JURISTISCHE ASPEKTE DER IT-SECURITY AUS SICHT DER VERNETZTEN UNTERNEHMEN

(Vortrag gehalten an IT-Security-Seminare mit der Trivadis AG
in Basel, Bern, Regensdorf, Stuttgart und München
im August und September 2001)
Es galt das gesprochene Wort

1. IT-Security – Chefsache?!

Angriffe auf die IT-Umgebung von Unternehmen gehören zur Tagesordnung. Sie verursachen zum Teil erhebliche Schäden. Ein Blick auf die Statistiken[1] genügt:
85% der Befragten stellten in den letzten 12 Monaten Verstösse gegen die Computersicherheit fest, 64% mussten dabei finanzielle Einbussen hinnehmen, wovon 35% diese Einbussen beziffern konnten und zwar auf ca. 380 Mio US $. Oftmals ist der Schaden jedoch gar nicht bestimmbar. Man denke insbesondere an Imageschäden oder andere Langzeitschäden, die durch Verlust von Wettbewerbsvorteilen entstehen, wenn sensible Geschäftsgeheimnisse oder Forschungsergebnisse aufgrund eines Hack-Angriffs z.B. eines Industriespions verloren gehen.

Allerdings ist das Internet kein rechtsfreier Raum. Im Gegenteil: unsere Rechtsordnung hält auch für dieses neuartige Rechtsgebiet Antworten bereit oder hat sich - soweit notwendig - den heutigen Bedürfnissen nach Rechtssicherheit im Internet angepasst. So wird im Falle eines Hack-Angriffs in erster Linie der Täter strafbar und schadenersatzpflichtig.
Aber auch das vernetzte Unternehmen selbst kann aus vielfachen Gründen einer Haftung unterliegen. Dabei ist häufig die Führungsebene betroffen, d.h. die Geschäftsleitung, der Vorstand oder die Aufsichtsräte, wenn diese keine nach den Umständen zu erwartenden Sicherungsvorkehrungen ergriffen haben, um Unternehmensdaten und Informationen vor internen oder externen Angriffen zu schützen. Daraus müssen die Führungskader die Konsequenzen ziehen und nicht mehr nur delegieren, sondern verstärkt kontrollieren; kurz: IT-Security ist Chefsache und dabei ein ernst zu nehmendes Thema.

2. Strafrechtliche Verantwortlichkeit

Nehmen wir an, dass der Hacker ein Mitarbeiter eines vernetzten Unternehmens ist und seinen Angriff von seinem Arbeitsplatz aus begangen hat. Über seine strafrechtliche Beurteilung wurden Sie bereits orientiert. Wie aber sieht es mit dem Unternehmen aus? Ist es auch

betroffen? Selbstverständlich, und zwar aus vielerlei Gründen: Zunächst hat es dem Täter den Zugang zum Internet via Firmennetz verschafft. Besteht eine strafrechtliche Verantwortlichkeit, wenn ein Mitarbeiter via Computer am Arbeitsplatz Internet-Seiten von Kunden unbrauchbar macht? Dies ist in der Lehre umstritten. Auf der einen Seite wird eine strafrechtliche Verantwortung abgelehnt. Nach einer anderen Lehrmeinung können dagegen die gleichen Grundsätze wie für Internet-Provider (vgl. CompuServe-Fall!) und zwar analog angewandt werden.

Allerdings sind im Strafrecht nur natürliche Personen belangbar, d.h. in unserem Fall auch nur natürliche Personen innerhalb des Unternehmens und nicht das Unternehmen selbst. Die Vorgesetzten, d.h. die Mitglieder des Verwaltungsrates bzw. der Geschäftsleitung sind kraft ihrer Autoritätsstellung und Befehlsmacht grundsätzlich dazu verpflichtet, Delikte ihrer Untergebenen zu verhindern. Sie machen sich aber nicht bereits strafbar, weil in ihrem Unternehmen strafbare Handlungen begangen werden, von denen der Verwaltungsrat bzw. die Geschäftsleitung nichts weiss oder wissen konnte. Man muss hier im Gegenteil differenzieren: da es sich bei den im Internet begangenen Straftaten jeweils um Vorsatz- und nicht um Fahrlässigkeitsdelikte handelt, müssen die Vorgesetzten positive Kenntnis der strafbaren Handlung ihres Angestellten haben, um selbst strafrechtlich zur Rechenschaft gezogen werden zu können. Daraus folgt aber, dass Verwaltungsrat bzw. Geschäftsleitung keine Nachforschungen darüber betreiben müssen, ob ein Mitarbeiter eine strafbare Handlung begeht oder nicht. Erst bei konkreten Hinweisen auf mögliche Delikte sind die notwendigen Schritte (Anzeige bei den Strafbehörden, Internet-Sperre etc.) einzuleiten, wollen die Vorgesetzten nicht mit der Anschuldigung belastet werden, die Tat wäre von ihnen bewusst in Kauf genommen (Eventualvorsatz) oder gar mitbegangen worden.

