

# Rechtliche Aspekte der IT-Sicherheit

**Unternehmen investieren jährlich beträchtliche Summen in die Herstellung und Aufrechterhaltung der Sicherheit ihrer IT-Infrastruktur. Welche Anforderungen stellt der Gesetzgeber an die IT-Sicherheit? Und wer ist tatsächlich dafür verantwortlich, dass die gesetzlichen Vorgaben eingehalten werden? Eine pauschale Antwort kann auf diese Fragen nicht gegeben werden.**

mag. iur. Maria Winkler

Die Bedeutung von IT-Sicherheit nimmt in dem Mass zu, in welchem der Wert der Information für die einzelnen Unternehmen und somit für die Wirtschaft steigt. Das Bedürfnis nach Schutz von unternehmensinternen Informationen ist nicht neu, auch im «vor-elektronischen Zeitalter» tätigten Unternehmen grosse Anstrengungen, um ihre Geschäfts- und Betriebsgeheimnisse vor zufälliger oder bewusster Preisgabe an unberechtigte Dritte zu schützen. Dabei bewegten sich die Massnahmen aber in erster Linie auf der organisatorischen Ebene. Man schloss Geheimhaltungsvereinbarungen, bewahrte geheime Dokumente in verschliessbaren Schränken auf etc.

Die technische Entwicklung hat nicht nur die Möglichkeiten der Datenbearbeitung revolutioniert, sondern auch bewirkt, dass der wirtschaftliche Erfolg von Unternehmen unter anderem davon abhängig ist, dass die technische Infrastruktur, mit der sie ihre geschäftsrelevanten Informationen erstellen, bearbeiten und unter Umständen sogar archivieren, korrekt funktioniert. Spricht man heute von IT-Security, dann geht es somit nicht mehr nur um den Schutz von Geschäfts- und Betriebsgeheimnissen sondern um den Schutz aller geschäftsrelevanten Informationen und dies während ihres gesamten

Lebenszyklus. Zudem beschränken sich die dabei erforderlichen Massnahmen nicht mehr nur auf die Abwehr vor unberechtigtem Zugriff oder der Verhinderung von unberechtigter Weitergabe von Informationen.

## Gibt es ein Gesetz über IT-Sicherheit?

Die Komplexität der Aufgabe IT-Sicherheit verlangt nach Vorgaben seitens der Technik aber auch seitens des Gesetzgebers. Während im technischen Bereich zahlreiche Normen existieren (z.B. BS 7799, COBIT etc.), gibt es in der Schweiz kein Gesetz, das den Unternehmen und deren Verantwortlichen abschliessend vorschreibt, welche Massnahmen genau zu treffen sind, um im Bereich der IT-Sicherheit «compliant» zu sein. Vielmehr finden sich in verschiedenen Gesetzen einzelne Bestimmungen, welche direkt oder indirekt die IT-Sicherheit beeinflussen.

Werden, wie dies z.B. in den HR-Abteilungen, in Krankenversicherungen etc. regelmässig der Fall ist, Personendaten bearbeitet, dann finden sich die anwendbaren Normen im Datenschutzgesetz des Bundes. Dieses schreibt vor, dass Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden müssen. In der dazu gehörenden Verordnung werden diese Anforderungen konkretisiert.

Buchführungspflichtige Unternehmen sind gemäss Art. 957 ff. OR und der dazu gehörenden Geschäftsbücherverordnung (GeBüV) verpflichtet, bei einer elektronischen Erstellung, Bearbeitung und Aufbewahrung von Geschäftsdaten die Grundsätze der ordnungsgemässen Datenbearbeitung einzuhalten.

## Die anwendbaren Normen sind oft branchenabhängig

Die genannten Normen des Datenschutzgesetzes und des Obligationenrechts sind nahezu von allen Unternehmen zu beachten. Darüber hinaus existieren für zahlreiche Branchen sowie für die öffentliche Verwaltung häufig Spezialgesetze, welche direkt oder auch indirekt Auswirkungen auf die IT-Sicherheit haben.

Auch ausländische Gesetze, EU-Richtlinien oder internationale Standards, denen sich ein Unternehmen freiwillig unterworfen hat, können die IT-Sicherheit in einem Unternehmen massgeblich beeinflussen. So verlangt der im Jahr 2002 erlassene Sarbanes Oxley Act von Unternehmen, welche an der US-Börse notiert sind, sowie von deren Tochtergesellschaften den Nachweis der Funktionsfähigkeit ihres internen Kontrollsystems für die Finanzberichterstattung. CEO und CFO müssen öffentlich erklären, dass die bekannt gegebenen Finanzdaten richtig sind, und dass die entsprechenden internen Kontrollen funktionieren. Da die in Frage stehenden Finanzdaten mit elektronischen Mitteln erstellt, bearbeitet und oft auch archiviert werden, kommt der IT-Sicherheit besondere Bedeutung zu – nur wenn die technische Infrastruktur richtig funktioniert, sind die bekannt gegebenen Finanzdaten korrekt.

