September 2001

Versicherbarkeit von Risiken des E-Commerce

Torsten Grzebiela
Albert-Ludwigs-Universität Freiburg, grzebiela@iig.uni-freiburg.de

In: Buhl, Hans Ulrich, u.a. (Hg.) 2001. *Information Age Economy*; 5. Internationale Tagung Wirtschaftsinformatik 2001. Heidelberg: Physica-Verlag

ISBN: 3-7908-1427-X

Versicherbarkeit von Risiken des E-Commerce

Torsten Grzebiela
Albert-Ludwigs-Universität Freiburg

Zusammenfassung: E-Commerce wird zunehmend von neuartigen Internet-Risiken bedroht. Versicherungen sind ein klassisches Instrument zur Risikotransformation. In diesem Kontext interessiert insbesondere die Versicherbarkeit von Internet-Risiken, die in diesem Beitrag klassifiziert und deren Eigenschaften anhand der entscheidungsorientierten Kriterien der Versicherbarkeit eingeschätzt werden. Eine Analyse existierender Versicherungsangebote ermöglicht Aussagen bezüglich der Versicherbarkeit gegen potentiellen Verletzungen einzelner Schutzziele.

Schlüsselworte: E-Commerce, Internet-Risiken, Risikoebenen, Versicherbarkeit, Schutzziele, Mehrseitige Sicherheit

1 Schadensszenarien und Schadensdimensionen

Dem E-Commerce, der das Betreiben von Geschäften über das weltweit offene Internet bezeichnet, werden hohe Umsätze und somit große Zukunftsperspektiven prognostiziert. Das Internet bietet folglich einerseits große Chancen, andererseits birgt es ein gewaltiges Schadenspotential in sich. Datenverluste durch Hackerangriffe oder Viren, Wirtschaftsspionage oder Profilbildung treffen sowohl Individuen als auch Unternehmen. So generierte die Distributed Denial of Service-Attacke am 8. Februar 2000 auf Yahoo, E-Bay und E-Trade einen Umsatzverlust von 250 Millionen US-$ [Welt00] und zog einen Börsenwertverlust in Höhe von 2,5 Milliarden US-$ nach sich [Hand00]. Die Ausbreitung des „I LOVE YOU“-Virus im Mai 2000 soll Schätzungen zufolge weltweit einen Gesamtschaden bis zu 30 Milliarden US-$ verursacht haben [heis00].

Die Konsequenzen des Verlusts unternehmenskritischer Daten können je nach Unternehmensgröße und Branche von enormen Ausmaß sein. Studien der Firma *Hewlett-Packard* zur Datensicherung belegen, dass die Kosten des Stillstandes, der Wiederbeschaffung oder entstandene Wettbewerbsnachteile etc. bis zu 7,3 Millionen US-Dollar pro Stunde betragen können. Die Untersuchung kommt weiter zu dem Ergebnis, dass bis zu 94% der Unternehmen bei einen Totalausfall ihrer Daten die nächsten zwei Geschäftsjahre nicht überleben würden [Vers99]. Eine aktuelle Studie von [KPMG01] zeigt, dass fast jedes zweite Unternehmen in Deutschland „Hacker“ als größtes Sicherheitsrisiko für sein E-Commerce-System

fürchtet. Bei 11 % der befragten Unternehmen ist es nach eigenen Angaben in den letzten zwölf Monaten zu Sicherheitsverletzungen gekommen. Hier handelt es sich nur um die entdeckten und gemeldeten Fälle. Die Dunkelziffer dürfte deutlich höher sein.

Sicherheitsmaßnahmen und Versicherungen gegen Internet-Risiken werden im Informationszeitalter zunehmend wichtiger. Seit kurzem werden in Deutschland spezielle Internet-Versicherungen angeboten. In diesem Kontext stellt sich die Frage, ob generell alle internetspezifischen Risiken versicherbar sind oder ob das Internet Risiken birgt, die nicht auf einen Versicherungsgeber überwälzt werden können.

2 Klassifikation von Risiken des Internet

Risikobegriff

Das Begriffsverständnis von Risiko ist in der Literatur nicht einheitlich [Mein97, S. 23]. Mittlerweile wird in der betriebswirtschaftlichen Risikotheorie nicht mehr versucht, Risiko zu definieren, sondern Risiko wird mit seinen wesentlichen Eigenschaften umschrieben [Helt94, S.2]. Die in diesem Beitrag verwendete zielorientierte Risikoauffassung sieht Risiko als Gefahr einer negativen Ziel- bzw. Erwartungsabweichung [Euck44; Hall86]. Dieses Verständnis ermöglicht im Gegensatz zu den verteilungsorientierten Definitionsansätzen auch die Berücksichtigung qualitativer Aspekte.

Risikoebenen und Internet

Den Chancen des E-Commerce stehen Risiken gegenüber, die einerseits nur eine Projektion altbekannter Risiken darstellen, andererseits aber auch einen neuen internetspezifischen Charakter aufweisen bzw. im Internet aufgrund der Globalität deutlich verschärft auftreten. Unter dem plakativen Begriff „Internet-Risiken“ lassen sich verschiedenartige Risiken subsummieren. Eine modellhafte Darstellungsform und Einteilung ist die in Abbildung 1 vorgenommene Abstraktion auf unterschiedliche Risikoebenen. Sie soll einer Klassifikation dienen, um die unterschiedlichen Dimensionen aufzuzeigen.

Die *technische Risikoebene* versucht, Risiken aus einer technischen Perspektive aufzuzeigen. Auf dieser Ebene untersuchen Angreifermodelle die Wirksamkeit spezieller Schutzmechanismen unter Berücksichtigung der einem potentiellen Angreifer unterstellten Stärke und Fähigkeiten [Pfit90]. Hier sind die fundamentalen Sicherheitsrisiken, die in Abschnitt 2.3 erläutert werden, zu nennen. Ebenso lassen

sich Hacker-, Viren-, oder Denial-of-Service (DoS)-Angriffe aber auch Systemrisiken dieser Ebene zuordnen.