Nicht zu unterschätzen ist jedoch der Tatbestand der ungetreuen Geschäftsbesorgung gemäss Art. 158 StGB/§ 266 DStGB. Das tatbestandsmässige Verhalten seitens des Täters liegt darin, dass er durch eine bestimmte Verhaltensweise (Begehung oder Unterlassung) Pflichten verletzt, welche ihm im Rahmen seiner Funktion als Geschäftsführer oder Aufsichtsorgan auferlegt worden sind. Ein solcher Vorgang muss pflichtwidrig sein, was bedeutet, dass dem Täter ein Verstoss gegen eine ihm obliegende Rechtspflicht, welche sich entweder aus gesetzlichen Bestimmungen oder aufgrund rechtsgeschäftlicher Grundlagen (beispielsweise aus Arbeitsvertrag, den Statuten der AG oder GV-Beschlüssen, etc.) ergeben kann, vorzuwerfen ist.

Die Konsequenzen sind beachtlich. Zu verweisen ist hier auf Art. 7 des Datenschutzgesetz, der besagt, dass Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden müssen. Das heisst, dass Datenbearbeiter deshalb verpflichtet sind, ein umfassendes, ganzheitliches Sicherheitskonzept aufzu-

---

[1] Aus: „2001 Computer Crime and Security Survey“, Computer Security Institute, San Francisco 2001; die Studie wurde aufgrund von Aussagen von 538 IT-Security Spezialisten in amerikanischen Unternehmen, Regierungsstellen, Finanzinstituten, Krankenhäusern und Universitäten erstellt.

bauen. Ungenügend wäre es z.B. auf einem Computersystem den Passwortschutz einzuführen (technische Massnahmen), sofern nicht gleichzeitig die Anwendung dieses System genügend instruiert, dokumentiert und überwacht wird (organisatorische Massnahme) und soweit nicht der räumliche Zutritt zu den Datenverarbeitungsanlagen in einer geeigneten Form eingeschränkt ist (bauliche Massnahme).

3. Zivilrechtliche Verantwortlichkeit

Auch in zivilrechtlicher Hinsicht können Verantwortlichkeiten bestehen. Zu denken wäre hier etwa an die **Haftung des Geschäftsherrn** (OR 55 / § 831 BGB), welche sehr viel weiter geht als die soeben besprochene Haftung des Unternehmens in strafrechtlicher Hinsicht: Ein Geschäftsherr kann eine natürliche Person (z.B. der Inhaber einer Internet-Beratungsfirma, die als Einzelfirma oder Kollektivgesellschaft organisiert ist), aber auch eine juristische Person (Aktiengesellschaft, GmbH, Verein, Stiftung etc.) oder bei gewerblichen Verrichtungen sogar ein Gemeinwesen sein.

