

Informationssicherheit – auch rechtlich eine Notwendigkeit

Dr. Ursula Widmer, Rechtsanwältin, Bern

ursula.widmer@widmerpartners-lawyers.ch

Der Ausfall der Informations- und Kommunikationsinfrastruktur kann für Unternehmen, Behörden und Private gravierende Folgen haben. Der Schutz unternehmenskritischer Informationen hat hohe Priorität. Der folgende Beitrag zeigt die rechtlichen Grundlagen auf, welche die Risikoprävention im Bereich der Informationssicherheit zu einer der zentralen Aufgaben im Verantwortungsbereich der Entscheidungsträger in Wirtschaft und Verwaltung machen.

Mit der Verbreitung moderner Informationstechnologien hat für Unternehmen, Behörden und Private die Abhängigkeit von Informationen zugenommen. Massnahmen zum Schutz von Informationen haben deshalb einen hohen Stellenwert.

Informations- und Kommunikationssysteme werden von aussen etwa durch Virentacken, Hacking oder Denial of Service Attacken bedroht. Aber auch Angriffe von innen, wie Datendiebstahl und -sabotage durch Mitarbeiter oder durch Softwarefehler verursachte Störungen und Schäden, stellen eine Gefahr für die Sicherheit der Information dar. Ausserdem bringt die Abhängigkeit von Dritten (etwa bei der Beschaffung von Informationssystemen, bei deren Wartung oder bei der Telekommunikation) Risiken für die Informationssicherheit mit sich. Störungen oder der Ausfall von Informationssystemen können unternehmensbedrohende Auswirkungen haben. Mögliche Folgen sind die Manipulation oder Zerstörung von Daten, die Offenlegung von Geheimnissen (Geschäfts-, Amts-, Berufsgeheimnisse) oder die Lahmlegung unternehmenswichtiger Infrastrukturen. Daraus können Vermögens-, Sach- und Personenschäden, aber auch Vertrauensschäden (Imageverlust) mit bedeutenden wirtschaftlichen Ausmassen, resultieren.

Wegen der weit reichenden Konsequenzen möglicher Störungen der Informations- und Kommunikationsinfrastruktur ist die Wahrung der Informationssicherheit eine Managementaufgabe. Sie stellt ein wesentliches Element der Führungsverantwortung dar, welche die Entscheidungsträger in Unternehmen und Verwaltung wahrzunehmen haben. Eine Vernachlässigung dieser Verantwortung kann zur Haftung für die daraus resultierenden Schäden führen.

Rechtliche Rahmenbedingungen: Anspruchsnormen

Die Verpflichtung, Massnahmen der Informationssicherheit zu treffen, ergibt sich aus zahlreichen gesetzlichen Bestimmungen.

Datenschutz

Für die Bearbeitung von Personendaten durch private Unternehmen und Behörden schreiben die Datenschutzgesetze des Bundes und vieler Kantone vor, dass technische und organisatorische Massnahmen zur Datensicherheit getroffen werden müssen. In der Datenschutzverordnung des Bundes wird festgelegt, dass für die Vertraulichkeit, die Verfügbarkeit und die Richtigkeit der bearbeiteten Daten zu sorgen ist. Es sind insbesondere Schutzmassnahmen gegen die unbefugte oder zufällige Vernichtung, den zufälligen Verlust, technische Fehler, die widerrechtliche Verwendung oder die unbefugte Bearbeitung von Daten zu treffen. In den gesetzlichen Datenschutzbestimmungen werden allerdings keine konkreten, technischen und organisatorischen Massnahmen zur Wahrung der Datensicherheit festgelegt. Es wird diesbezüglich auf den jeweiligen Stand der Technik und die Angemessenheit entsprechend dem Risikopotential verwiesen.

Geheimhaltungspflichten

Pflichten in Bezug auf die Informationssicherheit ergeben sich auch aus den Bestimmungen betreffend das Geschäfts-, Amts-, Berufs- und Fernmeldegeheimnis. Für die Daten, die unter die genannten Geheimhaltungsnormen fallen, ist die Vertraulichkeit sicherzustellen.

Die geheim zu haltenden Daten sind daher zum Beispiel gegen den Zugang durch unbefugte Personen zu schützen und bei der Übermittlung via offene Netzwerke zu verschlüsseln.

