

Managementaufgabe: IT Sicherheit

Grundlagen für ein funktionierendes IT Sicherheitssystem

Sicherheit in der Informatik ist mehr als der Schutz vor dem imaginärem Bösen, vielmehr ist es eine Managementaufgabe die alle Aspekte möglicher unternehmensbedrohender Risiken von IT Systemen im Unternehmen behandelt. Dies hat auch der Gesetzgeber erkannt und nimmt Vorstände und Geschäftsführer in die Pflicht.

Aus der Nutzung von Informationstechnologie entstehen Risiken, die sich in 3 Kategorien gliedern lassen. Dies sind organisatorische, infrastrukturelle sowie anwendungs- und prozessbezogene Risiken.

Dabei sind die Faktoren der Wertbestimmung durch die Grundwerte Authentizität, Integrität, Verfügbarkeit und Vertraulichkeit beschrieben. Diese gilt es, mithilfe eines IT-Risikomanagements, zu schützen.

Neben dem Eigennutzen, den ein Unternehmen von einer funktionierenden IT-Sicherheitsfunktion ableiten kann, sind **gesetzliche Regelungen** für die Notwendigkeit eines IT-Risikomanagements entscheidend. Insbesondere das Bundesdatenschutzgesetz (BDSG) und das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) sind rechtliche Vorgaben, welche in Unternehmen zu beachten sind. Das KonTraG ist ein Artikelgesetz, welches Auswirkungen im Aktiengesetz (AktG) und Handelsgesetzbuch (HGB) findet. Daraus ergibt sich im Wesentlichen die Einführung des § 91 Abs. 2 des AktG. Der eingefügte Absatz lautet:

„Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.“

Diese Vorschrift ist einerseits im Zusammenhang mit § 76 Abs. 1 AktG zu sehen. Hiernach ergeben sich aus der Leitungspflicht für die Vorstandsmitglieder auch Organisationspflichten zur Sicherung des Unternehmensfortbestandes. Andererseits ist zu beachten, dass Verstöße der Unternehmensleitung gegen ihre Verpflichtungen gemäß § 91 Abs. 2 AktG zu einer Schadensersatzverpflichtung gemäß § 93 Abs. 2 AktG führen. Dies bedeutet eine persönliche Haftung der Vorstandsmitglieder gegenüber der Gesellschaft.

Bei der Frage, welche Risiken durch § 91 Abs. 2 AktG adressiert werden, hat der Gesetzgeber die Vorgabe gemacht, dass es sich um solche Entwicklungen handeln muss,

die den Bestand der Gesellschaft gefährden. Das zu schaffende Risikofrüherkennungssystem ist daher auf die Erkennung von Entwicklungen auszurichten, die eine wesentliche Auswirkung auf die Vermögens-, Finanz- oder Ertragslage haben. Als Risikofrüherkennungssystem ist im Einzelnen ein Frühwarnsystem, ein Risikomanagement mit Risikoklassifizierung und Risikoberichtswesen und ein Risiko-Controlling gefordert.

Die Bedeutung des BDSG für die Datensicherheit ergibt sich daraus, dass Datenschutz insbesondere auch durch Datensicherheit gewährleistet werden soll und das Gesetz dazu bestimmte Anforderungen aufstellt.

Werden innerhalb eines Unternehmens erforderliche Maßnahmen zur IT-Sicherheit schuldhaft nicht oder nicht hinreichend getroffen, so droht bei einem dadurch eingetretenen Schaden bei Dritten stets eine entsprechende Schadensersatzverpflichtung. Solche Schadensersatzansprüche ergeben sich dabei entweder aus Verträgen mit dem Dritten oder aus Gesetzen (z.B. §§ 823 ff BGB oder § 7 BDSG).

Unternehmen haben verkehrsrübliche Sorgfaltspflichten einzuhalten, d.h. die im Rahmen der IT-Sicherheit zu treffenden Maßnahmen haben sich insbesondere daran zu orientieren, was von einem Unternehmen der betroffenen Art aus Sicht eines objektiven Dritten zu erwarten ist. Dabei sind insbesondere auch die unternehmensspezifischen Risiken zu berücksichtigen.

Aufgrund des Haftungsrisikos ist die IT-Sicherheit heute Managementaufgabe und muss innerhalb des Unternehmens daher an entsprechend verantwortlicher Stelle im Unternehmen angesiedelt sein.

Die **organisatorische Zuordnung** von IT Sicherheitsbeauftragten ist insbesondere von der Anforderung an Unabhängigkeit zur IT-Funktion eines Unternehmens bestimmt. Sicherheitssteigernde Maßnahmen stehen insbesondere in Bezug auf die Kostensituation oft im Gegensatz zu den Interessen der IT Funktionen. Dort sind finanzielle Mittel insbesondere für die Erweiterung von Informati-

onstechnologie und die Vereinfachung der Verwaltung der IT vorgesehen.

Die **fachliche Kompetenz** eines Verantwortlichen für das Thema IT Sicherheit ist insbesondere durch die spezielle Aufgabe bestimmt. So ist ein IT Sicherheitsbeauftragte immer Mittelsmann zwischen den Interessen des Nutzers, der IT-Funktion und dem Management. Daher sind eine gewisse Praxisnähe, kaufmännische und technische Kenntnisse erforderlich.

Eine Reduzierung von **sicherheitsrelevanten Risiken** innerhalb der IT ist für alle Bedrohungswege anzustreben. Dabei sind auch Telekommunikationswege wie TK-Anlagen, Modem-, ISDN und Wartungszugänge zu beachten. Diese Reduzierung wird dadurch erreicht, indem geeignete Maßnahmen in Abhängigkeit zum Risiko getroffen werden. Die Risikoanalyse ist dabei durch den IT-Sicherheitsbeauftragten zu organisieren. Die Risikoeinschätzung unterliegt dabei jedoch zwangsläufig dem System bzw. Prozesseigner.

Voraussetzung ist die Erstellung einer unternehmensweit gültigen Policy, die aus verschiedenen Richtlinien bestehen, die Benutzung und Management von Informationstechnologie beschreiben. Dabei ist intensiv darauf zu achten, dass diese für jeden Mitarbeiter verständlich ist und rechtlich bindend gemacht wird. Dies kann nur durch Weisung erfolgen. Grundsätzlich ist der Einbezug der Mitarbeiter eine grundlegende Maßnahme die eine so genannte ‚Awareness‘ erzeugen soll. Diese Notwendigkeit wird insbesondere dadurch begründet, dass diversen Studien zu folge der Anteil an erfolgreichen Angriffen auf IT Systeme zu mehr als 50% von aktuellen oder ehemaligen Mitarbeitern, sog. Insidern ausgeht.

Neben dem Aufbau eines IT-Risikomanagements sind **zusätzliche Maßnahmen** denkbar und durchaus realisierbar. So haben insbesondere universitäre Einrichtungen und Finanzdienstleister die Vorreiterrolle bei der Implementierung von ‚Tiger Teams‘ eingenommen. Dies sind aus Experten zusammengesetzte Gruppen, die bei neuen und bestehenden Systemen mit den gleichen Werkzeugen und Tricks, wie Hacker sie anwenden, Schwachstellen aufdecken. Dabei werden technische Möglichkeiten genauso genutzt wie das so genannte ‚Social Engineering‘, welches die Schwachstelle Mensch als Penetrationsmöglichkeit für Systeme ausnutzt.