Gegenüber Dritten, wie z.B. dem Endkunden, haftet in aller Regel das Unternehmen, da gemäss OR 101 (§ 278 BGB) (**= Haftung für Hilfspersonen)** das Unternehmen für fremdes Verschulden (seiner Mitarbeiter) ohne Rücksicht auf sein eigenes Verhalten haftet, sofern ein Vertragsverhältnis zwischen dem Unternehmen und dem Dritten besteht. Der Gesetzgeber hat diese Regelung getroffen, um den Geschädigten zu schützen, da in der Regel der eigentliche Schädiger – d.h. bei uns der Hacker – für den Schaden nicht aufkommen kann. Voraussetzung ist allerdings, dass die Handlung des Mitarbeiters dem Schuldner-Unternehmen auch vorzuwerfen wäre, wenn es sie selbst vorgenommen hätte (hypothetische Vorwerfbarkeit). Stellen Sie sich also beispielsweise vor, dass einer Ihrer Mitarbeiter während seiner Arbeitszeit einen Hack-Angriff gegen einen Ihrer Kunden lanciert und dessen Computersystem lahmlegt. Anderseits ist aber auch darauf hinzuweisen, dass eine Haftung für Exzess-Handlungen des Gehilfen nicht in Betracht kommt.

Ausserhalb eines solchen Vertragsverhältnisses findet OR 55 (§ 831 BGB) Anwendung, wonach der Geschäftsherr für alle Schäden haftet, die ein Mitarbeiter in Ausübung einer dienstlichen oder geschäftlichen Besorgung verursacht. Wichtig ist, dass der Mitarbeiter in einem Subordinationsverhältnis zum Unternehmen steht und der Schaden rechtswidrig verursacht wurde. Die Frage des Verschuldens ist weitgehend irrelevant (weitgehend, weil sie später bei der Schadensbemessung wieder eine Rolle spielen kann). Haften muss der Geschäftsherr vielmehr deswegen, weil er seinen Sorgfaltspflichten offenbar nicht nachgekommen ist. Diese vom Gesetzgeber vorgegebene Annahme kann allerdings vom Geschäftsherrn widerlegt werden, indem er den Entlastungsbeweis antritt und nachweist, dass er bei der Auswahl, der Instruierung und der Überwachung seines Untergebenen die im Verkehr erforderliche Sorgfalt beachtet hat. Dieser Beweis wird aber insbesondere dann schwierig sein, wenn ein Unternehmen keinen ausreichenden, dem heutigen Stand der Technik angemesse-

nen Schutz wie firewalls, chinese walls etc. vor fremden Zugriffen auf die eigenen Daten nachweisen kann und seine Angestellten zu wenig an der Hand geführt, sie über die möglichen Risiken und ihre Pflichten als Arbeitnehmer belehrt hat. Auch diese Beweiserbringung ist Chefsache!

Neben der Geschäftsherrenhaftung ist die **Verantwortlichkeit**sbestimmung OR 754 (§ 93 AktG; allerdings: keine Haftung gegenüber Kunden oder sonstigen Dritten) im Aktienrecht zu beachten. Sie legt fest, dass die Mitglieder des Verwaltungsrates, der Geschäftsleitung sowohl der Gesellschaft als auch den einzelnen Aktionären und den Gläubigern der Gesellschaft für Schäden persönlich verantwortlich sind, die sie durch absichtliche oder fahrlässige Verletzung ihrer Pflichten verursacht haben. Entscheidend ist hier ihre sog. Organstellung und ihre wesentliche Beteiligung an der Willensbildung im Unternehmen. Bei Schäden, die von Organen angerichtet werden, ist eine Haftungsbefreiung des Unternehmens nicht möglich, weil ihr Verhalten automatisch auch der juristischen Person zugerechnet wird (ZGB 55). Ist dem Geschäftsführer einer AG z.B. gleichgültig, dass die Marketingabteilung von sich aus auf der Firmen-Web-Site einen unlauteren Werbefeldzug gegen die Konkurrenz startet, so kann er für etwaige Schäden persönlich verantwortlich sein: erstens gegenüber der AG und den Aktionären, weil durch Verletzung seiner Aufsichtspflichten die AG aufgrund ihrer Geschäftsherrenhaftung (OR 722) für den Schaden aufkommen muss, als auch gegenüber dem direkt Geschädigten, falls die AG und die betreffenden Marketingmitarbeiter den Schaden nicht bezahlen können.

4. Schutzvorkehrungen

Denken Sie wieder an den Mitarbeiter, der vom Arbeitsplatz aus seine Hack-Angriffe lanciert. Welche Schutzvorkehrungen wären technisch, organisatorisch oder gar baulich sinnvoll und notwendig? Hiezu erfolgen nur summarische Ausführungen, da dies Teil des Betriebskonzeptes ist, das von der Trivadis erläutert wird.

