Die Haftung der Geschäftsführung bei Cyber-Angriffen

Dr. Jan Kraayvanger,
Partner/Rechtsanwalt,
Mayer Brown LLP

Unternehmen sind einer Vielzahl von Cyber-Risiken ausgesetzt, z.B. Phishing-E-Mails, Ransomware, DDoS-Attacken, Fake President- und Man-in-the Middle-Angiffen, etc. Im Falle eines Cyber-Angriffs drohen enorme, unter Umständen sogar bestandsgefährdende Schäden. Die Cyber-Sicherheit gehört daher zu den Kernaufgaben der Geschäftsleitung. IT-Sicherheit ist „Chefsache". Im Ausgangspunkt lässt sich der Pflichtenkreis der Geschäftsführung einteilen in einerseits Organisations- und Überwachungspflichten zum Schutz der IT-Systeme im Vorfeld von Cyber-Angriffen (Schadensprävention) und andererseits die pflichtgemäße Reaktion auf einen erfolgten Cyber-Angriff. Zur letzteren zählen etwa die Einhaltung von Meldepflichten an Behörden, Versicherer und betroffene Datensubjekte sowie von Schadensaufklärungs- und Schadensminderungspflichten. Um hierfür im Falle eines Cyber-Angriffs gerüstet zu sein, sollte ein Notfallkonzept (sog. Incident Response Plan) ausgearbeitet und implementiert werden.

Die Pflichten des Unternehmens und seiner Geschäftsleitung im Zusammenhang mit der IT-Sicherheit sind gesetzlich nicht zentral geregelt. Stattdessen ergeben sie sich aus unterschiedlichen Regelwerken und Normen. So existieren Sondervorschriften etwa für Betreiber sog. Kritischer Infrastrukturen, Telekommunikationsunternehmen, Kreditinstitute, Versicherer und Betreiber von Handelssystemen. Zentrale Bedeutung für sämtliche personenbezogene Daten verarbeitende Unternehmen hat die Datenschutzgrundverordnung. Gemäß Art. 5 Abs. 1 f) DSGVO müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der Daten gewährleistet. Dies beinhaltet den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor Verlust, Zerstörung und Schädigung. Demgemäß sind geeignete technische und organisatorische Maßnahmen zu treffen, um ein angemessenes Schutzniveau für personenbezogene Daten zu gewährleisten (Art. 32 Abs. 1 DSGVO). Hierzu zählt insbesondere die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen nach einem Cyber-Angriff rasch wiederherzustellen (Art. 32 Abs. 1 c) DSGVO). Im Falle eines Datenlecks bestehen zudem kurzfristige Meldepflichten an die Aufsichtsbehörde sowie die betroffenen Personen (Art. 33 und 34 DSGVO). Außerdem besteht gegenüber der Aufsichtsbehörde eine Dokumentationspflicht im Hinblick auf Datenschutzverletzungen, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen (Art. 33 Abs. 5 DSGVO). Bei Verstoß gegen diese Pflichten drohen Schadenersatzforderungen (Art. 82 DSGVO) und hohe Bußgelder (Art. 83 DSGVO).

Darüber hinaus ist die Geschäftsleitung nach § 91 Abs. 2 AktG (analog) gehalten, geeignete Maßnahmen zu treffen, damit Entwicklungen früh erkannt werden, die den Fortbestand der Gesellschaft gefährden. Mit dem Begriff der Bestandsgefährdung sind wesentliche Auswirkungen auf die Vermögens-, Ertrags- oder Finanzlage erfasst. Hieraus wird die Verpflichtung der Geschäftsleitung abgeleitet, eine „auf Schadensprävention und Risikokontrolle angelegte Compliance-Organisation" (LG München, Urteil vom 10.12.2013, Az. 5 HKO 1387/10, LS 1) einzurichten. Die Geschäftsleitung hat im Rahmen ihrer Legalitätspflicht dafür Sorge zu tragen, dass das Unternehmen so organisiert und beaufsichtigt wird, dass keine Gesetzesverstöße erfolgen und dass das Unternehmen jederzeit in der Lage ist, die vorbeschriebenen Pflichten – im vorliegenden Zusammenhang also insbesondere die Pflichten aus der DSGVO – einzuhalten.