Buchführungsvorschriften

Für Unternehmen sind weiter die Bestimmungen über die kaufmännische Buchführung relevant. Die Geschäftsunterlagen, die während zehn Jahren aufbewahrt werden müssen, dürfen zum grössten Teil auch in elektronischer Form geführt und aufbewahrt werden. In der Geschäftsbücherverordnung sind die für die elektronische Buchführung massgeblichen Grundsätze festgehalten. Sichertgestellt werden müssen insbesondere die Verfügbarkeit und die Integrität der Geschäftsdaten während der gesamten Aufbewahrungsdauer. Ohne entsprechende Massnahmen zur Informationssicherheit dürfen die Geschäftsunterlagen dagegen nicht in elektronischer Form aufbewahrt werden.

Vertragliche Lieferpflichten

Massnahmen der Informationssicherheit sind auch im Hinblick auf die Sicherstellung der Lieferfähigkeit gegenüber Kunden und Leistungsbezügern zu treffen. Wird die Erfüllung von Liefer- und Leistungspflichten durch eine Störung oder den Ausfall der Informations- und Kommunikationssysteme verunmöglicht (z.B. weil Informationen über laufende Bestellungen oder Verträge verloren gehen oder der Betrieb von Produktions- und Verteilanlagen unterbrochen ist oder beim Ausfall von Versorgungssystemen wie die Strom- oder Telekommunikationsnetze), kann dies wegen der nicht erbrachten und daher nicht verrechenbaren Leistungen einerseits zu erheblichen Einnahmeausfällen führen, andererseits aber zusätzlich Schadenersatzansprüche der betroffenen Kunden und Leistungsbezügler zur Folge haben.

Falls grundlegende Massnahmen der Risikoprävention unterlassen worden sind, haftet ein Unternehmen im übrigen auch dann, wenn es die Haftung für Schäden aus solchen Ereignissen in den Vertragsbedingungen mit den Kunden ausgeschlossen hat. Denn ein Haftungsausschluss für grobfahrlässige Verhaltensweisen ist nach schweizerischem Vertragsrecht ungültig.

Zu berücksichtigen ist seitens der Unternehmen zudem, dass sie auch für das Verhalten der von ihnen eingesetzten Hilfspersonen (z.B. Informatikunternehmen für Support/Wartung von Systemen, Outsourcingpartner, Telekommunikationsunternehmen) haften.

Öffentliches Organisationsrecht

Behörden sind generell für die Sicherheit der eigenen Informations- und Kommunikationsinfrastruktur verantwortlich. Die Bundesinformatikverordnung schreibt für Bundesbehörden je nach Sensitivität der Daten und dem damit verbundenen Risikopotential abgestufte Schutzmassnahmen in Bezug auf die Vertraulichkeit, Verfügbarkeit, Integrität und Nachweisbarkeit von Informatikmitteln und Daten vor. Die exakten diesbezüglichen Anforderungen an die Schutzmassnahmen sind von spezialisierten Gremien des Bundes in Weisungen und Handbüchern festgehalten worden.

Sicherstellung der Landesversorgung

Das Bundesgesetz über die wirtschaftliche Landesversorgung regelt beispielsweise die Massnahmen des Bundes zur Sicherstellung der Landesversorgung mit lebenswichtigen Dienstleistungen bei schweren Mangellagen, denen die Wirtschaft nicht aus eigener Kraft zu begegnen vermag. Die Fernmeldedienste gehören zu diesen lebenswichtigen Dienstleistungen. Der Bund ist danach verpflichtet, präventiv Massnahmen zur Sicherung ausreichender Kommunikationsmöglichkeiten zu treffen. Zur Sicherstellung der Kommunikation in ausserordentlichen Lagen kann der Bundesrat die Fernmeldedienstleister zudem zur Erbringung von Leistungen verpflichten.

Branchenspezifische Vorschriften

Pflichten zur Informationssicherung ergeben sich aus branchenspezifischen Anforderungen und spezialgesetzlichen Regelungen. Für das Gesundheitswesen gelten zahlreiche Bestimmungen auf Bundes- und kantonaler Ebene, welche die Pflicht zur Aufzeichnungen und Aufbewahrung von Daten während Fristen von 10-20 Jahren vorsehen (z.B. Krankengeschichten, Daten im Zusammenhang mit Strahlentherapien, Transplantationen, Entnahme und Verabreichung von Blut etc.).

Ohne angemessene Massnahmen der Informationssicherheit können diese Pflichten nicht erfüllt werden.

