Riskmanagement und Recht

(Referat gehalten am TechEvent der Trivadis AG, www.trivadis.com,
am 15. April 2005 im Hotel Mövenpick in Regensdorf)
(Es gilt das gesprochene Wort)

A. Einleitung

"No risk, no fun". Dieser neudeutsche Satz ist wohl jedem bekannt und er wird auch gerne beigezogen, wenn man tollkühne Projekte angeht, sei es im privaten Bereich oder in Unternehmen. Dabei wird diese Aussage oft dergestalt falsch verstanden, dass man glaubt, der Spass komme mit zunehmendem Risiko. Dies ist jedoch zweifellos unzutreffend. Ich würde gar sagen, diese Schlussfolgerung ist geradezu verantwortungslos. Im privaten Bereich mag diese Aussage noch einen gewissen Reiz haben, da der Kreis der Betroffenen für den Fall, dass der „fun" exzessiv wurde, begrenzt und möglicherweise überschaubar ist. In einem Unternehmen jedoch ist diese Sichtweise unannehmbar. Zwar ist es gerade in einem immer härteren Wettbewerb Aufgabe des Managements Chancen zu nutzen, was letztlich dazu führt, dass das Unternehmen tendenziell auch mit mehr Risiken konfrontiert wird. Für die Sicherung des zukünftigen Erfolges ist es jedoch entscheidend, dass Chancen und Risiken rechtzeitig erkannt, ganzheitlich analysiert und wirkungsvoll gemanagt werden. Dabei gilt es Grundsätze, Methoden und Instrumente zur risikobewussten Unternehmensführung zu kennen und unternehmensintern intensiv zu diskutieren. Diese Instrumente müssen vom Management erarbeitet und den Mitarbeitern zur Verfügung gestellt werden. Das heisst nichts anderes, als dass das Bewusstsein der nachhaltigen Sicherheit innerhalb eines Unternehmens beim Management beginnen muss. Sicherheit kommt also nicht von unten nach oben, sondern von oben nach unten. Es braucht das Top-Down-Prinzip, ausgehend von der Geschäftsleitung bis hin zu jedem einzelnen Mitarbeiter. Zwar ist die Geschäftsleitung für die Sicherheit verantwortlich, doch muss sie in einem Unternehmen auch gelebt werden, was ich Ihnen an einem Beispiel noch aufzeigen werde. Dieses auf allen Ebenen angesiedelte Sicherheitsbewusstsein hat auch direkte Auswirkungen auf die Reputation des Unternehmens und das Vertrauen der Kunden.

Interessant ist, dass auch heute noch immer ein mangelndes Bewusstsein über die Abhängigkeit geschäftlicher Prozesse von IT-Systemen und den daraus resultierenden Risiken existiert. Während das Risikomanagement für die „klassischen" Unternehmensbereiche gut entwickelt ist, ist dies mit Bezug auf die IT-Sicherheit nur bedingt der Fall. IT-Sicherheit wird in den meisten Unternehmen nach wie vor **nicht** als grundlegende Voraussetzung für geschäftliche Prozesse betrachtet, was vielfach in sehr verteilten, ineffizienten und technik-zentrierten Ansätzen resultiert. Durch regulative Vorgaben und geeignete „best practice"-Ansätze - die eben von der Führung erarbeitet werden müssen - lassen sich langfristig aber sicherlich auch hier ähnliche Vorgehensweisen für das Risikomanagement bei der IT-Sicherheit in den Unternehmen und Verwaltungen verankern. Dabei sollten sich alle Entscheidungsträger rechtzeitig mit der Informationssicherung auseinandersetzen, da im Krisenfall dazu keine Zeit mehr bleiben wird.

B. Die Verantwortlichkeit für das eigene Handeln

Kommen wir nach diesen einführenden Worten über Risiko und Risikomanagement zu den Konsequenzen oder ihren Grundlagen. Ich spreche hier von der Rechtsordnung, also den Gesetzen, Verordnungen usw. Dabei gibt es aber einen klaren, wenn auch banalen Grundsatz: Jede Handlungsweise ist zu verantworten, sei es zivil- oder gar strafrechtlich.