In technischer Hinsicht können die Risiken im Zusammenhang mit der Internet- und Emailnutzung z.B. Antivirus- und Diskquotaprogramme, Backups und Firewalls (um nur einige wenige zu nennen) reduziert werden.

Es stellt sich darüber hinaus die Frage, ob der Mitarbeiter bei seiner gewöhnlichen Arbeitstätigkeit vom Arbeitgeber überwacht werden kann. Es gelten die Bestimmungen der 3. Arbeitsordnung[2], Art. 26. Sie verbieten grundsätzlich den Einsatz von Überwachungs- und Kontrollsystemen zur Überwachung am Arbeitsplatz. Es soll nicht Gleiches mit Gleichem vergolten werden: Spionprogramme oder ständige Auswertungen wären verbotene Beschnüffelungen der Angestellten. Statt die Mitarbeiter zu überwachen, könnte er z.B. den Internet-Zugang einschränken, indem er keine persönlichen Emailkonten zur Verfügung stellt. Ob Angestellte nämlich das Recht haben, privat Internet und Email zu nutzen, hängt in erster Linie vom Willen des Arbeitgebers ab. Ähnlich wie in anderen Bereichen des Arbeitsverhältnisses, hat er ein Weisungsrecht (OR 321d). Es wäre daher z.B. ratsam, eine schriftliche Weisung über die Nutzung netzbasierter Anwendungen zu erlassen. Eine solche konkrete Nutzungsregelung schafft Klarheit und Rechtssicherheit und drängt sich schon allein wegen der soeben besprochenen Geschäftsherrenhaftung auf; eine nur mündlich kommunizierte Nutzungsregelung ist zwar ebenfalls verbindlich, kann aber im Streitfall zu Nachweisschwierigkeiten führen.

Nochmals: grundsätzlich darf eine gezielte personenbezogene Verhaltensüberwachung durch Auswertung der automatischen Protokollierungen der Surfspuren nicht erfolgen. Gestattet sind aber stichprobenartige, anonyme Kontrollen der Protokollierungen, um zu überprüfen, ob die Nutzungsregelung eingehalten werden. Wenn diese Massnahmen einen konkreten Missbrauch aufzeigen, kann dies zu einer personenbezogenen Verhaltensüberwachung führen, indem die Protokollierungen ausgewertet werden. Solche Auswertungen dienen dazu, Beweise zu erheben, um Missbräuche zu sanktionieren. Allerdings muss die Belegschaft vorher entsprechend informiert worden sein, da ansonsten die Registrierungspflicht gemäss DSG 11 Abs. 3 bei Anlegung einer Datensammlung auflebt.

Das Verbot der Verhaltensüberwachung gemäss ArGV3 Art. 26 gilt also nicht absolut. Vielmehr ist die Frage, wie weit diese Überwachungsmethoden im Einzelnen gehen dürfen, durch Abwägung der konkret betroffenen Interessen des Unternehmens und seiner Arbeitnehmer zu beantworten. Es stehen sich nämlich einerseits das Interesse des Arbeitgebers an

[2] SR 822.113.

ordentlicher Arbeitszeitnutzung, welches sich aus den Treue- und Sorgfaltspflichten des Arbeitnehmers ergeben, OR 321a, und andrerseits das berechtigte Interesse (und Recht!) des Arbeitnehmers auf Schutz seiner Persönlichkeit aus OR 328b und DSG gegenüber.

Spätestens bei konkretem Verdacht auf strafbares Verhalten eines Mitarbeiters sind aber die Strafverfolgungsbehörden einzuschalten. Zwar besteht keine Pflicht, jedoch ist es empfehlenswert, zumindest im Zusammenhang mit Offizialdelikten, Anzeige zu erstatten, um die Gefahr der Mittäterschaft zu verhindern, z.B. bei StGB 144bis Ziff. 2.