Persönliche Verantwortlichkeit der Entscheidungsträger

Werden die rechtlich geforderten Massnahmen zur Wahrung der Informationssicherheit unterlassen oder nicht ordnungsgemäss durchgeführt und resultiert daraus eine Schädigung Dritter, wie z.B. von Kunden oder Bezüger öffentlicher Leistungen, hat dies regelmässig die Haftung des betreffenden Unternehmens oder der betreffenden Behörde zur Folge.

Es können aber auch die verantwortlichen Entscheidungsträger persönlich für die Schäden haftbar gemacht werden, die einem Unternehmen oder einer Behörde wegen mangelnder Informationssicherheit direkt oder aufgrund der Haftung gegenüber Dritten entstehen. Für Aktiengesellschaften beispielsweise gilt, dass die Mitglieder des Verwaltungsrates und der Geschäftsleitung generell für den Schaden verantwortlich sind, den sie durch absichtliche oder fahrlässige Verletzung ihrer Pflichten verursachen. Unterlassen daher diese verantwortlichen Entscheidungsträger die ihnen obliegende Pflicht, für angemessene Massnahmen zur Wahrung der Informationssicherheit zu sorgen, haften sie gegenüber der Gesellschaft mit ihrem privaten Vermögen für allfällige Schäden aufgrund dieser Unterlassung.

Ist die Informations- und Kommunikationsinfrastruktur für wesentliche Unternehmensfunktionen von Bedeutung, was regelmässig der Fall ist, so stellt die Wahrung der Informationssicherheit eine Aufgabe der zwingend vom Verwaltungsrat zu erfüllenden Oberleitung der Gesellschaft dar. Eine vollständige Delegation der Verantwortung für die Informationssicherheit auf untergeordnete Stufen der Unternehmensorganisation ist daher ausgeschlossen. Möglich ist nur die Delegation von Teilaufgaben in einem den jeweiligen Umständen angepassten Umfang. Für GmbHs, Genossenschaften, Stiftungen oder Vereine gelten ähnliche Haftungsregeln wie für die Aktiengesellschaft.

Auch die Entscheidungsträger in der Verwaltung haben ein persönliches Haftungsrisiko. Kommt es nämlich wegen der Verletzung der Pflichten bezüglich der Informationssicherheit zu einer Haftung des Staates gegenüber Dritten (etwa weil wegen ungenügender Massnahmen zur Wahrung der Vertraulichkeit von Daten Amtsgeheimnisse verletzt werden) kann auf den verantwortlichen Beamten Rückgriff genommen werden. Dieser haftet in der Regel dann persönlich, wenn er durch vorsätzliche oder grobfahrlässige Verletzung seiner Dienstpflichten die Ersatzpflicht des Staates gegenüber geschädigten Dritten verursacht hat.

Massgeblichkeit von Standards

Es stellt sich die Frage, welche konkreten Massnahmen zur Informationssicherheit getroffen werden müssen, um die erwähnten Haftungsrisiken auszuschliessen oder zu minimieren. Die gesetzlichen Bestimmungen, aus denen sich die Pflicht zur Wahrung der Informationssicherheit ableitet, schreiben keine konkreten technischen, organisatorischen und rechtlichen Massnahmen vor. Zu beachten sind daher die Standards, welche sich in der Praxis bezüglich der Informationssicherheit und der damit verbundenen technischen und organisatorischen Aspekte etabliert haben.

In Bezug auf organisatorische Massnahmen und das Management von Risiken betreffend die Informationssicherheit hat sich der British Standard „Information Security Management System“ (BS 7799), der inzwischen in einen ISO/IEC-Standard (ISO/IEC 17799: Code of Practice for Information Security Management) eingeflossen ist, durchgesetzt. Von Bedeutung sind in diesem Zusammenhang auch die Control Objectives for Information and related Technology (Cobit) und der ISO/IEC-Standard „Evaluation Criteria for IT Security“ (ISO/IEC 15408, Common Criteria). Im deutschsprachigen Raum hat das IT-Grundschutzhandbuch des deutschen Bundesamtes für Sicherheit in der Informationstechnik allgemeine Bedeutung erlangt. Für die Bundesverwaltung sind die Weisungen und Handbücher des Informatikstrategieorgans Bund (ISB) zu beachten. Daneben existieren weitere sektor- und branchenspezifische Standards.

