IT-Risiken im Schadenversicherungsmodell: Implikationen der Marktstruktur

Rainer Böhme

Technische Universität Dresden
Institut für Systemarchitektur
rainer.boehme@inf.tu-dresden.de

Abstract: Versicherungen gelten als geeignetes Mittel um Schäden durch Computerpannen finanziell abzufedern und um gleichzeitig Anreize zur Konstruktion sicherer Computersysteme zu schaffen. Allerdings führt eine starke Dominanz weniger Systemplattformen zu Schadenkorrelationen, die nur unter Prämienaufschlägen wirtschaftlich versichert werden können. Dieser Beitrag beleuchtet anhand eines Schadenversicherungsmodells die Versicherbarkeit von IT-Risiken bei konzentrierter Anbieterstruktur. Dabei wird eine Prämiendifferenzierung für Nutzer einer dominierenden bzw. einer alternativen Plattform diskutiert. Ein Kostenvorteil für Nutzer wenig verbreiteter Plattformen könnte zu einer ausgeglicheneren Marktstruktur führen, indem er ein Gegengewicht zu den starken Skaleneffekten verbreiteter Plattformen bildet.

1 Ökonomie der Computersicherheit

Es ist weithin bekannt, dass Sicherheitslücken in Computersystemen jährlich einen immensen wirtschaftlichen Schaden verursachen, auch wenn das wahre Ausmaß kaum durch seriöse Schätzungen beziffert werden kann. Mangelnde Computersicherheit hat jedoch nicht nur wirtschaftliche Konsequenzen, sondern mitunter auch ökonomische Ursachen. Ross Anderson [And01] begründet dies mit der Feststellung, dass weder Hersteller noch Nutzer Anreize haben, in ihrem Verantwortungsbereich angemessen in Schutzmaßnahmen zu investieren.

1.1 Versicherung von IT-Risiken

Die Informatik und verwandte Disziplinen stellen eine Vielzahl an technischen Schutzmaßnahmen für alltägliche Probleme der Computersicherheit bereit. Diese können ihre Wirkung allerdings nur dann entfalten, wenn sie effektiv eingesetzt werden. Genau dies geschieht offenbar wegen fehlender Anreize zu selten [And94b]. Deshalb liegt es nahe, Computersicherheit nicht nur mit technischen Hilfsmitteln anzustreben, sondern auch die ökonomischen Aspekte zu berücksichtigen. So argumentiert der Ökonom Hal Varian [Var00], dass zunächst die Haftung für Schäden an die Partei übergehen müsste, die sie am einfachsten vermeiden kann. So müssten Hersteller für ihre Produkte haften, aber auch Netzknoten – bis hin zum Anwender – zur Verantwortung gezogen werden, wenn sie ih-

ren Wartungspflichten nicht nachkommen[1]. In einem zweiten Schritt müssten diese „neuen Risiken" übertragbar sein, so dass sich alle Parteien gegen mögliche Regressforderungen versichern können. Die Bewertung der Risiken würde dann in einem Marktmechanismus erfolgen, der bei ausreichender Liquidität automatisch effizient ist.

Neben dem augenscheinlichen Vorteil, der finanziellen Abfederung von Sicherheitsrisiken, offenbart eine Reflektion über das Versicherungsmodell drei weitere interessante Unteraspekte: *Erstens* werden Versicherungsanbieter die Prämien nach unterschiedlichen Risikokriterien differenzieren. Das schafft konkrete Anreize zur Investition in Sicherheitstechnologie [YD02]. Dabei ist offensichtlich, dass eine Prämienreduktion nur für tatsächlich wirksame Sicherheitsmaßnahmen gewährt werden kann. Damit wird, *zweitens*, der Wert von Sicherheitsmaßnahmen besser quantifizierbar. Dies verhindert eine Überinvestition in Sicherheitstechnologie auf militärisches Niveau [And94a], und reduziert gleichzeitig den Einsatz von design-immanent wirkungslosen Lösungen, die aus irrationalen Gründen (subjektives Sicherheitsgefühl, Sichtbarkeit von Sicherheit, Orientierung an Branchenstandards) verbreitet sind [Sch04b]. Der *dritte* Aspekt betrifft die Forschung und Entwicklung von Sicherheitstechnologie: Um die versicherten Risiken zu bewerten und mit angepassten Prämien zu übernehmen, müssen Versicherungsunternehmen Informationen über die Art und den Grad einzelner Risiken einholen. Sie haben also einen Anreiz, einen Teil ihrer Gewinne in die Verbesserung ihrer Informationslage – und damit in die Verbesserung ihres Angebots an Deckung – zu reinvestieren. Versicherungsunternehmen können also unabhängige Code-Reviews und Labortests nachfragen, deren Ergebnisse wiederum zu sichereren Produkten führen. Sie können selbst Technologieentwicklung finanzieren, um Risiken zu minimieren und Schadensummen zu reduzieren [KY94, Ins04].