Die *individuelle Risikoebene* stellt insbesondere die Risiken der Verletzung der Privatheit und Identität in den Vordergrund. Hier lassen sich zwei Dimensionen erkennen: Zum einen ist der einzelne Nutzer z.B. durch Missbrauch seiner persönlichen Daten und mögliche Profilbildung in seiner Privatheit bedroht. Privatheit wird hier als die Gesamtheit der Eigentumsrechte an den eigenen, personenbezogenen Daten aufgefasst [Eggs01]. Zum anderen existiert ein ähnliches Risiko auch bei Unternehmen, die einer Manipulation oder einem Diebstahls spezifischer Unternehmensinformationen (z.B. Kundendaten, Forschungsdaten) ausgesetzt sind. Derartige Daten sind oftmals kritische Erfolgsfaktoren der Unternehmung, die deren Überleben bestimmen. Privatheit, die in diesem Kontext die proprietären Rechte der Unternehmung an ihren spezifischen Informationen darstellt, ist folglich ein Ziel, das für Unternehmen und Organisationen von höchstem Stellenwert ist.

Die *ökonomische Risikoebene* benennt die wirtschaftlichen Auswirkungen, die sich beispielsweise unmittelbar in Umsatzeinbußen oder mittelbar in Imageverlust widerspiegeln. Hier sind zum einen die genannten mikroökonomischen Risiken zu nennen, zum anderen auch die makroökonomischen Risiken, die sich auf die gesamte Volkswirtschaft beziehen.

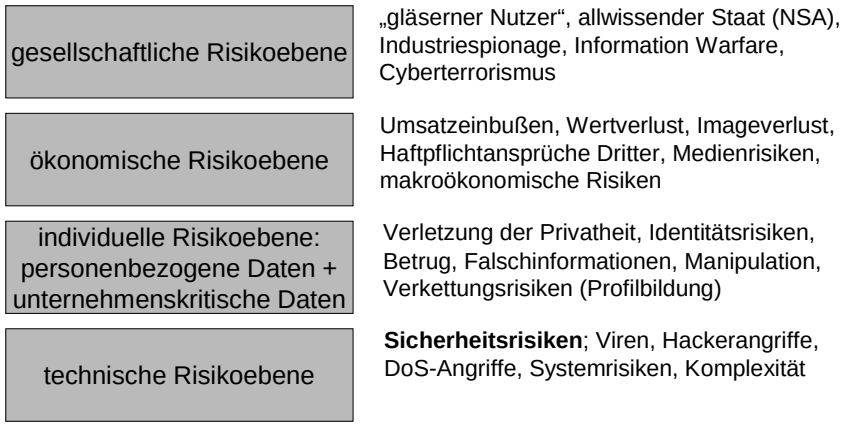

Abbildung 1: Risikoebenen

Die *gesellschaftliche Risikoebene* verdeutlicht die gesellschaftliche Dimension, die durch moderne Informations- und Kommunikationstechnologien und insbesondere durch das Internet entsteht. Cyberterrorismus, Information Warfare und der „gläserne Nutzer“ sind Stichworte, die die Gefahren umreißen. Aber auch ein „allwissender Staat“, eine international agierende National Security Agency

(NSA) sowie Industriespionage sind Gefahren, die gesellschaftliche Auswirkungen haben.

Die beschriebenen Risikoebenen lassen sich nicht eindeutig voneinander abgrenzen. So gibt es Rückkopplungen und Interdependenzen zwischen den einzelnen Ebenen. Deutliche Interdependenzen sind insbesondere bei der individuellen und der ökonomischen Risikoebene erkennbar. Der Abgrenzung dient vornehmlich das Kriterium der Auswirkung. Betrachtet wird hier z.B. die Auswirkung des Verlustes spezifischer Daten oder gezielter Hackerangriffe.

3 Mehrseitige Sicherheit als Referenz

Für die Untersuchung spezifischer Internet-Risiken bietet sich das Konzept der Mehrseitigen Sicherheit an [MüPf97]. Um der Grenzenlosigkeit des Mediums Internet als Marktplatz für E-Commerce gerecht zu werden, bedarf es bei der Analyse der Sicherheit neben der Betrachtung externer Angreifer auch der Einbeziehung aller anderen beteiligten Parteien als potentielle Angreifer [RaPf96; RaPf97]. Mehrseitige Sicherheit fordert somit die Berücksichtigung der Sicherheitsanforderungen aller beteiligten Parteien. So soll möglichst jeder gegen jeden geschützt sein.

Die aus technischer Sicht abgeleiteten Sicherheitsrisiken können als Fundament für weitere individuelle, ökonomische oder gesellschaftliche Internet-Risiken gemäß den Risikoebenen in Abbildung 1 angesehen werden und ergeben sich entsprechend obiger Anforderungen als Bedrohungen der sog. *Schutzziele* der Mehrseitigen Sicherheit [Rann98]:

- Verlust der Vertraulichkeit, d.h. das Risiko des unbefugten Informationsgewinns: Informationen über die Identität und die Präferenzen einzelner Nutzer, vertrauliche Unternehmensdaten (z.B. Informationen aus Forschung und Entwicklung, kritische Geschäftsdaten wie Kundendateien etc.) oder Kommunikationsdaten sollen vor unbefugter Einsicht bzw. Diebstahl sicher sein. Angriffe auf die Vertraulichkeit haben folglich zum Ziel, Informationen zu erhalten ohne diese zu verändern (passive Angriffe). Beispiele sind neben dem gezielten Hacking insbesondere bei der Datenübertragung sog. packet sniffer, die unverschlüsselte Nachrichteninhalte abhören können oder cookies, mit deren Hilfe sich Nutzerprofile erstellen lassen.
- Verlust der Integrität, d.h. das Risiko der unbefugten Modifikation von Informationen und Daten: Fälschungen von Nachrichteninhalten wie z.B. Unternehmensangebote oder Bestellungen sollen erkannt werden. Angriffe auf die Integrität bei der Datenübertragung können durch Man in the middle-Attacken geführt werden, bei denen ein Angreifer zwei Kommunikationspartnern den jeweils anderen Partner vortäuscht.