Die meisten **zivilrechtlichen** Regelungen über die Verantwortlichkeit für das eigene Handeln finden sich zweifellos im OR. Dabei unterscheidet man zwischen vertraglicher und ausservertraglicher Haftung und innerhalb dieser beiden Gruppen unterscheidet man dann wiederum nach Verschuldenshaftung und nach Kausalhaftung. Ein kleines Beispiel für eine ausservertragliche Kausalhaftung, damit dies etwas deutlich wird, ist die Tierhalterhaftung. Wenn Sie einen Hund besitzen und der beisst einem Spaziergänger in die Wade, so haften Sie als Tierhalter, unabhängig davon, dass Sie selber dem Dritten gar nicht in die Wade gebissen haben. Sie haften also, obwohl Sie nicht der Täter sind. Die Kausalhaftung ist also eine Haftung für eine bestimmte Ursache, unabhängig davon, ob Sie persönlich ein Verschulden trifft oder nicht. Eine andere ausservertragliche Kausalhaftung - also eine Haftung ohne Verschulden - ist die sog. Geschäftsherrenhaftung, auf die ich noch zu sprechen komme.

C. Zwei konkrete Beispiele für rechtliche Rahmenbedingungen

Nach diesen wenigen rechtlichen Ausführungen gehen wir doch in medias res und beleuchten das Ganze anhand zweier konkreter Sachverhalte. Zuerst zu

a) P2P-Filesharing

Wie alles im Verlauf der letzten Jahrzehnte ist insbesondere der IT-Bereich einer rasanten technischen Entwicklung unterworfen. Diese ist teilweise derart rasant, dass die rechtlichen Auswirkungen häufig vielfach anfänglich gar nicht überblickt werden resp. anfänglich gar nicht erkannt werden. Ich spreche von den sogenannten OnlineTauschbörsen oder peer-to-peer-Netzwerken (P2P).

Sie alle kennen wohl BitTorrent oder KaZaA, eDonkey und Gnutella. Die technischen Aspekte, also die Funktionsweise der Software, kennen Sie viel, viel besser als ich, da wage ich nicht einmal im Ansatz darüber zu reden. Aber ich spreche von den rechtlichen Konsequenzen, wenn Sie da in irgendeiner Form mitmachen. Wie Ihnen bekannt ist, kann die entsprechende Software problemlos aus dem Internet heruntergeladen und auf dem Laptop installiert werden. Damit hat man problemlos die Möglichkeit, im weltweiten Netz urheberrechtlich geschützte Computerspiele, Musik, Filme usw. herunterzuladen. Nun darf aber nicht übersehen werden, dass die internationale Musik- und Filmindustrie energisch gegen den Austausch von Musiktiteln und Filmen in P2P-Netzwerken vorgeht. Mittlerweile geht die Industrie gar mit strafrechtlichen Mitteln direkt gegen die „Fileswappers“ vor, d.h. gegen die am Austausch beteiligten P2P-User. In Deutschland, der Schweiz, Dänemark, Spanien, Italien und Grossbritanien sind entsprechende Strafverfahren gegen die Beteiligten im Gange. Die Staatsanwaltschaft Mühlhausen (Thüringen) will gar

nicht nur gegen die Betreiber von ftpwelt.com Strafverfahren einleiten, sondern gegen alle 45'000 Abonnenten!

Kommen wir aber zurück zu unserem Eingangsspruch und stellen uns die Frage: Gibt es auch „more fun“ und „less risk“? Ich betrachte dies mal aus der Sicht des Unternehmens Trivadis.

Fakt ist, dass sich Personen, die sich Filme oder Musik aus dem Netz herunterladen kaum strafbar machen. Dies als Folge des sog. „rechtmässigen Eigengebrauchs“ gemäss Art. 19 Abs. 1 lit.a URG. Das gilt aber nicht für Computerspiele. Wer diese herunterlädt und Urheberrechte verletzt, macht sich strafbar, da der rechtmässige Eigengebrauch gemäss Abs. 4 von Art. 19 URG nicht für Computerprogramme gilt.

Wie sieht nun die Rechtslage aus, wenn sich Dateien auf einem unternehmenseigenen Laptop finden und während der Arbeitszeit heruntergeladen wurden? Immerhin existiert ein Art. 100quater StGB, der wie folgt lautet: *Wird in einem Unternehmen in Ausübung geschäftlicher Verrichtung im Rahmen des Unternehmenszwecks ein Verbrechen oder Vergehen begangen und kann diese Tat wegen mangelhafter Organisation des Unternehmens keiner bestimmten natürlichen Person zugerechnet werden, so wird das Verbrechen oder Vergehen dem Unternehmen zugerechnet. In diesem Fall wird das Unternehmen mit Busse bis zu CHF 5 Mio. bestraft.*

Nun kann man sich in der Tat fragen, ob auch in einem IT-Unternehmen das Herunterladen von Dateien aus einem P2P-Netzwerk durch einen Mitarbeiter in Ausübung geschäftlicher Verrichtung erfolgt oder Teil des Unternehmenszweckes ist, doch weiss ich aus Erfahrung, dass die Strafverfolgungsbehörden die Tendenz haben, die Strafbarkeit eher auszuweiten als einzuengen. Ich verweise hier auf das Beispiel der Absicht der Staaatsanwaltschaft Mühlhausen. Aber auch die Bundesgerichtspraxis ist hiefür beredtes Beispiel.