## Einige Empfehlungen

Trotz der Vielfalt der gesetzlichen Grundlagen können einige grundlegende Empfehlungen abgegeben werden, die von allen Unternehmen im Bereich IT-Sicherheit zu beachten sind.

### **Der Geschäftsbereich des Unternehmens prägt die IT-Security-Anforderungen.**

Jedes Unternehmen sollte individuell für den eigenen Geschäftsbereich abklären, ob neben den erwähnten Vorgaben des Datenschutzgesetzes und der Buchfüh-

rungsvorschriften noch Vorschriften in Spezialgesetzen vorhanden sind, welche die IT-Sicherheit beeinflussen.

### **IT-Governance ist nicht die alleinige Aufgabe der IT-Abteilung.**

Der «Swiss Code of Best Practice for Corporate Governance», welcher im Juli 2002 vom Verband der Schweizer Unternehmen Economiesuisse veröffentlicht wurde, konkretisiert die Vorschriften des Obligationenrechts über die Aufgaben und Verantwortung des Verwaltungsrats und der Geschäftsleitung eines Unternehmens. Er verlangt, dass der Verwaltungsrat, mittels auf die Bedürfnisse des Unternehmens abgestimmter interner Kontrollsysteme und einem Risikomanagement, die finanziellen und operativen Risiken abdeckt. Daneben bleibt aber selbstverständlich auch der CIO dafür verantwortlich, dass er seine Aufgaben entsprechend seiner Ausbildung und den ihm zur Verfügung stehenden Informationen gemäss dem aktuellen Stand der Technik erfüllt.

### **IT-Security beginnt mit «sicheren Verträgen».**

Die Beschaffung und der Betrieb der IT-Infrastruktur erfolgt meist in Zusammenarbeit mit Drittunternehmen. Dass in der heutigen hochspezialisierten Arbeitswelt das Outsourcing der gesamten oder zumindest von Teilen der Informatik bereits unverzichtbar ist, kann wohl nicht mehr abgestritten werden. Die Verantwortung für IT-Sicherheit bleibt aber immer beim Unternehmen selbst, was bereits bei der Ausarbeitung der Verträge mit den externen Anbietern zu berücksichtigen ist. Es ist zu empfehlen, in die Verträge Vorgaben über IT-Sicherheitsmassnahmen und Kontrollmechanismen zur Überprüfung der Einhaltung dieser Vorgaben zu integrieren.

### **Die eingesetzten IT-Systeme sollen nur können, was das Unternehmen darf.**

Sämtliche Investitionen in die technische Sicherheit der IT-Infrastruktur sind vergebens, wenn sich schlussendlich herausstellt, dass die damit mögliche und vorgesehene Bearbeitung der Daten unzulässig ist. Erlaubt z. B. eine Personaladministrationslösung die Aufbewahrung von Unterlagen von Stellenbewerbern über Jahre hinaus, dann kann dies für die zu-

ständige Personalabteilung unter Umständen durchaus praktisch sein. Da gemäss Art. 4 Datenschutzgesetz (DSG) Daten nur zu dem Zweck bearbeitet werden dürfen, zu dem sie erhoben wurden, müssen aber Unternehmen die Daten, welche sie von einem Bewerber zum Zweck des Abschlusses eines Arbeitsvertrages erhalten, wieder retournieren oder löschen, wenn kein Anstellungsverhältnis zustande kommt.

### **Die gewählten Massnahmen müssen angemessen sein.**

Es ist zu empfehlen, die bearbeiteten Daten nach ihrem Schutzbedarf zu kategorisieren und die Massnahmen entsprechend zu wählen. Je sensibler die zu schützenden Daten sind, umso sorgfältiger ist darauf zu achten, dass die IT-Sicherheit im Unternehmen dem aktuellen Stand der Technik und anerkannten nationalen und internationalen Standards entspricht.

## IT-Sicherheit ist Teil der Corporate Governance

Wegen der immensen Bedeutung welche heute das richtige Funktionieren der IT-Infrastruktur für die meisten Unternehmen hat, ist dem korrekten Funktionieren der IT-Systeme im Rahmen eines umfassenden Risikomanagements ausreichend Beachtung zu schenken.

So haben der Verwaltungsrat und die Geschäftsleitung sicherzustellen, dass

- zur Erfüllung der IT-Sicherheitsaufgaben ausreichend ausgebildetes Personal eingesetzt wird, welches Zugang zu allen entscheidungsrelevanten Informationen hat;
- Verantwortlichkeiten und Kompetenzen klar zugewiesen werden;
- die mit dem Einsatz von Informationstechnologien im Unternehmen verbundenen Risiken identifiziert und Massnahmen zu deren Ausschaltung oder Reduzierung ergriffen werden;
- dafür genügend Budget zur Verfügung gestellt wird;
- durch ein funktionierendes internes Kontrollsystem sichergestellt wird, dass interne Weisungen, Regeln der Technik und nationale sowie relevante internationale Normen eingehalten werden (Compliance). ■