16.12.2011

Kosten und Nutzen des Datenschutzes

Nicht unerhebliche Kostensenkungen können auch durch eine professionelle Umsetzung des Maßnahmenkatalogs im Anhang zu § 9 BDSG erreicht werden. Nach dieser Rechtsvorschrift müssen Unternehmen und Behörden, die personenbezogene Daten automatisch verarbeiten, die technischen und organisatorischen Maßnahmen treffen, die erforderlich sind, um die Ausführung der Vorschriften des Bundesdatenschutzgesetzes zu gewährleisten. Insbesondere müssen die in der Anlage zu diesem Gesetz genannten Anforderungen durch Einsatz von bestimmten Techniken und Verfahren erfüllt werden.
Wer diesen Vorschriften durch eine professionelle Vorgehensweise gerecht wird, verbessert aber nicht nur die Situation des Datenschutzes im Hause. Er erhöht die Sicherheit der Informationstechnik in Unternehmen und Behörden in der Regel auch in solchen Bereichen, in denen es um handfeste eigene Interessen geht, die mit dem Datenschutz gar nichts oder nur wenig zu tun haben. Denn: Datenschutz ist Selbstschutz !!

(Quelle: Haufe Datenschutz)

Dass es auch hier fast immer um Kostensenkung geht, kann den Beispielen der folgenden Tabelle entnommen werden:

	Vorschrift nach § 9 BDSG (Anlage)	Auswirkungen von § 9 BDSG auf die IT-Sicherheit von Unternehmen und Behörden und die damit verbundenen Vorteile (im Sinne von Gruppe 1 Kap. 1)	Beispiele für den eigenen Vorteil, den Unternehmen und Behörden hierdurch haben können:
1	… die Innerbehördliche oder innerbetriebliche Organisation ist so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (Satz 1)	Tendenz zu mehr Vertraulichkeit beim Umgang mit firmeninternen Daten. Höhere Verlässlichkeit der firmeneigenen Datenbestände. Weniger Ausfälle der Datenverarbeitung. Gewinn an Transparenz der Datenverarbeitung	Geringere Fehleranfälligkeit der Datenverarbeitung. Rationalisierung der Datenverarbeitung z. B. durch Abbau von "Wildwuchs." Dadurch u. U. erhebliche Kostenersparnis.
2	… Unbefugten den Zutritt zu Datenverarbeitungs-Anlagen zu verwehren (Zutrittskontrolle)	**Vertraulichkeit** von firmeninternen Daten/Vertraulichkeit von Kommunikationsbeziehungen **Integrität** (Richtigkeit und Vollständigkeit) der firmeninternen Daten Verfügbarkeit der DV-Anlage, der Programme und Daten	Unbefugten wird es erschwert, Daten zur Kenntnis zu nehmen, Daten zu löschen oder zu verändern, Rechenprogramme zu manipulieren, Sabotage der Datenverarbeitung zu betreiben usw. Kostenersparnis, z. B. auch, weil Ausfall der Datenverarbeitung unwahrscheinlicher wird. Auch werden Kosten der Wiederherstellung von Daten, Hard- und Software gespart.

3	… zu verhindern, dass Datenverarbeitungsanlagen von Unbefugten genutzt werden können. (Zugangskontrolle)	**Vertraulichkeit** von firmeninternen Daten/Vertraulichkeit von Kommunikationsbeziehungen **Integrität** (Richtigkeit und Vollständigkeit) der firmeninternen Daten Verfügbarkeit **der DV-Anlage, der Programme und Daten**	Zum Teil erhebliche Kostenersparnis, weil es Unbefugten erschwert wird, Daten zur Kenntnis zu nehmen (z. B. Betriebsgeheimnisse), Daten zu löschen oder zu verändern (z. B. Kundendaten), Rechenprogramme (z. B. von Produktionsabläufen) zu manipulieren, Rechner (und damit Know-how) auszuspionieren (z. B. durch Einpflanzen von Trojanischen Pferden), Sabotage der Datenverarbeitung zu betreiben (und damit u. U. Insolvenz des Unternehmens auszulösen). Auch werden Kosten der Wiederherstellung von Daten, Hard- und Software gespart.
4	… zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können … (Zugriffskontrolle 1)	**Vertraulichkeit** von firmeninternen Daten/Vertraulichkeit von Kommunikationsbeziehungen Integrität **(Richtigkeit und Vollständigkeit) der firmeninternen Daten**	Zum Teil erhebliche Kostenersparnis, weil es Unbefugten erschwert wird, Daten zur Kenntnis zu nehmen (z. B. Betriebsgeheimnisse), Daten zu löschen oder zu verändern (z. B. Kundendaten), Rechenprogramme (z. B. von Produktionsabläufen) zu manipulieren, Rechner (und damit Know-how) auszuspionieren (z. B. durch Einpflanzen von Trojanischen Pferden). Verstärkt teilweise die Wirkung der Zugangskontrolle (Zeile 3)
5	… zu gewährleisten, … dass personenbezogene Daten bei der Verarbeitung und Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. (Zugriffskontrolle 2)	**Vertraulichkeit** von firmeninternen Daten/Vertraulichkeit von Kommunikationsbeziehungen Integrität **(Richtigkeit und Vollständigkeit) der firmeninternen Daten**	Verstärkt teilweise die Wirkung der Zugriffskontrolle 1 (Zeile 4)