- Verlust der Verfügbarkeit, d.h. das Risiko der unbefugten Beeinträchtigung der Funktionalität: Der Verlust der Verfügbarkeit des Online-Auftritts eines Unternehmens im Internet beispielsweise, der allen nutzungsberechtigten Partnern jederzeit die Kommunikation bzw. einen Informationszugriff ermöglichen soll, wirkt geschäftsschädigend. Angriffe auf die Verfügbarkeit können z.B. mittels Distributed-Denial-of-Service-Attacken ausgeführt werden. Hier greifen gleichzeitig viele verschiedene unwissende Server an und bewirken den Systemabsturz der angegriffenen Zielrechner durch Überflutung.
- Verlust der Zurechenbarkeit, d.h. das Risiko der unzulässigen Unverbindlichkeit: Die Möglichkeit der Nachweisbarkeit, dass eine Instanz eine Nachricht gesendet hat, soll für den Empfänger gegenüber einem Dritten bestehen. Vorgänge, die nicht eindeutig einem Initiator zugerechnet werden können, können zu verantwortungslosem Handeln und zu nicht nachweisbaren Schadenersatzansprüchen, z.B. aufgrund der Verbreitung von Falschinformationen, führen. Angriffe auf die Zurechenbarkeit werden beispielsweise durch sog. Maskerade-Angriffe getätigt, bei denen falsche Identitäten vorgetäuscht werden. In diesem Kontext ist auch die Gefahr des IP Spoofing zu nennen, bei dem der Angreifer Pakete mit falscher IP-Adresse generiert und sich so als falscher Rechner ausgibt.

4 Versicherungen zur Risikotransformation

Sicherheit, Vertrauen und Versicherung

Die Handhabung der Sicherheitsrisiken und der weiteren resultierenden Internet-Risiken ist von zentraler Bedeutung für den E-Commerce. Mit geeigneten technischen Sicherungsmaßnahmen kann den Sicherheitsrisiken nur teilweise begegnet werden [FePf97]. Neben der notwendigen technischen Sicherheit ist für einen prosperierenden E-Commerce der Aufbau und die Aufrechterhaltung von Vertrauen ein zusätzliches zur technischen Sicherheit komplementäres Erfordernis [Eggs01; EgMü01], da Vertrauensprobleme zu den größten Hürden des E-Commerce zählen [EgEn00]. Die Reduktion verbleibender Risiken erfordert folglich den Einsatz nicht-technischer Instrumente. Hier lassen sich neben Versicherungen als ein ökonomisches Mittel zur Schadensvorsorge auch institutionelle Lösungsansätze nennen, die der Vertrauensbildung dienen. Ein Beispiel dafür sind die Schlüsselzertifizierung und Schlüsselinfrastrukturen (Public Key Infrastructures). Diese Mechanismen dienen bei der Verwendung digitaler Signaturen u.a. der sicheren Zuordnung öffentlicher Schlüssel zu der jeweiligen Person. Aber auch Reputationsdienste, Inspektions- und Empfehlungsdienste sowie Konfliktlösungsdienste lassen sich hinsichtlich einer Vertrauensgenese nennen [EgMü01, S.38f].

Versicherung als Instrument des Risikomanagements

Ökonomische Maßnahmen zur Risikobewältigung lassen sich in die risikopolitischen Instrumente Risikovermeidung, Risikoüberwälzung, Risikoverminderung und das Selbsttragen bzw. die Bildung von Risikoreserven klassifizieren [Hall86].

Risikovermeidung impliziert ein generelles Unterlassen von Aktivitäten, die mit Risiken verbunden sind. Im Rahmen der *Risikoüberwälzung* kommt speziell die Überwälzung auf fremde Risikoträger durch Versicherung, durch allgemeine oder spezielle Vertragsbedingungen oder die Überwälzung aufgrund von Gesetzen in Frage. *Risikoverminderung* bezeichnet Maßnahmen, die die Wahrscheinlichkeit von schadenverursachenden Ereignissen (self-protection) oder deren Schadenswirkungen (self-insurance) verringern. Insbesondere sind hier die technischen Sicherungsmaßnahmen bei der Nutzung des Internets zu nennen. Beispielsweise kryptographische Verfahren, die bei der Übertragung von Daten bestehende Risiken verringern, digitale Signaturen und Zertifikate, die der Sicherstellung der Identität dienen, Virenscanner sowie Firewall-Konzepte, welche die Kommunikation zwischen dem internen Unternehmensnetz und dem Internet regulieren und unerlaubte Zugriffe auf das unternehmensinterne Netz abwehren. Ebenso Intrusion Detection-Systeme, die Firewalls sinnvoll durch automatische Erkennung und Abwehr von Angriffen in der Präventivabwehr ergänzen. Wenn Risiken weder durch technische Sicherungsmaßnahmen noch durch ökonomische Instrumente begegnet werden kann oder wenn es ökonomisch nicht sinnvoll ist, derartige Instrumente einzusetzen, wird das *Restrisiko selbst getragen*. Die Bildung von Risikoreserven kann in diesem Kontext sinnvoll sein.

