von Rechtsanwalt **Max-Lion Keller**, LL.M. (IT-Recht)

Wer haftet für die IT-Sicherheit?

Das Thema "IT-Sicherheit" betrifft keineswegs nur Computer-Spezialisten, sondern hat absolute unternehmerische Relevanz. Unternehmen, die der IT-Sicherheit nur wenig Beachtung schenken, handeln grob fahrlässig und werden mittlerweile auch seitens der Gerichte als schlicht "blauäugig" bezeichnet. Rechtsanwalt Max-Lion Keller erläutert anhand eines Falls, den das Oberlandesgericht (OLG) Hamm im Jahr 2003 zu entscheiden hatte, welche rechtlichen Konsequenzen sich aus einer derartigen Blauäugigkeit für ein Unternehmen ergeben.

Ein Reiseunternehmen hatte Probleme mit seinem Server und beauftragte einen Computer-Reparaturdienst, nach dem Grund für eine bestimmte Fehlermeldung zu suchen. Der Mitarbeiter des Reparaturdienstes wollte daraufhin eine Festplatte austauschen und erkundigte sich vorher, ob die betreffenden Daten gesichert seien. Dies bejahte das Reiseunternehmen und es kam, wie es kommen musste: Bei der Vorbereitung des Festplattenaustausches kam es zu einem Absturz des Servers mit der Folge, dass zahlreiche Geschäftsdaten gelöscht wurden.

Das Reiseunternehmen hatte seine Daten noch nicht einmal monatlich gesichert, so dass Teile der Daten tatsächlich unwiederbringlich gelöscht waren. Das Reisebüro verklagte nun den Reparaturdienst auf Zahlung von Schadensersatz mit der Begründung, dass der Dienstleister bei den Arbeiten an der Festplatte nicht sachgemäß vorgegangen sei und dabei das System zerstört oder beschädigt habe. Es sei jedenfalls nicht genügend Sorge für eine hinreichende Datensicherung vor diesen Arbeiten getragen worden. Dazu sei der Reparaturdienst aber verpflichtet gewesen. Das Gericht hatte nun zu entscheiden, in wessen Verantwortungsbereich die Datensicherung fällt.

Bei mangelnder Datensicherung selbst schuld

Das OLG Hamm fand in seinem **Urteil vom 1. Dezember 2003 (Az:13 U 133/03)** deutliche Worte: Es legte dem Reiseunternehmen zur Last, dass dieses nicht für eine zuverlässige Sicherheitsroutine gesorgt, sondern diese vielmehr grob vernachlässigt habe. So habe der nach dem Absturz festgestellte Stand der Komplettsicherung dem Stand vier Monate vor den Wartungsarbeiten entsprochen! Dies sei "grob fahrlässig, ja blauäugig", so das OLG Hamm. Schließlich habe eine Sicherung der Unternehmensdaten "täglich zu erfolgen, eine Vollsicherung mindestens einmal wöchentlich." Das Gericht legte noch nach: Selbst wenn dem Mitarbeiter des Reparaturdienstes eine Pflichtverletzung im Sinne der Wahrnehmung seiner Controllerpflichten vorzuwerfen wäre, bliebe es dabei, dass dem Reiseunternehmen eine Alleinschuld am entstanden Datenverlust und damit am finanziellen Schaden vorzuwerfen wäre.

Haftung der Beteiligten

Die nun schon vielfach zitierte "Blauäugigkeit" kann für den jeweiligen IT-Verantwortlichen in einem Unternehmen und unter Umständen auch für die Geschäftsleitung gravierende Folgen haben: So ist die Geschäftsleitung nach dem am 27. April 1998 in Kraft getretenen Kontroll- und Transparenzgesetz (KonTraG) verpflichtet, ein System zur frühzeitigen Erkennung von den Fortbestand des Unternehmens bedrohenden Entwicklungen und Risiken zu implementieren. Schenkt die Geschäftsleitung der Gefahr einer fehlenden Datensicherung keine Beachtung, so ist in Anbetracht der zu erwartenden Schäden, die sogar eine Insolvenz des Unternehmens auslösen können, auch deren Verhalten als grob fahrlässig zu bezeichnen.