6	… zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können … (Weitergabekon-trolle 1)	**Vertraulichkeit** von firmeninternen Daten/ Vertraulichkeit von Kommunikationsbeziehungen **Integrität** (Richtigkeit und Vollständigkeit) der firmeninternen Daten Zurechenbarkeit **von Daten und Personen im Netz (Internet)**	Zum Teil erhebliche Kostenersparnis, weil es Unbefugten erschwert wird, Daten zur Kenntnis zu nehmen, zu löschen oder zu verändern (z. B. Kunden-E-Mails). Bei Umsetzung dieser Maßnahme (zum Beispiel durch Einsatz entsprechender Verschlüsselungsverfahren) kommt hinzu, dass man sich darauf verlassen kann, dass Absender und Inhalt von E-Mails richtig und vollständig sind. Dann kann man sich z. B. auch darauf verlassen, dass die Ankündigung -eines Auftrags per E-Mail vom richtigen Auftrag-geber angekündigt wurde und der Inhalt nicht verfälscht wurde. Dadurch womöglich Vermeidung von finanziellen Ver-lusten.
7	… zu gewährleisten, dass personenbezogene Daten … während ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können … (Weitergabekon-trolle 2)	**Vertraulichkeit** von firmeninternen Daten / Vertraulichkeit von Kommunikationsbeziehungen bei Datentägeraustausch Integrität **(Richtigkeit und Vollständigkeit) der firmeninternen Daten**	Unbefugten wird es erschwert, Datenträger zu entwenden, Daten auf Datenträgern zur Kenntnis zu nehmen, Daten zu löschen oder zu verändern und unbefugt Datenträger zu kopieren. Auf diese Weise lässt sich z. B. auch verhindern oder zumindest erschweren, dass Betriebsgeheimnisse, Firmen-Know-how, Kundendaten usw. in die Hände von Konkurrenten gelangen.
8	… dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekon-trolle 3)	**Vertraulichkeit** von firmeninternen Daten / Vertraulichkeit von Kommunikationsbeziehungen **Integrität** (Richtigkeit und Vollständigkeit) der firmeninternen Daten Zurechenbarkeit **von Daten und Personen im Netz (Internet)**	Vermeidung von finanziellen Verlusten durch Verhinderung der unbeabsichtigten, aus Gründen der Schädigung oder aus kriminellen Gründen beabsichtigten Übermittlung von Daten (oder auch E-Mails) an Stellen, die diese Daten nicht haben sollen (Mitbewerber, Konkurrenten, Medien, Finanzämter usw.).

9	… zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle**)**	Integrität (Richtigkeit und Vollständigkeit) der firmeninternen Daten	Diese Maßnahme sollte nur aus Datenschutz-Gründen durchgeführt werden, da sie die Möglichkeit einer allgemeinen Leistungs- und Verhaltenskontrolle ermöglicht. Falls sie trotzdem auf die gesamte Datenverarbeitung ausgedehnt werden sollte, bringt sie natürlich vor allem einen Gewinn an Integrität der Daten
10	… zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers -verarbeitet werden können (Auftragskontrolle)	**Vertraulichkeit** von firmeninternen Daten / Vertraulichkeit von Kommunikationsbeziehungen Integrität **(Richtigkeit und Vollständigkeit) der firmeninternen Daten**	Verhinderung einer unbeabsichtigten, aus Gründen der Schädigung oder aus kriminellen Gründen beabsichtigten Datenverarbeitung beim Auftragnehmer und der unerwünschten Übermittlung von Daten des Auftraggebers an Dritte. Damit auch Verminderung der Gefahr von Betriebsspionage, Manipulation von Ergebnissen der Datenverarbeitung.
11	… zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)	Verfügbarkeit der DV-Anlage, der Programme und Daten	Schutz aller für das Unternehmen bzw. die Behörde wichtigen Daten gegen zufällige Zerstörung oder Verlust. Damit auch hier Vermeidung von unnötigen Kosten.
12	… zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können	**Vertraulichkeit** von firmeninternen Daten Integrität **(Richtigkeit und Vollständigkeit) der firmeninternen Daten**	Vermeidung von Fehlern mit finanziellen Konsequenzen bei der Bearbeitung von Kundenaufträgen. Verhinderung von Schadensersatzansprüchen aus unzulässiger Datenverarbeitung. Erhalt von "Herrschaftswissen".

Quelle: Haufe Datenschutz