Bedingungen der Versicherbarkeit von Internet-Risiken

Kriterien der Versicherbarkeit

Unabhängig davon, ob eine Nachfrage nach internetspezifischen Versicherungen besteht, ist es notwendig, die Bedingungen der Entstehung eines Versicherungsangebots bezüglich der Risiken des Internets zu untersuchen. Zur Prüfung der Versicherbarkeit wurden im Laufe der Zeit unterschiedliche Kriterienkataloge entwickelt [Luci79, S. 203ff]. Nachfolgend wird auf den häufig in der versicherungsökonomischen Literatur zitierten entscheidungsorientierten Katalog mit fünf Kriterien von *Karten* [Kart72] Bezug genommen. Die Kriterien, nach denen Risiken beurteilt werden können, sind Zufälligkeit, Eindeutigkeit, Schätzbarkeit, Unabhängigkeit und Größe.

Eigenschaften von Internet-Risiken anhand der entscheidungsorientierten Kriterien der Versicherbarkeit

Die Erfüllung des Kriteriums der *Zufälligkeit* fordert, dass ein den Versicherungsfall auslösendes Ereignis bei Vertragsabschluß ungewiß und unbeeinflußbar sein muß [Kart72, S. 287]. Ungewißheit verlangt den gleichen Informationsstand auf beiden Vertragsseiten (Gefahr der Adversen Selektion). Unbeeinflussbarkeit bezieht sich auf die typischerweise von bestehendem Versicherungsschutz ausgehenden Anreize, schadensverhütende Aktivitäten zu reduzieren (Problem des Moral Hazard [Holm79]). Schäden entstehen im Internet vorwiegend durch beabsichtigte Angriffe Dritter oder durch technische Defekte. Um dem Versicherungsnehmer den Anreiz zu nehmen, Schadensfälle absichtlich herbeizuführen bzw. seine Sorgfalt bezüglich Sicherheit zu vernachlässigen, verwenden Versicherungsgeber bestimmte Obliegenheiten sowie Versicherungsvertragskomponenten wie die Selbstbeteiligung des Versicherungsnehmers oder die Deckungssummenbegrenzung, um die Versicherungsleistung im Schadensfall zu begrenzen.

Das Kriterium der *Eindeutigkeit* verlangt, dass sowohl das Ereignis (der Eintritt des Schadensfalls) als auch die Schadenshöhe in objektiv nachprüfbarer Weise festgelegt werden können [Mugl80, S. 77]. Allerdings können erhebliche Probleme auftreten, da bei bestimmten Schäden, die durch die Nutzung des Internets auftreten können, das Vorliegen des Schadensfalls nicht objektiv nachweisbar ist. Ein Beispiel dafür ist die im Internet verstärkt auftretende Gefahr der Verletzung der Vertraulichkeit, für die es i.d.R. nur dann eine Beweismöglichkeit gibt, wenn ein objektiv nachweisbarer Folgeschaden entsteht, der einen unmittelbaren kausalen Zusammenhang mit der Vertraulichkeitsverletzung erkennen lässt [Blin96, S. 185]. Derartige Schäden, die sich infolge der Dominanz immaterieller Werte zum einen nur sehr schlecht quantifizieren lassen, können zum anderen sehr wohl materielle Schäden nach sich ziehen. Ein mögliches zeitliches Auseinanderfallen der Vertraulichkeitsverletzung und des erlittenen Vermögensschadens verschärft außerdem das Problem der Beweisbarkeit. Eine weitere Schwierigkeit bei Schäden, die einen immateriellen Charakter aufweisen, ergibt sich durch die unterschiedliche Wahrnehmungsintensität dieser Schäden durch verschiedene Individuen. Dies macht die Bestimmung einer objektiven Schadenshöhe und eine adäquate Versicherung nahezu unmöglich.

Das dritte Kriterium der *Schätzbarkeit* repräsentiert das Problem des unzureichenden Wissens. Ein Versicherungsgeber, der sowohl die durchschnittliche Schadenshöhe als auch die Schadenseintrittswahrscheinlichkeit schätzen muß, wird dabei subjektiv urteilen. In diesem Kontext wird oft als Grundbedingung der Versicherbarkeit angeführt, dass eine hinreichend große Zahl von Individuen potentiell durch gleichartige Risiken bedroht sein müssen [Rejd92, S. 24; Blin96, S. 185], damit der Versicherungsgeber das Gesetz der großen Zahlen zur Schätzung des Erwartungswertes der Versicherungsleistungen anwenden kann. Dies trifft bezüglich des Internet sicher zu.

Das Kriterium der *Unabhängigkeit* bezieht sich auf positiv korrelierte Risiken, die ausgeschlossen werden sollen, um einen Zufallsprozess der versicherten Schadensereignisse im Versicherungsbestand zu gewährleisten. Negativ korrelierte Risiken sind wünschenswert und werden daher nicht weiter betrachtet. Hinreichend stochastische Unabhängigkeit der einzelnen versicherten Risiken ist zentrale Voraussetzung für den Effekt des Risikoausgleichs im Kollektiv. Erleidet im Schadensfall ein großer Teil der Versicherten gleichzeitig einen Schaden, dann stellen die individuellen Schadensfälle keine unabhängigen Ereignisse mehr dar. Hier können Virenangriffe bzw. Fehler oder Lücken in weit verbreiteter Software bei vielen Anwendern, die diese Software nutzen, als Beispiele angeführt werden, die hochkorrelierte Einzelschäden verursachen (sog. Ansteckungsrisiken). Aber auch Distributed-Denial-of-Service-Angriffe, die zeitgleich viele Systeme treffen, können eine Kumulierung von Schäden nach sich ziehen. Solche Anhäufungen von Schadensereignissen, Kumule genannt, gefährden die Zahlungsfähigkeit des Versicherungsgebers im Schadensfall, wenn die auf einmal fällige hohe Schadensumme die individuellen Kapazitätsgrenzen des Versicherungsgebers deutlich übersteigen. Jedoch verdeutlicht die Praxis, das viele abhängige Risiken versichert werden (z. B. Versicherungen von Elementarereignissen). Gewisse Grenzen der Abhängigkeit sollten jedoch nicht überschritten werden.