Wenn die Voraussetzungen und die Regeln der Überwachung eingehalten worden sind, kann das Unternehmen im Falle eines erwiesenen Missbrauchs arbeitsrechtliche Sanktionen gegen den Mitarbeiter aussprechen, z.B. die Sperrung des Internetzugriffs, Schadenersatzforderungen aus OR 321e, Lohnkürzungen oder Versetzungen. In Extremfällen, wie etwa bei Wiederholungen oder bei erwiesenen Straftaten kann natürlich auch die Kündigung ausgesprochen werden, OR 335. Die fristlose Entlassung eines Angestellten kann aber nur dann ausgesprochen werden, wenn dem Arbeitgeber nach Treu und Glauben die Fortsetzung des Arbeitsverhältnisses nicht mehr zugemutet werden kann, OR 337. Aber Achtung: wenn der Arbeitgeber die einschlägigen Voraussetzungen und Regeln bei der Überwachung der Internet- und Emailaktivitäten seiner Angestellten nicht einhält, so kann dies als widerrechtliche Persönlichkeitsverletzung des Arbeitnehmers von diesem gerichtlich angefochten werden. Ich verweise hier auch ausdrücklich auf die Art. OR 328b und DSG 15/25.

5. Elektronische Signatur

Ich möchte nun auf eine besonders aktuelle technische Massnahme hinweisen, die es erlaubt, durch die Zertifizierung von Mitteilungen bzw. Informationen einerseits die Identität von Absender und Empfänger zuverlässig sicherzustellen sowie vor unbemerkter Veränderung zu schützen. Dies kann z.B. bei einem Hacking-Szenario entscheidend sein, in dem der Hacker via E-mail gefährliche Viren verbreitet, sich aber nicht zu erkennen gibt. Sie ahnen, worum es geht: die elektronische Signatur. Mit ihr werden elektronische Daten rechtsgültig signiert und verschlüsselt. Im Rahmen dieser Zertifizierung kommt ihr die wichtige Funktion einer Sicherheitsvorkehrung zu.

Natürlich spielt die elektronische Signatur noch eine andere bedeutende Rolle, nämlich dann, wenn unsere Rechtsordnung zur Gültigkeit eines Geschäfts eine „Unterschrift" verlangt. Wie Sie wissen, bedürfen Verträge zu ihrem Zustandekommen nur ausnahmsweise der Schriftform, da grundsätzlich Formfreiheit besteht, OR 11 Abs. 1 (BGB 127). Die Parteien können sich die Schriftform jedoch vertraglich vorbehalten, OR 16 (BGB 127), oder sie wird durch das Gesetz als Gültigkeitsvoraussetzung angeordnet, OR 12 (BGB 126), wobei dann der Vertrag die Unterschrift aller sich verpflichtenden Personen zu tragen hat, OR 13 (BGB 126). Im E-Commerce stellt sich jetzt die Frage, inwieweit die eigenhändige Unterschrift auch elektronisch geleistet werden kann.

Ich werde Sie jetzt kurz mit dem technischen Ablauf der elektronische Signatur bemühen, da sie – um genau zu sein - eigentlich genau das ist: eine technische Massnahme, eine Schutzvorkehrung vor Haftungs- und anderen rechtlichen Risiken:
Als Grundlage wird für jede Person ein einmaliges Schlüsselpaar generiert. Die Schlüssel werden als je öffentlich und privat bezeichnet. Zuständig für die Generierung der Schlüsselpaare sind die sog. Trust Center (öffentliche Zertifizierungsstellen, Problematik einer Haftung im Zusammenhang mit ihren Aufgaben hier nicht berücksichtigt). Der private Schlüssel wird dort aber nicht gespeichert, sondern befindet sich auf einer Chip-Karte, die dem Berechtigten/Unterzeichner ausgeteilt wird. Der öffentliche Schlüssel wird dagegen in einem öffentlich zugänglichen Verzeichnis zum jederzeitigen Abruf bereit gehalten.