Versicherungen sind also ein durchaus geeignetes Mittel zum Umgang mit IT-Risiken. Allerdings konzentriert sich die Betrachtung in der Literatur bislang auf die Perspektive einzelner Versicherungsnehmer. Der vorliegende Beitrag untersucht dagegen die Situation aus der Sichtweise eines Versicherungsunternehmens, das die Gesamtheit der versicherten Risiken schließlich übernehmen muss. Dies erfolgt unter Berücksichtigung der besonderen Marktstruktur im IT-Sektor.

1.2 Besonderheiten der Marktstruktur

Bei der Untersuchung der Marktstruktur in der Informationstechnologie stellt man, je nach Definition des Marktabgrenzungskriteriums, eine im Vergleich zu anderen Branchen außerordentlich starke Dominanz des jeweiligen Marktführers fest. Diese Konzentration von Marktmacht lässt sich mit ökonomischen Theorien aus den Besonderheiten der IT-Industrie, insbesondere der Softwareindustrie, erklären: Netzwerk-Externalitäten, vernachlässigbare Grenzkosten und Abhängigkeiten durch Komplementärprodukte verstärken sich gegenseitig in ihrer Wirkung, die Marktanteile zugunsten des Marktführers zu verschieben [SV98, And01].

[1] Es ist anzumerken, dass eine Durchsetzung bei Anwendern gegenwärtig realistischer erscheint, während eine Haftungsumkehr für Hersteller durch ihren revolutionären Charakter eher als Gedankenmodell zu verstehen ist. Der Umfang an Haftungsverschiebung ist allerdings für die Gültigkeit der folgenden Ausführungen irrelevant, da er lediglich die Dimension der Konsequenzen beeinflusst, nicht jedoch die Logik der Zusammenhänge.

Dieser Prozess konvergiert schließlich in eine Monopolsituation. Neben der aus wohlfahrtstheoretischen Betrachtungen bekannten Ineffizienz von Monopolen [Var99] verursacht diese Anbieterstruktur gleichzeitig eine „Monokultur", also eine geringe Diversität an installierten Systemen. Dies hat zur Folge, dass ein Großteil der heute im Einsatz befindlichen Rechentechnik die *gleichen* Schwachstellen und Fehler aufweist [Eco03]. So können Viren und Würmer neue Lücken systematisch ausnutzen und epidemieartig große Schäden verursachen, indem sie quasi *gleichzeitig* alle in einem Kommunikationsnetz zusammengeschlossenen Rechner angreifen.

Die zentrale Frage des vorliegenden Beitrags beschäftigt sich mit den Konsequenzen dieser Angriffskorrelation auf das Versicherungsprinzip. Dabei soll anhand eines einfachen Schadenversicherungsmodells geklärt werden, ob IT-Risiken unter der Prämisse von starken Schadenkorrelationen überhaupt versicherbar sind. D.h., gibt es ein Geschäftsmodell mit dem Versicherungsunternehmen Deckung gegen Schäden durch Viren und Hacker zu akzeptablen Prämien anbieten können? In einem zweiten Schritt wird dann der Fall einer Prämiendifferenzierung zwischen zwei Risikotypen vorgenommen und Prämien für Nutzer einer dominierenden Plattform mit denen einer unabhängigen, deutlich weniger verbreiteten Alternativplattform verglichen. Dadurch ist eine Abschätzung möglich, inwieweit Versicherungsprämien einen Anreiz zur Diversifizierung geben und damit ein Gegengewicht zu den oben genannten Konzentrationstendenzen darstellen können.

Das folgenden Kapitel 2 bietet zunächst einen Rückblick der einschlägigen Literatur, auf deren Grundlage in Kapitel 3 ein geeignetes Schadenversicherungsmodell entwickelt wird. Kapitel 4 beschreibt die Ergebnisse, die mit Hilfe dieses Modells ermittelt wurden. Das letzte Kapitel enthält neben einer weiterführenden Interpretation (Abschnitt 5.1) auch eine kritische Betrachtung der Modellannahmen sowie Fragestellungen für weitere Forschung auf diesem interdisziplinären Gebiet (Abschnitt 5.2).