Unter dem letzten Kriterium der *Größe* wird der höchstmögliche Schaden eines Einzelrisikos verstanden. Die Größe des zu versichernden Risikos ist ein schlecht quantifizierbares Kriterium, da die Versicherbarkeit von der Zeichnungskapazität der Versicherungswirtschaft bzw. der Zeichnungspolitik des Versicherungsgebers abhängt [Mugl80, S. 77]. Allerdings kann der maximal mögliche Schaden immer durch Deckungsabgrenzungen oder die Bereitschaft des Versicherungsgebers, nur einen bestimmten Prozentsatz der Gesamtschadenssumme in Deckung zu nehmen, eingeschränkt werden. Des Weiteren kann der Versicherungsgeber die Zeichnungskapazität mittels Rückversicherer zusätzlich ausweiten.

Grenzen der Versicherbarkeit

Generell betrachtet gibt es keine eindeutigen Grenzen der Versicherbarkeit bzw. sog. nicht-versicherbare Risiken [Eszl99]. Allerdings lässt sich beobachten, dass nicht für jedes Risiko eine Versicherung angeboten wird. Eine Erklärung dafür versucht der Ansatz von *Berliner* zu liefern, der die Nichtexistenz eines eindeutigen Versicherbarkeitsbereich mit der Existenz einer sog. grauen Zone begründet, die zwischen dem objektiven Versicherbarkeits- und Unversicherbarkeitsbereich liegt [Berl82; Berl88]. Diese graue Zone umfasst die Risiken, die aufgrund unterschiedlicher Risikoaversionen nicht alle potentiellen Versicherungsgeber decken wollen aber die durchaus von einigen policiert werden. Die Existenz der grauen Zone macht somit eine allgemeine Definition der Versicherbarkeit von Risiken unmöglich. Versicherbarkeit lässt sich folglich am besten mittels eines *empirisch-realistischen Ansatzes* beurteilen, der quasi die Realität der Versicherbarkeit abbildet [Eszl99; Eszl00]. Das Ziel einer solchen Untersuchung sind Aussagen zur

praktischen Versicherbarkeit, die in Abschnitt 4.2 hinsichtlich der Sicherheitsrisiken gemacht werden.

5 Versicherungsangebot gegen Internet-Risiken

„Traditionelles“ Versicherungsangebot

Dem Unternehmen als Versicherungsnehmer steht eine ganze Reihe von Versicherungen zur Verfügung, um Risiken von IT-Systemen finanziell abzusichern. Diese „traditionellen“ im Sinne von schon länger am Markt existierenden EDV- bzw. Elektronik-Versicherungen sind keine speziellen Versicherungen gegen inhärente Internet-Risiken; sie verschaffen dem Versicherungsnehmer aber dennoch die Möglichkeit, bestimmte Teilrisiken der Informationssicherheit abzusichern [Blin96, S. 194]. Sie bieten allerdings nur einen ziemlich restringierten Versicherungsschutz. Eine gute Übersicht dieser Versicherungsangebote liefert [DVSV92].

Die *Elektroniksachversicherung* bezeichnet die Versicherung der Hardware. In einer Art „Allgefahrendeckung“ sind hier alle Sachschäden abgedeckt, die direkt aus dem Abhandenkommen der versicherten Gegenstände oder aus nicht rechtzeitig vorhergesehenen Ereignisse resultieren können. Sie umfaßt außerdem fest installierte Datenträger sowie System-Programmdaten aus Betriebssystemen bzw. damit gleichzusetzende Daten. Die gespeicherten Daten sind von den Datenträgern losgelöst zu betrachten. Insofern sie nicht für die Grundfunktionen der versicherten Hardware notwendig sind, die von der Elektroniksachversicherung berücksichtigt werden, greift hier die *Datenträgerversicherung*. Diese steht in einem komplementären Verhältnis zur Elektroniksachversicherung, da hier die Beeinträchtigung der Hardware zwingende Voraussetzung für eine monetäre Kompensation ist [Blin96, S. 194f]. Die *Softwareversicherung*, die einer erweiterten Datenträgerversicherung entspricht, verleiht dem Deckungskonzept der Datenträgerversicherung eine neue Dimension, da hier für Schäden durch Löschung oder Manipulation der Daten eingestanden wird, ohne dass der Datenträger oder die Hardware beeinträchtigt wird. Versichert ist u.a. auch Vorsatz Dritter wie z.B. Sabotage oder Hacker- bzw. Virenangriffe. In einem Schadensfall werden dem Versicherungsnehmer grundsätzlich nur die Kosten ersetzt, die er für die Wiederbeschaffung der Datenträger sowie die Wiederherstellung der versicherten Daten aufwenden muß. Außerdem kennt die Softwareversicherung sehr restriktive Versicherungsbedingungen. Neben einem hohen Selbstbehalt für die Hardware ist die Versicherungssumme bei verlorengegangenen Daten begrenzt.