Der Signaturvorgang erfolgt so, dass das zu signierende Dokument derart komprimiert wird, dass es den sog. Hash-Code ergibt, mit anderen Worten zu einer Art Quersumme seiner Originalform reduziert wird. Dann wird in einem kryptografischem Verfahren die elektronische Signatur aus dem Hash-Code und dem privaten Schlüssel des Unterzeichners erzeugt und dem Dokument angehängt. Nach der Signierung besteht die komplette Datei nun aus der ursprünglichen Datei selbst, der angehängten elektronischen Signatur und dem Signaturschlüssel-Zertifikat des Unterzeichners, d.h. also seinen persönlichen Angaben (Name, Pseudonym, Adresse etc.). Der Empfänger vermag anschliessend das Verfahren in umgekehrter Richtung mit dem öffentlichen Schlüssel durchzuführen, so dass der ursprüngliche

Hash-Code wieder vorliegt. Dann wird von der übermittelten Datei ebenfalls auf Empfängerseite der Hash-Code gebildet und mit dem entschlüsselten Hash-Code verglichen. Bei Übereinstimmung ist dies der Beweis dafür, dass die Signatur nicht unterwegs verändert und von einem Hacker angegriffen worden ist.

Im Grunde genommen garantiert die elektronische Signatur - in den Grenzen der heutigen Technik – dass der Inhalt der Datei während ihrer Reise durch das Internet unversehrt und echt geblieben ist, nicht allerdings, dass sie selbst nicht derweil von einem Unberechtigten gelesen wurde. Man kann die Nachricht allerdings selbst auch verschlüsseln, wobei der Sender die Signatur mit seinem privaten Schlüssel erstellt und die Nachricht mit dem öffentlichen Schlüssel des Empfängers chiffriert. Der Empfänger kann sodann mit dem öffentlichen Schlüssel des Senders die digitale Signatur überprüfen und mit seinem privaten Schlüssel die Nachricht dechiffrieren. Eine solche Kombination aus Signierung und Verschlüsselung ist natürlich die beste und sicherste Lösung des Datentransfers.

Das ganze Signaturverfahren basiert – kurz gesagt - auf einem komplizierten Prozedere, das auf der speziellen mathematischen Abhängigkeit des privaten und des öffentlichen Schlüssels zueinander basiert. Die Sicherheit resultiert daraus, dass die Berechnung des einen Schlüssels aus dem anderen sehr aufwendig ist, da sie selbst auf Primzahlen zurückgehen. Selbst ein Verbund aus vielen Rechnern mit der heute verfügbaren Rechenleistung würde mehrere Jahrzehnte arbeiten, um einen einzigen Schlüssel zu errechnen. Allerdings ist die Gefahr nie ganz auszuschliessen, dass es einem genialen Mathematiker dennoch gelingt, sich in dieses Signierprozedere einzuhacken und die Schlüssel auf irgendeine Weise schneller zu berechnen.

Auch wenn die eigenhändige Unterschrift – wie sie heute gilt - selbst nicht hundertprozentig vor Fälschungen sicher ist, dürfte das gesamtwirtschaftliche Schadenspotential bei ihr doch geringer sein, als bei der elektronischen Signatur, die sich - einmal geknackt - ohne nennenswerten Aufwand beliebig oft von neuem fälschen lässt. Ob die beiden Unterschriftsformen nach Einführung des neuen Art. 15a OR durch das Bundesgesetz über die elektronische Signatur -BGES; seit dem 17.1.2001 in der Vernehmlassung, Botschaft des Bundesrates am 3.7.2001 verabschiedet (SigG2001) - daher zu Recht gleichgesetzt werden, ist in der Lehre umstritten. Insbesondere erscheint in diesem Zusammenhang die neue Haftungsregelung als relativ problematisch: wer die Chip-Karte, auf welcher der private Schlüssel gespeichert ist, ungenügend sichert, soll für allfällige Missbräuche der Signatur grundsätzlich haften. Behauptet dieser Inhaber, dass sein privater Signaturschlüssel „ohne seinen Willen“ zum Einsatz gelangt ist, so soll er dafür die Beweislast tragen und nachweisen, dass er seine gesetzlichen Sorgfaltspflichten erfüllt hat.

Das alles bedeutet letztlich, dass es dank der Anerkennung der elektronischen Signatur zwar in Zukunft einfacher wird, in einem Streitfall die Herkunft einer elektronischen Erklärung zu beweisen. Es drohen aber Schlupflöcher, welche die gewonnene Rechtssicherheit wieder

zunichte machen könnten. Bleibt diese auf die Dauer zu gross, wird das BGES der Wirtschaft nicht die erwartete Unterstützung bringen.