Persönlich vertrete ich die Auffassung, dass das Unternehmen strafrechtlich zur Verantwortung herangezogen werden kann, wenn wegen mangelhafter Organisation die Tat keiner bestimmten natürlichen Person zugerechnet werden kann. Für die Computerspiele gilt dies ohnehin, da kein rechtmässiger Eigengebrauch gemäss Art. 19 Abs. 4 URG geltend gemacht werden kann. Ich behaupte nun, dass die Strafbarkeit auch auch für heruntergeladene Film- und Musikdateien gegeben ist. Dies deshalb, weil die Exculpation des Privatgebrauches gemäss Art. 19 Abs. 1 lit.a URG beim Unternehmen nicht greift. Privatgebrauch ist nämlich nur dann anzunehmen, wenn nicht beliebige Dritte Zugriff auf das Werk haben und dieses mitbenutzen können. Dies ist aber m.E. bei einem unternehmenseigenen Computer nicht der Fall. Damit aber haben wir „high risk“ für das Unternehmen, auch wenn der Mitarbeiter „a lot of fun“ hat.

Aber unbeachtlich der wahrscheinlichen strafrechtlichen Verantwortung des Unternehmens, hat der Urheber zivilrechtliche Ansprüche. Er kann also seine Ansprüche gegenüber dem Urheberrechtsverletzer geltend machen. Die Frage ist nur, wer ist der Urheberrechtsverletzer? Ist es der Mitarbeiter, der die Files heruntergeladen hat oder ist es das Unternehmen, dem der Computer gehört?

Wahrscheinlich ist, dass der Verletzte wohl nur die IP-Adresse des Unternehmens eruieren kann, nicht aber den Mitarbeiter, der die Files heruntergeladen hat. Die Frage also ist, ob das Unternehmen direkt haftbar gemacht werden kann über Art. 41 OR, der Verschuldenshaftung, oder über die Kausalhaftung, nämlich der sogenannten Geschäftsherrenhaftung nach Art. 55 OR. Diese Frage ist nicht so einfach zu beantworten. Und letztlich stellt sich die Frage der Verantwortlichkeit der Organe beispielsweise nach dem Aktienrecht.

Das Unternehmen wird aus OR 41 haftbar, wenn einem seiner Organe ein Verschulden zur Last fällt (BGE 107 II 496 E.b). Und Organ einer juristischen Person ist, wer deren Geschäftsführung besorgt oder für sie in leitender Stellung tätig ist. Dabei genügt Fahrlässigkeit, die in einem Tun **oder** Unterlassen bestehen kann. Fahrlässigkeit beruht auf Unsorgfalt resp. mangelnder Sorgfalt, wobei ein objektiver Massstab angelegt wird. Dabei genügt es, wenn sich der Schädiger - also das Unternehmen resp. seine Organe - nach der ihm zuzumutenden Aufmerksamkeit und Überlegung hätte sagen sollen, es bestehe eine konkrete Gefahr der Schädigung. Wenn es dem Geschädigten gelingt, diesen Beweis zu führen, dann haben wir den Haftpflichttatbestand, da die Widerrechtlichkeit und der Schaden ausgewiesen ist.

Aber auch wenn OR 41 nicht greifen sollte, ist noch Art. 55 OR zu beachten, wonach der Geschäftsherr für den Schaden haftet, den seine Arbeitnehmer in Ausübung ihrer dienstlichen oder geschäftlichen Verrichtungen verursacht haben. Zwar muss es einen Zusammenhang geben zwischen der Tätigkeit und der aufgetragenen Verrichtung. Doch wenn dies bejaht wird, dann hat der Geschäftsherr resp. das Unternehmen nur zwei Haftungsbefreiungsgründe. Es muss den Nachweis erbringen,

- dass alle nach den Umständen gebotene Sorgfalt angewendet wurde, um einen Schaden dieser Art zu verhindern oder
- dass der Schaden auch bei Anwendung dieser Sorgfalt eingetreten wäre.