Im Rahmen einer *Elektronik-Mehrkostenversicherung* ersetzt der Versicherer die Kosten für Überbrückungsmaßnahmen, die durch den Ausfall der versicherten Anlagen infolge eines Sachschadens entstehen und die Leistungserbringung der

Unternehmung unterbrechen bzw. beeinträchtigen. Die *Elektronik-Betriebsunterbrechungs-Versicherung* leistet, wenn ein Ausfall von Unternehmensanlagen nicht überbrückt werden kann, und erstattet den entgangenen Gewinn und die laufenden Kosten. Zahlreiche Ausschlussklauseln verhindern die Anwendung der herkömmlichen Elektronik-Betriebsunterbrechungs-Versicherung bei Schäden, die nicht durch Störungen des unternehmensinternen Kommunikationssystems hervorgerufen werden, sondern ursächlich der Anbindung an das Internet zugerechnet werden können (z.B. ein Ausfall von Internet-Netzknoten). Allerdings werden schon vereinzelt erweiterte Deckungen gegen derartige unternehmensexterne Schadensursachen, wie beispielsweise auch gegen Stromausfall, angeboten.

Die *Vertrauensschadenversicherung* schützt vor Vermögensschäden, die durch vorsätzliche Handlungen der Mitarbeiter entstehen können. Die sog. *Computer-Missbrauchs-Versicherung* ist eine spezielle Form der Vertrauensschadenversicherung [Heid80]. Der Versicherungsschutz ist zeitlich und auf Schäden begrenzt, die in unmittelbarem Zusammenhang mit der Datenverarbeitung stehen. Da im Gegensatz zu Sachversicherungen keine konkreten Versicherungswerte bestimmt werden können, muss der Versicherungsnehmer ex ante eine risikoadäquate Versicherungssumme festlegen.

Im Verlauf der Verarbeitung und Übermittlung personenbezogener Daten mittels EDV können Verstöße gegen die Vorschriften des Bundesdatenschutzgesetzes (BDSG) dazu führen, dass das Unternehmen für daraus entstehende Vermögensschäden in Anspruch genommen werden kann. Mögliche Haftpflichtansprüche beziehen sich oft auf den Ersatz materieller Schäden aufgrund der Verletzung der Privatheit oder eines geschädigten Leumundes (z.B. Einkommensverlust, zurückgezogene Darlehenszusage). Da sich die exakte Schadenshöhe dabei oft kaum bemessen lässt, kommt es regelmäßig zu gerichtlichen Prüfungen des tatsächlichen Schadens. Die *Daten-Haftpflichtversicherung* dient der Abdeckung der Vermögensschäden, die aus derartigen gerichtlichen Prüfungen herrühren sowie der Erstattung nachgewiesener Schadenersatzansprüche. Die *Daten-Rechtschutzversicherung* kann als eine Art Ergänzung zur Daten-Haftpflichtversicherung für spezielle Prozesskostenrisiken, in denen die Daten-Haftpflichtversicherung nicht einspringt, gesehen werden.

Spezielle Internet-Versicherungen

Versicherungen, die Transaktionsrisiken des E-Commerce abdecken, werden am Markt angeboten. So bietet die *Gerling Speziale Kreditversicherungs-AG* mit *Trusted Trade* für Business-to-Business-Transaktionen und *Trusted Shops* für Business-to-Consumer-Transaktionen entsprechend integrierte Versicherungskonzepte an. Diese sollen jedoch hier nicht weiter erläutert werden. Auch Risiken, die sich aus der Unsicherheit von Zahlungstransaktionen im Internet ergeben und für die es erste Versicherungsansätze gibt (z.B. *Wire Card AG*), sollen nicht weiter betrach-

tet werden. Vielmehr werden Internet-Versicherungen betrachtet, die sich insbesondere den Sicherheitsrisiken widmen.
Die Kalkulation von Internet-Risiken erweist sich aufgrund mangelnder Erfahrungswerte von Schadenseintrittswahrscheinlichkeiten und durchschnittlicher Schadenshöhen oder dem Auftreten von Kumulen, die sich bei Ausfall- bzw. Störungsrisiken ergeben, als äußerst schwierig. Einige Internet-Risiken werden schon durch oben angeführte „traditionelle“ Versicherungsangebote abgedeckt. Trotz Kalkulationsschwierigkeiten werden am Markt auch erste Versicherungen speziell gegen Internet-Risiken angeboten.

Neben weiteren Anbietern von Internet-Versicherungen wie der WÜBA Versicherungs-AG, Zürich Versicherung, Gerling Allgemeine Versicherungs-AG, Winterthur Versicherungen, AON Jauch & Hübener oder Lloyd´s sollen hier beispielhaft einige Konzepte angeführt werden. Die Gothaer Versicherungen bietet seit Dezember 1999 in strategischer Allianz mit der secunet Security Networks AG eine Kombination aus zwei Versicherungen gegen Internet-Risiken an. Die „Gothaer secusure Internet-Versicherung“ deckt die durch die Zerstörung oder Manipulation der Homepage entstandenen Schäden und haftet für die durch Mißbrauch sensibler Daten wie z.B. Kreditkartennummern entstandenen Folgeschäden. Die integrierte „Gothaer Software-Betriebsunterbrechungsversicherung“ hingegen leistet Entschädigungen für Störungen, die durch den Verlust von Daten oder EDV-Programmen entstehen. Es sind neben der Wiederherstellung verlorengegangener Daten beispielsweise auch Imageschäden, Umsatzeinbußen und Haftpflichtansprüche Dritter versichert. Für den Abschluss der Versicherung ist die Aktualität der Sicherheitssysteme zwingende Voraussetzung. Diese wird mittels speziellem Zertifikat von secunet nachgewiesen. Ebenso sieht die Versicherungspolice die Durchführung regelmäßiger Audits vor, um das Zertifikat zu verlängern. Eine Alternative dazu ist der Abschluß eines Servicevertrages mit secunet, der die Aktualität der Sicherheitstechnologie garantiert.