Natürlich kann sich auch der unmittelbare IT-Verantwortliche aus dem Arbeits- bzw. Anstellungsvertrag haftbar machen. Es muss heutzutage zudem jedem klar sein, dass Pflichtverletzungen im Bereich der IT-Sicherheit arbeitsrechtliche Abmahnungen und im Wiederholungsfall gar Kündigungsfolgen nach sich ziehen können.

Ähnlich stellt sich die Problematik bei externen bzw. freien Mitarbeitern dar, die in aller Regel in einem Dienst- oder auch Werkvertragsverhältnis zu ihren Auftraggebern stehen. Abhängig von der jeweiligen Vertragsausgestaltung können hier grobe sicherheitsrelevante Verfehlungen schnell zur sofortigen wie auch entschädigungslosen Auflösung des Vertrages führen. Darüber hinaus kommen natürlich auch Schadensersatzansprüche des Auftraggebers in Betracht.

Bei unzureichenden Datensicherungsmaßnahmen spielt es übrigens keine Rolle, wie dilettantisch etwaige Wartungsarbeiten vorgenommen werden. Das Risiko des Datenverlusts tragen in diesen Fällen ausschließlich die Unternehmen bzw. die jeweiligen Verantwortlichen.

Auch GmbH-Geschäftsführer persönlich haftbar

Im Aktiengesetz ist festgelegt, dass eine persönliche Haftung des Vorstand dann in Betracht kommt, wenn er Entwicklungen, die zukünftig ein Risiko für das Unternehmen darstellen könnten, nicht durch ein Risikomanagement überwacht und durch geeignete Maßnahmen vorbeugt (§ 91 Abs. 2 und § 93 Abs. 2 AktG). Nahezu dieselben Anforderungen gelten:

- Für den Geschäftsführer einer GmbH, der die "Sorgfalt eines ordentlichen Geschäftsmannes" aufzubringen hat (§ 43 Abs. 1 GmbHG). Diese, zugegebenermaßen eher allgemein gehaltene, Formulierung beinhaltet in der rechtlichen Praxis ganz ähnliche Folgerungen für das Risikomanagement wie für Vorstände nach dem Aktiengesetz.
- Für andere Gesellschaftsformen, wie etwa die Offene Handelsgesellschaft oder die Kommanditgesellschaft. Diese sind nämlich den Kapitalgesellschaften hinsichtlich der Rechtspflichten zur IT-Sicherheit dann gleichgestellt, wenn sie keine natürliche Person als persönlich haftende Gesellschafter haben (vgl. dazu das Kapitalgesellschaften und Co-Richtlinie-Gesetz, "KapCoRiLiG").

Kommt die Geschäftsführung oder der Vorstand - als Verantwortliche - der oben beschriebenen Risikovorsorgepflicht nicht nach und entsteht dadurch dem Unternehmen ein finanzieller Schaden, kann dies zu einer persönlichen Haftung der Mitglieder des Vorstands und der Geschäftsführung, unter Umständen auch der Aufsichtsratmitglieder (§116 AktG) führen.

Schadensersatz

Die mangelhafte IT-Sicherheit eines Unternehmens kann auch Schadensersatzansprüche desjenigen Vertragpartners nach sich ziehen, dem durch die Leistungserbringung des Unternehmens konkret bezifferbare Schäden entstanden sind, etwa in Form eines kompletten oder auch nur teilweisen Produktions- oder gar Betriebsausfalles. Dasselbe gilt für den Fall, dass vertrauliche fremde Informationen abhanden gekommen sind. Als Haftungsgrundlage kommen hierbei schuldrechtliche Schadensersatzansprüche in Betracht, gemäß § 280ff. BGB. Gerade in diesem Zusammenhang ist auch § 241 Abs. 2 BGB zu beachten, wonach die Pflicht besteht, auf die Rechte, Rechtsgüter und Interessen des Vertragspartners Rücksicht zu nehmen. Hierzu gehören insbesondere die Beachtung von Schutzpflichten, Aufklärungs- und Beratungspflichten.