Und letztlich sprechen wir auch von der aktienrechtlichen Verantwortlichkeit, wenn nicht dem Sorgfaltsmassstab entsprochen wird, der durch Art. 717 OR an das Verhalten der Geschäftsführung einer AG gestellt wird. Dabei ist einzugrenzen, dass einzig Gesellschaftsgläubiger, die Gesellschaft und die Aktionäre klageberechtigt sind. Aber auch hier gilt, dass im Rahmen der aktienrechtlichen Verantwortung die **Unterlassung einer Handlung** relevant ist. Die aktienrechtliche Sorgfaltspflicht verlangt von den mit der Geschäftsführung betrauten Personen, dass sie in jedem Fall aktiv einschreiten, wenn sie in ihrem Kompetenzbereich Sachverhalte feststellen, welche zu einer Schädigung der Gesellschaft führen könnten. Werden die notwendigen Massnahmen unterlassen, so macht sich die betreffende geschäftsführende Person für den aus der Unterlassung entstehenden Schaden haftbar. Um es nun konkret auf unseren Sachverhalt anzuwenden, heisst dies, dass die Organe haftbar gemacht werden können, wenn sie nicht die technischen und organisatorischen Massnahmen getroffen haben, die dem Stand der Technik zu entsprechen haben, wobei wohl als objektiver Massstab die Art. 7 DSG i.V.m. Art. 8 DSV heranzuziehen sind, die äusserst weit gehen.

Eines darf letztlich aber nicht übersehen werden: Auch der Mitarbeiter kommt nicht ungeschoren davon, sei es zivil- oder allenfalls strafrechtlich. Daraus wird ersichtlich, dass das Sicherheitsbewusstsein bei jedem Mitarbeiter verankert sein muss.

Kommen wir nun zum zweiten Sachverhalt,

b) Die personenbezogene Überwachung der Mitarbeiter

Die Frage ist, ob angesichts der Risiken, die einem Unternehmen als Folge des vorstehenden Beispieles erwachsen können, der Arbeitnehmer überwacht werden darf. Diese Frage wurde in Art. 26 ArGV eigentlich recht lapidar beantwortet in dem Sinne, dass Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen sollen, **nicht** eingesetzt werden dürfen. Das heisst, dass es ohne vorherige Information dem Arbeitgeber grundsätzlich nicht erlaubt ist, E-Mails und Internetzugriffe der Arbeitnehmer zu speichern, zu überwachen oder zu kontrollieren, weil er dabei auf private Inhalte und Informationen stossen und das Verhalten der Arbeitnehmer überwachen kann. Entsprechend aber ist eine Überwachung erlaubt, wenn *ausgeschlossen* werden kann, dass private Inhalte gespeichert und überwacht werden. Eine Ausnahme vom grundsätzlichen Verbot der Überwachung von E-Mails und Internet-Zugriffen ist - vorbehältlich einer Regelung in einem Benützungsreglement - möglich, wenn konkrete Anhaltspunkte für Missbrauch vorliegen. Wenn aber Anhaltspunkte für rechtswidriges, insbesondere strafbares Handeln vorliegen, hat die Arbeitgeberin die Strafverfolgungsorgane einzuschalten, auch um eine Mittäterschaft auszuschliessen. Wegen des schweren Eingriffs in die Persönlichkeit kann jedoch nur die zuständige Strafjustizbehörde eine solche Überwachung anordnen.

D. Schlussbemerkung

Ich komme zur Schlussfolgerung und der Behauptung, dass letztlich „more fun, auch more risks“ bedeutet. Der technische Fortschritt hat durchaus seinen Reiz. Es macht Spass, die immer neuen Möglichkeiten zu kennen und auszuprobieren und der technische Fortschritt bietet nicht zu unterschätzende Chancen im immer härter werdenden Wettbewerb. Es muss aber gleichzeitig berücksichtigt werden, dass den damit verbundenen Risiken ein entsprechendes Augenmerk zu widmen ist. Im Ergebnis heisst dies, dass technische Entwicklungen im Auge zu behalten sind, um Chancen zu erkennen und zu nutzen und gerade Sie als IT-Consultants müssen sie kennen. Gleichzeitig aber gilt es von der Geschäftsleitung her, jeden Einzelnen darauf zu sensibilisieren, dass das technisch Machbare auch mit dem Recht im Einklang stehen muss. Gelingt dies, so hat dies auch direkte Auswirkungen auf die Reputation des Unternehmens und das Vertrauen der Kunden in das Unternehmen. Zu Recht hat deshalb die Geschäftsleitung diese „Compliance“-Problematik zu einem TTC-Forschungsprojekt erklärt.

Ich danke Ihnen für die Aufmerksamkeit.

Patrik A. Häberlin, Verwaltungsrat