Auch die *Marsh GmbH* bietet ein Versicherungspaket an, das nach eigenen Angaben sämtliche E-Commerce-Risiken wie etwa Betriebsunterbrechungen durch Manipulation von Hackern oder eigenen Mitarbeitern abdeckt. Netzwerkausfälle durch fehlerhafte Software oder Fehlfunktionen von Servern sind ebenso versichert wie Schäden, die Dritten durch Betriebsunterbrechungen im Internet entstehen. Sogar eventuelle Börsenwertverluste durch Hackerangriffe wie die anfangs erwähnten Distributed-Denial-of-Service-Angriffe am 8. Februar 2000 auf US-amerikanische Internet-Unternehmen sind in gewissen Grenzen versicherbar. Ein Sicherheitsaudit durch einen vom Versicherer vorgeschalteten Gutachter, der die technischen Sicherungsmaßnahmen des Unternehmens prüft, ist auch hier Voraussetzung. Das Versicherungspaket wird daraufhin für jeden einzelnen Kunden individuell geschnürt (Versicherungssumme, Prämienhöhe etc.).

Die Analyse von einerseits „traditionellen“ Versicherungsangeboten und andererseits speziellen neuartigen Internet-Versicherungen führt zu in Abbildung 2 angeführten Beurteilung der derzeitigen Versicherbarkeit von Internet-Risiken:

	Vertraulichkeit: Diebstahl von Informationen und Daten	**Integrität:** Manipulation bzw. Löschen von Informationen und Daten	**Zurechenbarkeit:** Nicht-zurechenbare Vorgänge / Verbreitung von Falschinformationen	**Verfügbarkeit:** Website nicht verfügbar / Beeinträchtigung der Funktionalität; kein Zugang
Versicherbarkeit	-	ja	-	ja
Problematik	eindeutig kausaler Zusammenhang, Beweisbarkeit, Quantifizierung	niedrige Deckungsgrenzen, kostenintensive techn. Sicherungsmaßnahmen	eindeutig kausaler Zusammenhang, Beweisbarkeit	niedrige Deckungsgrenzen, kostenintensive techn. Sicherungsmaßnahmen

Abbildung 2: Versicherungsmöglichkeiten für Unternehmen

6 Zusammenfassung und Ausblick

Technische Sicherungsmaßnahmen stehen in einem komplementären Verhältnis zu Versicherungen. I.d.R. ist ein gewisses Mindestmaß an technischen Schutzvorkehrungen neben klassischen Produktgestaltungselementen wie Selbstbeteiligungen oder Deckungsabgrenzungen notwendig, um Internet-Risiken erst versicherbar zu machen.

Eine Analyse der bestehenden Versicherungsangebote zeigt, dass potentielle Verletzungen von Integrität und Verfügbarkeit versicherbar sind. Die Problematik liegt abgesehen von den erforderlichen kostenintensiven technischen Sicherungsmaßnahmen in verhältnismäßig niedrigen Deckungsgrenzen. Ein Lösungsansatz ist die Ausdehnung der Kapazitätsgrenzen der Versicherungsgeber mittels Rückversicherung. Des Weiteren können Ineffizienzen bzw. Grenzen der Versicherungen mit innovativen Risikofinanzierungslösungen, den Alternative Risk Transfer-Produkten, begegnet werden [Rome00]. Diese Produkte eignen sich insbesondere für Risiken, die auf den bestehenden Versicherungsmärkten nicht oder nur sehr teuer transferiert werden können. Hier besteht aktueller Forschungsbedarf. Die Bedrohung des Verlustes der Zurechenbarkeit lässt sich aufgrund äußerst schwieriger Beweisbarkeit und fehlenden eindeutigen kausalen Zusammenhängen kaum versichern. Der Lösungsansatz, Verletzungen der Zurechenbarkeit versicherbar zu machen, ist ein weit verbreiteter Einsatz von Verfahren der digitalen Signatur und digitalen Zertifikaten, die von vertrauenswürdigen Instanzen vergeben werden. Z.Zt. kann von verbreitetem Einsatz allerdings nicht die Rede sein. Verletzungen der Vertraulichkeit letztlich sind nicht versicherbar. Illegaler Informationsabfluß

bei Unternehmen oder illegale Veräußerung personenbezogener Daten werden i.d.R. zunächst „nicht am eigenen Leib erlebt“. Der Datenverlust ist – wenn überhaupt – oft erst im Nachhinein feststellbar. Eine Beweisbarkeit und die Identifizierung von Schuldigen ist äußerst schwierig bzw. sehr oft nicht möglich. Ebenso ist die exakte Quantifizierung der entstandenen Vermögensschäden kaum möglich. Ein Unternehmen, das bei der Markteinführung eines nahezu identischen Konkurrenzproduktes, das noch vor dem eigenen entwickelten Produkt präsentiert wird, feststellt, dass es zu Informationsabfluss gekommen sein muss, wird den daraus entstandenen Schaden nur schwerlich abschätzen können. Es ist ebenso anzunehmen, dass sich aufgrund der stark eingeschränkten Beweisbarkeit und Quantifizierungsproblematik die angesprochenen Risiken der Verletzung von Privatheit nicht versichern lassen.

Literatur

[Berl82] Berliner, Baruch: Die Grenzen der Versicherbarkeit von Risiken. Schweizerische Rückversicherungsgesellschaft, Zürich 1982.

[Berl88] Berliner, Baruch: Versicherbarkeit. In: Farny, Dieter, et al. (Hrsg.): Handwörterbuch der Versicherung, VVW, Karlsruhe 1988, S. 951-958.

[Blin96] Blind, Knut: Allokationsineffizienzen auf Sicherheitsmärkten: Ursachen und Lösungsmöglichkeiten; Fallstudie: Informationssicherheit in Kommunikationssystemen. Lang, Frankfurt am Main et al. 1996.

