache. Es erfordert Fachkenntnis und Erfahrung, um einschätzen zu können, welchen Kriterien ein Risiko unterliegt. Es wären beispielsweise die Kriterien

- Kosten bei Eintritt
- Eintrittswahrscheinlichkeit
- Möglicher Imageverlust

auf einer Skala von 1 bis 5 möglich. Entweder man summiert oder multipliziert die Kriterien und bildet somit eine Rangfolge oder man gewichtet nochmals die Kriterien an sich. Tipp: Vermeiden sie Rechenspiele, indem Sie die Kriterien vorher

Schätzen Sie daher den Aufwand einer Maßnahme (oder lassen Sie schätzen) und stellen Sie es den Risikokennziffern gegenüber. Um das oben erwähnte Pareto-Prinzip im übertragenen Sinne anzuwenden: prüfen Sie, wie Sie 80% der erforderlichen Maßnahmen mit 20% des Gesamtaufwandes umsetzen können. Gehen Sie die restlichen 20% der Maßnahmen zu einem späteren Zeitpunkt an – außer diese Maßnahme steht ganz oben auf Ihrer Prioritätenliste. Aber selbst dann können Sie noch abwägen, dieses Risiko einzugrenzen, indem Sie die Maßnahmen Schritt für Schritt oder nur zu einem gewissen Grad durchführen und somit das Risiko mindern.

Ob Sie als Leser nun Datenschutzbeauftragter, IT Mitarbeiter oder Geschäftsführer sind, holen Sie bei Unklarheiten oder bei Themen, die nicht in Ihr Wissensgebiet fallen Hilfe von Experten, Beratern oder besser informierten Mitarbeitern. So kann ein Geschäftsführer wahrscheinlich nicht beurteilen, wie viel die Installation und Konfiguration einer sicheren Firewall-Lösung kostet. Ein IT Mitarbeiter ist möglicherweise in die Vorgaben der Auftragsdatenverarbeitung nicht eingeweiht und kann somit nicht beurteilen, ob diese umgesetzt werden oder nicht. Ein hohes Maß an Kooperation und Zusammenarbeit ist für eine reibungslose Festlegung der technischen und organisatorischen Maßnahmen demnach unabdingbar.

Fazit

Die technischen und organisatorischen Anforderungen sind wichtige Bestandteile des Bundesdatenschutzgesetzes. Sie geben explizit vor, welche Maßnahmen zum Schutz personenbezogener Daten zu treffen sind. Dies kann mit hohem Aufwand verbunden sein. Der Satz 2 in §9 BDSG gibt dem Datenschutzbeauftragten und später auch der verantwortlichen IT Abteilung jedoch den notwendigen Spielraum, um das Budget nicht zu überfordern. Dies kann die Akzeptanz des Datenschutzes in Unternehmen erhöhen. Eine Risikoanalyse ist jedoch unabdingbar um die Entscheidungen im Nachhinein rechtfertigen zu können.

Thomas Göhrig

Zum Autor

Thomas Göhrig hat Wirtschaftsinformatik an der Dualen Hochschule Baden-Württemberg studiert und als Dipl.-Wirtschaftsinformatiker (BA) abgeschlossen. Weiterhin ist er IHK geprüfter externer Datenschutzbeauftragter. Seit Anfang 2007 ist er Geschäftsführer des auf kleine und mittelständische Unternehmen spezialisierten Unternehmens IT & Management Solutions GmbH. Das Unternehmen bietet neben einer ganzheitlichen Systemadministration auch die Beratung im Hinblick auf EDV Sicherheit und Datenschutz an. Zum Portfolio gehören zudem auch die Erstellung von Webseiten und Webanwendungen sowie individuelle EDV Trainings.
www.ims-web.de