6. Risikoverlagerung

Kehren wir zurück zum Unternehmen und den möglichen Risiken, mit denen es durch den Anschluss ans Internet konfrontiert ist. In vielen Fällen wird die Geschäftsleitung in fachlicher Hinsicht nicht in der Lage sein, die potentiellen Risiken zu beurteilen und die erforderlichen Massnahmen zu deren Abwendung zu ergreifen. Wie wir gesehen haben, läuft die Chefetage Gefahr, einer zivil- und strafrechtlicher Haftung zu unterliegen.

Allerdings steht ihnen die Möglichkeit einer Haftungsverlagerung offen, d.h. die Einschaltung eines geeigneten qualifizierten IT-Security-Unternehmens, welches die Sicherheitslage überprüft, auf dem Laufenden hält und der Geschäftsführung gegenüber Bericht erstattet. Aber aufgepasst: auch hier besteht eine Sorgfaltspflicht, die darauf gerichtet ist, ein geeignetes und seriöses Unternehmen zu finden und zu beauftragen und dabei sicherzustellen, dass dessen Arbeit in das eigene Berichtsystem einbezogen wird. Denn grundsätzlich bestehen hier die gleichen Zurechnungs- und Haftungsrisiken wie wir sie eben gesehen haben, sofern die IT-Spezialisten dem Unternehmen in einem Subordinationsverhältnis unterstehen. Jedoch hat das betroffene Unternehmen die Möglichkeit, etwaige Ersatzansprüche auf das Beratungsunternehmen abzuwälzen.

Letztlich stellt sich die Frage, ob Versicherungen eine Schadensabsicherung gegen diese Internet-Risiken anbieten: Stellen Sie sich vor, der Hack-Angriff auf den Server eines Unternehmens bewirkt, dass der Betrieb für mehrere Tage lahmgelegt wird und empfindliche Ertragseinbussen entstehen.

Herkömmliche Betriebsversicherungen schützen grundsätzlich nur physisches Eigentum bzw. nur dann auch Betriebsunterbrüche, wenn der Schaden durch äussere Einflüsse wie Feuer oder Wasser entstanden ist. Schäden aus dem Internet waren bisher durch keine Versicherungspolice gedeckt. Das ändert sich: letzten Herbst hat eine grosse schweizerische Versicherung eine neue E-Business-Versicherung lanciert, welche aus vier Gefahrenbausteinen besteht: Hacker und Viren, Missbrauch durch Mitarbeiter, widerrechtliche Publikationen sowie Rechtsstreitigkeiten.

Um allerdings einen bedarfsgerechten Versicherungsschutz anbieten zu können, muss zuerst eine Analyse der individuellen Risikosituation des zu versichernden Unternehmens erfolgen, und zwar in Bezug auf die verschiedenen Gefahren sowie die sich aus den jeweiligen Kunden- und Lieferantenbeziehungen ergebenden Haftungsgegebenheiten. Erst im Anschluss kann ein angemessener Risikoschutz überhaupt angeboten bzw. eine entsprechende Prämie berechnet werden.

Natürlich sind der Versicherbarkeit von IT-Risiken Grenzen gesetzt. Es gibt Schäden, deren Bewertung für den Versicherer objektiv nicht möglich ist – ich möchte hier insbesondere an die Imageschäden erinnern, die durch Hack-Angriffe entstehen, indem sie Kunden vor etwaigen Online-Geschäftsabschlüssen, Buchungen oder ähnlichen kompromittierenden Handlungen abschrecken. Die Gefahrenquellen nehmen ausserdem bei grösseren Unternehmen exponentiell zu, weshalb die Versicherungen im Moment eher auf KMU abzielen und die max. Versicherungssumme relativ gering ist (CHF 50‘000.--). Allerdings: ein Versicherungsschutz kann Sicherheitsmassnahmen nur ergänzen, nicht komplett ersetzen. Daher dürfen Risk-Management und vernünftige Schutzvorkehrungen nicht ausser Acht gelassen werden. Im Gegenteil: sie sind notwendige Bedingung für den Versicherungsschutz.

lic. iur. Patrik A. Häberlin, Rechtsanwalt