[DVSV92] Deutscher Versicherungs-Schutzverband: Wie Sie Ihre EDV-Risiken richtig versichern – Eine Anleitung für Betriebe. 2. Auflage, Bonn 1992.

[EgEn00] Eggs, Holger; Englert, Jürgen: Electronic Commerce Enquête 2000 – Vernetzte kleine und mittlere Unternehmen. Konradin-Verlag, Leinfelden-Echterdingen 2000.

[EgMü01] Eggs, Holger; Müller, Günter: Sicherheit und Vertrauen: Mehrwert im E-Commerce. In: Müller, G., Reichenbach, M. (Hrsg.): Sicherheitskonzepte für das Internet. Springer-Verlag, Berlin et al. 2001, S. 27-44.

[Eggs01] Eggs, Holger: Vertrauen im Electronic Commerce: Herausforderungen und Lösungsansätze, zugl. Dissertation, Universität Freiburg, 2001.

[Eszl99] Eszler, Erwin: Versicherbarkeit und ihre Grenzen. Analyse und Systematisierung auf erkenntnistheoretisch-ontologischer Basis. VVW, Karlsruhe 1999.

[Eszl00] Eszler, Erwin: Versicherbarkeit und ihre Grenzen: Logik – Realität – Konstruktion. In: Zeitschrift für die gesamte Versicherungswissenschaft (2000), S. 285-300.

[Euck44] Eucken, Walter: Die Grundlagen der Nationalökonomie. 4. Auflage, Fischer, Jena, 1944.

[FePf97] Federrath, Hannes; Pfitzmann, Andreas: Bausteine zur Realisierung mehrseitiger Sicherheit. In: Müller, G., Pfitzmann, A. (Hrsg.): Mehrseitige Sicherheit in der Kom-

munikationstechnik, Bd. 1: Verfahren, Komponenten, Integration. Addison-Wesley-Longman, Bonn et al. 1997, S. 83-104.

[Hall86] Haller, Matthias: Risiko-Management – Eckpunkte eines integrierten Konzeptes. In: Jacob, H. (Hrsg.): Schriften zur Unternehmensführung – Risiko-Management. Gabler, Wiesbaden 1986, S. 7-44.

[Hand00] Handelsblatt vom 11./12.2.2000.

[Heid80] Heidinger, Jan L.: Die Computer-Missbrauchs-Versicherung. VVW, Karlsruhe 1980.

[heis00] o.V.: US-Politiker kritisieren Software-Industrie. In: heise online news, http://www.heise.de/newsticker/result.xhtml?url=/newsticker/data/chr-11.05.00-001/, Abruf am 2001-05-30.

[Helt94] Helten, Elmar: Die Erfassung und Messung des Risikos. In: Asmus, W., Gassmann, J. (Hrsg.): Versicherungswirtschaftliches Studienwerk, 4. Aufl., Studientext 11, Wiebaden 1994.

[Holm79] Holmström, Bengt: Moral Hazard and Observability. In: Bell Journal of Economics, 10/1979, S. 74-90.

[Kart72] Karten, Walter: Zum Problem der Versicherbarkeit und zur Risikopolitik des Versicherungsnehmers – betriebswirtschaftliche Aspekte. In: Zeitschrift für die gesamte Versicherungswissenschaft (1972), S. 279-299.

[KPMG01] KPMG: efr@ud.survey. Umfrage zur Wirtschaftskriminalität im eCommerce. KPMG-Studie Integrity Services, Februar 2001, http://www.kpmg.de/library/surveys/satellit/efraud.pdf, Abruf am 2001-05-30.

[Luci79] Lucius, Ralph-René: Die Grenzen der Versicherbarkeit. Haag und Herchen, Frankfurt am Main 1979.

[Mein97] Meinecke, Hubertus: Integriertes Risiko-Management für Unternehmenseigentümer. St. Gallen 1997.

[MüPf97] Müller, Günter, Pfitzmann, Andreas (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Bd. 1: Verfahren, Komponenten, Integration. Addison-Wesley-Longman, Bonn et al. 1997.

[Mugl80] Mugler, Josef: Risikopolitische Strategien im Grenzbereich des Versicherbaren. In: Zeitschrift für die gesamte Versicherungswissenschaft (1980), S. 71-87.

[Pfit90] Pfitzmann, Andreas: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz. Springer, Berlin, Heidelberg 1990.

[Rann98] Rannenberg, Kai: Zertifizierung mehrseitiger IT-Sicherheit: Kriterien und organisatorische Rahmenbedingungen. Vieweg, Braunschweig, Wiesbaden 1998.

[RaPf96] Rannenberg, Kai; Pfitzmann, Andreas, Müller, Günter: Sicherheit, insbesondere mehrseitige IT-Sicherheit. In: Informationstechnik und technische Informatik (it+ti), Heft 4/1996, S. 7-10.

[RaPf97] Rannenberg, Kai; Pfitzmann, Andreas, Müller, Günter: Sicherheit, insbesondere mehrseitige Sicherheit. In: Müller, G., Pfitzmann, A. (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Bd. 1: Verfahren, Komponenten, Integration. Addison-Wesley-Longman, Bonn et al. 1997, S. 21-27.

[Rejd92] Rejda, George E.: Principles of Risk Management and Insurance, 4. Aufl., HarperCollins, New York 1992.

[Rome00] Romeike, Frank: IT Risiken und Grenzen traditioneller Risikofinanzierungsprodukte. In: Zeitschrift für Versicherungswesen, Heft 17/2000, S. 603-610.

[Vers99] o.V.: Dem „Data loss“ folgt oft das Aus. In: Versicherungswirtschaft, Heft 20/1999, S. 1482.

[Welt00] Die Welt vom 19.4.2000.