

Der IT-Sicherheitsbeauftragte in Unternehmen des Gesundheits- und Sozialwesens (GSW)

Problemfall:

Rechtliche und inhaltliche Voraussetzungen sowie Unterstellungsverhältnisse bei der Bestellung eines IT-Sicherheitsbeauftragten im Vergleich mit dem Datenschutzbeauftragten (DSB)

Frage:

Welche Anforderungen müssen aus gesetzlicher und fachkundlicher Sicht bei der Bestellung eines IT-Sicherheitsbeauftragten durch das Unternehmen Krankenhaus beachtet werden?

Antwort:

Das Thema insgesamt ist sehr komplex, da es bisher keine der Bestellung eines DSB adäquate Regelungen gibt. Im Rahmen des IT-Grundschutzes hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Rolle des IT-Sicherheitsbeauftragten beschrieben. Es gibt hierzu den Vorschlag zu einer Dienstanweisung, in dem einige der wichtigsten Punkte festgelegt werden. Dort wird auch auf die Haftungspflicht der Geschäftsführung (die gesetzlich geregelt ist) und die Möglichkeit der Delegation von Aufgaben verwiesen. Im Internetangebot des Landesamtes für Datenschutz des Saarlandes ist eine Dienstanweisung für IT-Sicherheitsbeauftragte zu finden, die im Prinzip den Vorgaben im Grundschutzhandbuch nachempfunden ist (siehe unter <http://www.lfd.saarland.de>).

Über den bereits aufgeführten Bezug auf das Grundschutzhandbuch des BSI hinaus ist als wesentlicher Aspekt zu nennen, dass - sofern ein interner Mitarbeiter mit dieser Funktion beauftragt werden soll - in vergleichbarer Weise wie der DSB seitens der Geschäftsführung eine Bestellung einschließlich Funktionsbeschreibung und Vereinbarungen über Haftungsrisiken in Zusammenhang mit der Ausführung dieser Funktion erfolgen sollte. Eine verbindliche gesetzliche Basis wie etwa für den DSB oder den Umweltbeauftragten gibt es aber nicht. Dem zu Folge ist die Ernennung bzw. Bestellung eines IT-Sicherheitsbeauftragten als eine Erforderlichkeit im Rahmen von allgemeinen IT-Sicherheitskonzepten zu sehen und liegt so im Ermessen des jeweiligen Unternehmens, seine IT-Sicherheitspolitik entsprechend zu organisieren. Dabei ist eine sehr enge Verzahnung der Arbeit des DSB mit der des IT-Sicherheitsbeauftragten unerlässlich für den Erfolg der Maßnahmen.

Einige Einrichtungen haben sich schon wegen der Komplexität der Problematik in ihren Unternehmen entschieden, die IT-Sicherheit in die Hand eines IT-Sicherheitsausschusses mit einem Vorsitzenden zu legen. Der DSB hat dabei das Recht, jeder Zeit an den Sitzungen teilzunehmen.

Im § 22 SGB VII gibt es den "üblichen" Sicherheitsbeauftragten, der bzgl. IT-Sicherheit auch für die üblichen Prüfungen (wie die jährliche Plombe am Netzkabel) und z.B. für die Umsetzung der Bildschirmordnung (Stichwort Ergonomie) zuständig ist. Für diesen Sicherheitsbeauftragten gibt es im § 22 SGB VII entsprechende Vorgaben, wie z.B. das Benachteiligungsverbot.

Aus dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) wird i.d.R. der IT-Sicherheitsbeauftragte abgeleitet. Danach müssen Vorstände und Geschäftsleitungen ein für die Aufsichtsgremien und Abschlussprüfer nachvollziehbares Risikomanagement und Überwachungssystem errichten (vgl. z.B. §§ 321 und 322 HGB). Dafür wird dann allgemein der IT-Sicherheitsbeauftragte gebraucht. Explizit benannt ist er in den relevanten Gesetzen (wie Aktiengesetz, HGB usw.) allerdings nicht.

Ein IT-Sicherheitsbeauftragter wird auch nach § 101 (2) TKG gefordert, wenn es sich um TK-Diensteanbieter für die Öffentlichkeit handelt (z.B. die großen Anbieter). Darüber hinaus existiert ein internes Dokument für diejenigen Unternehmen und Behörden, welche in eine erhöhte Geheimhaltungsstufe eingereiht werden. Da die Fragen bereits Aufschluss über die Art der Geheimhaltung geben könnten, ist selbst das Dokument geheim und wird der Öffentlichkeit nicht preisgegeben.

Zu Stellung und Funktion eines IT-Sicherheitsbeauftragten wurde ein Interview in der IT-SICHERHEIT 6/2002, S. 17ff veröffentlicht. Die darin genannte Stellenbeschreibung enthält folgende Aufgabenbereiche:

- Erarbeitung der Sicherheitsziele bei der Informationsverarbeitung
- Kontrolle der Einhaltung der Sicherheitsziele
- Erarbeitung, Pflege, Umsetzung und Steuerung des IT-Sicherheitskonzepts
- Regelmäßige Überprüfung und Aktualisierung des IT-Sicherheitskonzepts und seiner Voraussetzungen
- Beratung und Mitwirkung in allen Fragen der IT-Sicherheit und der IT-Konzeptionsentwicklung
- Schaffung und Aufrechterhaltung des Sicherheitsbewusstseins
- Sensibilisierung des Managements und der Mitarbeiter für Sicherheitsfragen
- Unterstützung der Fachbereiche bei der Umsetzung der IT-Sicherheitskonzeption
- Hilfe bei der Lösung von Konfliktsituationen
- Definition der Kontrollkreisläufe
- Analyse und Audit der IT, Durchführung von Schwachstellen- und Risikoanalyse
- Entwicklung eines Schulungskonzepts und Durchführung von Schulungen
- Zusammenarbeit und Abstimmung mit DV-Revision und DSB
- Regelmäßige Information an den Vorstand zum Stand der IT-Sicherheit
- Analyse der Problemstellung Outsourcing, Problemstellung der Tätigkeit von niedergelassenen Ärzten im Krankenhaus

Diese Auffassung ist die abgestimmte Meinung des GDD-Arbeitskreises „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen“. Im Einzelfall sollte sie juristisch geprüft werden.

gez.: GDD-AK GSW (Bearbeiter Herr Peter Pharow)
06.12.2005