Darüber hinaus ist in den meisten Fällen die Funktionsfähigkeit der IT-Systeme für die Aufrechterhaltung des Geschäftsbetriebs des Unternehmens erforderlich. Es besteht also eine doppelte Anknüpfung, warum die IT-Sicherheit Kernaufgabe der Geschäftsleitung ist. Zum einen, weil die Funktionsfähigkeit des IT-Systems als ein betriebsnotwendiger Bestandteil des Unternehmens geschützt werden muss, und zum anderen, weil die Geschäftsleitung aus ihrer Legalitätspflicht heraus sicherstellen muss, dass das Unternehmen die DSGVO und ggf. anwendbare IT-Spezialgesetze einhält.

Die Organisationspflichten zum Schutz der IT-Systeme obliegen dabei nicht nur dem für die IT-Sicherheit unmittelbar zuständigen Mitglied der Geschäftsleitung, sondern allen Geschäftsführern gemeinsam. Es besteht eine Gesamtverantwortung der Geschäftsleitung. Die Geschäftsleitung als Kollegialorgan muss die grundsätzlichen Entscheidungen treffen, welche Vorkehrungen und Maßnahmen zum Schutz der IT-Systeme zu ergreifen sind. Dies schließt nicht aus, dass die Zuständigkeit für die IT-Sicherheit einem bestimmten Mitglied der Geschäftsleitung übertragen wird. Bei den restlichen Mitgliedern der Geschäftsleitung verbleibt jedoch eine Kontroll- und Überwachungsverantwortung. Erforderlich ist daher, dass sich das Gesamtgremium regelmäßig vom ressortzuständigen Geschäftsführer berichten lässt und ggf. gezielte Nachfragen stellt, um sich ein eigenes Bild über den Geschäftsbereich machen zu können.

Bei der konkreten Ausgestaltung der IT-Compliance handelt es sich um eine unternehmerische Entscheidung. Aufgrund der Unterschiedlichkeit der Unternehmen ist deren jeweiliges individuelles Risikoprofil ausschlaggebend, so dass generalisierende gesetzliche Vorgaben praktisch nicht sinnvoll wären. Folglich kommt der Geschäftsleitung die Haftungserleichterung der Business Judgment Rule zugute. Sind deren Voraussetzungen erfüllt, scheidet eine Pflichtverletzung aufgrund des weiten unternehmerischen Ermessensspielraums aus. Demnach liegt eine Pflichtverletzung nicht vor, wenn die Geschäftsleitung vernünftigerweise annehmen durfte, auf der Grundlage angemessener Information zum Wohle der Gesellschaft zu handeln (§ 93 Abs. 1 S. 2 AktG). Zusätzlich sollte die Geschäftsleitung auf eine ausreichende Dokumentation ihrer Entscheidungsfindung achten. Eine fehlende Dokumentation erschwert den Geschäftsführern nicht nur den Entlastungsbeweis im Falle ihrer Inanspruchnahme, sondern stellt für sich selbst bereits eine Verletzung der Geschäftsleiterpflichten dar.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat Handlungsempfehlungen herausgegeben, die beim Aufbau eines angemessenen und effizienten Managementsystems für IT-Sicherheit sowie eines Notfallkonzeptes helfen können. Darin sind unter anderem Management-Prinzipien und Sicherheitsprozesse beschrieben. Diese Leitlinien, die sog. „BSI-Standards“, sind auf der Homepage des BSI unter www.bsi.bund.de abrufbar (BSI-Standards 200-1, 200-2, 200-3, 100-4 bzw. zukünftig 200-4). Ebenfalls auf der Homepage des BSI findet man das sog. IT-Grundschutz-Kompendium, welches auf über 800 Seiten sehr detailliert eine Vielzahl von Bedrohungsszenarien beschreibt und für alle Unternehmensbereiche aufzeigt, mit welchen konkreten Sicherheitsmaßnahmen den dort jeweils bestehenden Gefährdungslagen begegnet werden kann. Diese Leitlinien des BSI orientieren sich an der ISO-Norm 27001. Hierbei handelt es sich um eine internationale Norm zum Management von Informationssicherheit. Die Norm macht Vorgaben zur Einführung, zum Betrieb und zur Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems.