Risikomanagement: Schadens- und Haftungsprävention

Um ihre Verantwortung im Zusammenhang mit der Wahrung der Informationssicherheit wahrzunehmen, ist durch die Entscheidungsträger in Wirtschaft und Verwaltung insbesondere Folgendes vorzukehren:

Technische und organisatorische Massnahmen

Als Basis für die Evaluation sinnvoller Massnahmen zur Informationssicherheit ist zuerst eine Analyse durchzuführen, über welche Informationen sowie Infrastrukturen zur Informationsverarbeitung ein Unternehmen oder eine Organisation verfügt, welchen Störungs- und Ausfallrisiken in Frage kommen und wie diese Risiken zu bewerten sind. Aufgrund einer solchen Risikoanalyse müssen die nötigen technischen, organisatorischen und rechtlichen Massnahmen zur Informationssicherung definiert und die entsprechenden Aufträge zur Umsetzung erteilt werden. Die Bereitstellung der hierzu notwendigen Ressourcen in personeller und finanzieller Hinsicht sowie der notwendigen Infrastrukturen ist sicherzustellen. Die Umsetzung der Massnahmen ist zu überwachen und soweit erforderlich ist korrigierend einzugreifen. Schliesslich ist der Stand der Informationssicherheit in regelmässigen Abständen überprüfen und gegebenenfalls sind erforderliche Anpassungen vorzunehmen bzw. anzuordnen.

Rechtliche Massnahmen

Die Informationssysteme von Unternehmen und Organisationen sind regelmässig abhängig von Leistungen Dritter wie Software- und Hardwarelieferanten oder Telekommunikationsunternehmen. Mittels entsprechender vertraglicher Vereinbarungen sind gegenüber diesen Dritten und für die von diesen zu erbringenden Leistungen die Anforderungen bezüglich der Informationssicherheit verbindlich vorzugeben. So ist in den Verträge mit diesen Lieferanten beispielsweise eine klar definierte Leistungsumschreibung (z.B. bezüglich der Leistungsfähigkeit und Verfügbarkeit von Systemen, der Qualifikation des eingesetzten Personals, der Reaktions- und Behebungszeiten bei auftretenden Störungen), eine verbindliche Terminplanung sowie eine detaillierte Regelung der Verantwortungen, verbunden mit entsprechenden Sanktionen, vorzusehen.

Mittels eines qualifizierten Vertragsmanagements muss sichergestellt werden, dass alle für die Informationssicherheit relevanten Leistungen von Dritten vertraglich korrekt abgesichert werden. Dazu müssen die betroffenen ICT-Projekte möglichst frühzeitig durch eine professionelle Rechtsberatung begleitet werden. Bereits abgeschlossene Verträge sind, z.B. im Zusammenhang mit Verhandlungen über Wartungsleistungen, zu überprüfen und im Rahmen von Nachverhandlungen allenfalls notwendige Korrekturen vorzunehmen.

Ebenfalls durch vertragliche Vereinbarungen zu beschränken ist das Haftungsrisiko von Unternehmen gegenüber ihren Kunden. So ist etwa die Haftung für Schäden im Zusammenhang mit dem Ausfall von Informationssystemen, die das betreffende Unternehmen nicht zu vertreten hat, in den Verträgen mit Kunden wegzubedingen oder zu limitieren.

Für verbleibende Restrisiken, die weder durch technische, organisatorische noch rechtliche Massnahmen ausgeschlossen werden können, ist, soweit möglich und betriebswirtschaftlich sinnvoll, die Deckung durch eine Versicherung vorzusehen.

Fazit

Wegen der grossen Bedeutung der Ressource Information ist der Schutz unternehmenskritischer Informationen eine Managementaufgabe. Die Entscheidungsträger in Wirtschaft und Verwaltung sind verantwortlich für die Durchführung entsprechender Risikoanalysen, die Definition von technischen, organisatorischen und rechtlichen Massnahmen zur Risikominimierung, die Kontrolle deren Umsetzung und die Versicherung von Restrisiken. Wird diese Verantwortung nicht hinreichend wahrgenommen, können Unternehmen, Behörden und deren Entscheidungsträger, in einem Schadensfall haftbar gemacht werden.

Dr. Ursula Widmer ist Rechtsanwältin in Bern. Ihre Kanzlei, Dr. Widmer & Partner, ist spezialisiert auf Fragen des Informatik-, Internet-, E-Business und Telekommunikationsrechts.