Datenschutzrechtliche Haftung

Die Haftungsrisiken im Bereich des Datenschutzrechts sind enorm, sowohl für das Unternehmen als auch für die Geschäftsführung. So ergibt sich aus § 7 S. 1 Bundesdatenschutzgesetz (BDSG) ein verschuldensunabhängiger Schadensersatzanspruch. Diese Vorschrift bestimmt nämlich, dass ein Unternehmen für alle Schäden verschuldensunabhängig (!) und unbegrenzt haftet, die es Dritten durch unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten zufügt. Darüber hinaus kommen hierbei auch deliktische Ansprüche gem. § 823 BGB in Betracht, da das von § 823 I BGB geschützte Rechtsgut Eigentum eben auch die Integrität von Daten umfasst. Nicht zuletzt wäre hier auch eine Verletzung des allgemeinen Persönlichkeitsrecht zu denken, etwa wenn es um

personenbezogene Daten geht.

Beispiel: Ein Hacker kann Kundendaten auslesen, weil keine Firewall eingesetzt wird, vgl. Anlage zu § 9 Satz 1 BDSG Nr. 2. Dabei ist insbesondere für Unternehmen die in § 7 BDSG enthaltene Beweislastumkehr problematisch. Es wird nämlich zunächst immer erst einmal von einem Verschulden des Unternehmers ausgegangen. Bezüglich der Haftung gilt nur für den Fall etwas anderes, in dem das Unternehmen die "gebotene Sorgfalt" (vgl. § 7 S. 2 BDSG) beachtet hat. Dies ist natürlich dann der Fall, wenn es die oben aufgeführten Verpflichtungen zur Einhaltung des Datenschutzes beachtet und auch umgesetzt hat.

Bußgelder und Freiheitsstrafe

Auch in den Fällen, bei denen noch kein Schaden entstanden ist, kann die mangelnde Umsetzung von IT-Sicherheitsbestimmungen im besonders sensiblen Bereich des Datenschutzes teuer werden. So können in Fällen, in denen personenbezogene Daten nicht ausreichend gemäß den Vorgaben des BDSG geschützt werden, je nach Schwere des Verstoßes

- Bußgelder (bis zu 250.000 Euro, auch bei fahrlässiger Begehungsweise, § 43 BDSG)
- und sogar Freiheitsstrafen von bis zu zwei Jahren gegen die Verantwortlichen verhängt werden (vgl. § 44 BDSG).

In solchen Fällen können die IT-Verantwortlichen - gleich ob Vorstand, Geschäftsführer, Behördenleiter, angestellter oder externer IT-Administrator - tatsächlich mit "einem Bein im Gefängnis stehen".

Eigener Finanz- und Imageschaden

Ausfälle der IT-Infrastrukur können natürlich dem betroffenen Unternehmen auch direkt hohe finanzielle Verluste bescheren, etwa wenn es um einen länger andauernden Ausfall der unternehmenseigenen IT-Infrastruktur geht. Hinzu kann zudem der Imageverlust des Unternehmens kommen, weil etwa grobe Versäumnisse im Bereich des Datenschutzes an die Öffentlichkeit gelangen sollten. Nur am Rande sei noch erwähnt, dass Defizite im Bereich der IT-Sicherheit dazu führen können, dass die Versicherungen ihre Leistungen kürzen und sich dabei auf ein mögliches Mitverschulden des "blauäugigen" Unternehmens berufen. In diesem Zusammenhang kann es dann auch leicht zu einer Erhöhung der Versicherungsprämie für zukünftige Fälle kommen.

Autor:
RA Max-Lion Keller, LL.M. (IT-Recht)
Rechtsanwalt