In einem Anhang werden mehr als 100 Maßnahmen aufgeführt, aus denen unter Berücksichtigung der relevanten Risiken ausgewählt werden kann. Es besteht zudem die Möglichkeit, sich die Einhaltung dieser Grundsätze zertifizieren zu lassen. Die Geschäftsleitung kann sich dann im Schadenfall damit verteidigen, ein ISO-zertifiziertes IT-Compliance-System etabliert zu haben. Zudem kann die Zertifizierung auch gegenüber Vertragspartnern als Nachweis genutzt werden, dass ein effektives IT-Compliance-System implementiert ist.

Weiterhin sollte die Geschäftsleitung im Rahmen des Risiko-Managements die Option prüfen, eine Cyber-Versicherung abzuschließen. Sie kann sinnvoll sein, um das Schadensrisiko im Rahmen der Deckung auf einen Versicherer zu transferieren. Zum anderen bieten Cyber-Policen umfangreiche Assistance-Leistungen und Zugang zu einem Experten-Netzwerk, auf die das Unternehmen im Falle eines Cyber-Angriffs zugreifen kann. Jedoch gewährt eine solche Versicherung keinen Rundumschutz. Schon gar nicht stellt sie einen Ersatz für ein effektives IT-Compliance-System dar. Eine Cyber-Versicherung schützt die Geschäftsleitung im Falle eines Verstoßes gegen ihre Compliance-Pflichten nur bedingt, selbst wenn die Organe mitversichert sind. So sind die Innenhaftungsansprüche der Gesellschaft gegen die Geschäftsleitung unter den AVB Cyber ausdrücklich von der Deckung ausgenommen (Ziff. A3-7.2a) AVB Cyber). Zudem ist möglich, dass der Cyber-Versicherer die Geschäftsleitung nach § 86 Abs. 1 VVG in Regress nehmen kann, wenn er nach einem erfolgten Cyber-Angriff den Schaden des Unternehmens reguliert hat. Da im Falle eines Cyber-Angriffs die Cyberkriminellen regelmäßig nicht ermittelbar bzw. greifbar sind und Mitarbeiter, die etwa durch fahrlässiges Verhalten den Cyber-Angriff erst ermöglicht haben, den Schutz des Arbeitnehmerprivilegs genießen, bleibt als einziger Haftungsschuldner die Geschäftsleitung übrig.

Auch eine eventuell vorhandene D&O-Versicherung sollte die Geschäftsleitung nicht in falscher Sicherheit wiegen. Denn D&O-Versicherungen enthalten oftmals gerade für Schäden aufgrund eines Cyber-Angriffs Deckungsausschlüsse. Diese haben zur Folge, dass die Geschäftsleitung schon bei leichter Fahrlässigkeit mit ihrem vollen Privatvermögen haftet, wenn ihr nicht der Nachweis gelingt, sämtliche Organisationspflichten zur Errichtung und Unterhaltung eines effektiven IT-Compliance-Systems eingehalten zu haben und auf den Cyber-Angriff pflichtgemäß reagiert zu haben. Eine intensive Beschäftigung der Geschäftsleitung mit dem Thema IT-Sicherheit und deren lückenlose Dokumentation sind daher unverzichtbar, um deren Haftungsrisiko zu minimieren. ■