2 Literaturrückblick

In diesem Kapitel wird auf drei Typen von Literatur verwiesen, die jeweils im Zusammenhang mit der in diesem Beitrag diskutierten Fragestellung stehen: Grundlagenliteratur zur ökonomischen Betrachtung von IT-Sicherheit[2], Fallstudien und Typologien zum Management von IT-Risiken sowie mathematische Grundlagen der Versicherungswirtschaft. Dem Verfasser sind dagegen bislang keine Publikationen bekannt, die sich speziell mit der Versicherung korrelierter IT-Risiken auseinander setzen.

2.1 Ökonomische Prinzipien für die Informationssicherheit

Grundlegende mikroökonomische Konzepte, wie Preisbildung unter bestimmten Markt- und Kostenstrukturen, finden sich z. B. bei [Var99] und werden für die Besonderheiten des IT-Sektors in [SV98] aufbereitet. Eine Anwendung dieser allgemeinen Theorien zur Softwareökonomie auf den Bereich der Computersicherheit ist in [And01] dokumentiert.

[2] Der Begriff „Sicherheit" bezieht sich hier und im Folgenden auf die Dimension *Security*, also der Sicherheit gegen intentionale Gegenspieler, und schließt damit die Bedeutung als „Fehlertoleranz" (*Safety*) explizit aus.

Diese und weitere Autoren [CW00, Var00] schlussfolgern, dass unsichere Softwareprodukte auf dem Markt zu günstig angeboten werden und ihre wahren Kosten erst durch negative externe Effekte zum Vorschein treten. So gefährden unsichere Netzteilnehmer nicht nur ihre eigenen Systeme, sondern auch die Allgemeinheit, indem sie unbeabsichtigt Viren verbreiten und fahrlässig verteilte Angriffe über ihre Rechner dulden. Diese gesellschaftlichen Kosten (Externalitäten) werden aber nicht den Verursachern zugeordnet, so dass Letztere wiederum keinen Anreiz haben, die Sicherheit ihrer Systeme zu verbessern.

Als Reaktion auf das Marktversagen entstand eine Reihe von Lösungsvorschlägen durch regulatorische Eingriffe: In [CW00] wird eine Steuer für unsichere Netzteilnehmer vorgeschlagen, andere Autoren setzten dagegen mit Markt- bzw. Auktionspreistheorien bei der Softwareentwicklung an [Sch04a, Ozm04].

Als Beispiel für Investitionsmodelle, die Kosten- und Nutzen von Sicherheitstechnologien auf betriebswirtschaftlicher Ebene betrachten, sei auf [GL02] und [Adk04] verwiesen.

2.2 Versicherungsmodelle für IT-Risiken

Der Übergang von Investitionsmodellen unter Unsicherheit zu Versicherungsmodellen ist fließend. Erste Vorschläge für reine Versicherungsmodelle befinden sich bei [And94a], folgende in [Var00, YD02, Sch04b, KMY04]. Der Fokus dieser Darstellungen liegt aber eindeutig auf der Nachfrageseite. Die Angebotsseite charakterisiert [Duf02] eher als Kunst denn als Wissenschaft, was unter anderem mit der mangelnden Verfügbarkeit empirischer Daten über IT-Schäden begründet wird.

Lawrence Gordon et al. beschreiben in [GLS03] eine Vorgehensweise zur Anwendung von *Cyber-Insurance*-Policen als Instrument des Risikomanagements. Die Autoren weisen bereits auf eine Anzahl von real existierenden Angeboten zur Versicherung von IT-Risiken hin. Sie unterscheiden dabei zwei Risikotypen (siehe auch [Ins04]):

- *Eigenschäden* entstehen beim Versicherungsnehmer selbst und umfassen bspw. Gewinnausfall durch Datenspionage, Zerstörung von Eigentum (inkl. Daten) sowie Betriebsunterbrechungen durch Hacker-Angriffe, Computerviren, Softwarefehler etc.
- *Drittschäden* sind Kosten, die Dritten durch Fehler im Verantwortungsbereich des Versicherungsnehmers entstehen, so z. B. Schäden durch weitergeleitete Computerviren, Vertragsstrafen aus Lieferverzug durch IT-Ausfälle, sowie Urheberrechts- oder Datenschutzverletzungen nach Spionagefällen.

Zum besseren Verständnis der Besonderheiten von IT-Risiken sei dieser Klassifikation nach Schadenstelle (Versicherungsnehmer, Dritte) eine weitere Unterscheidung nach Schadenursache angestellt: Hard- und Software sind in Policen gegen „klassische" Schäden, wie z.B. der Feuer- und Elementarschadenversicherung, bereits inbegriffen. Ähnliches gilt für Betriebsunterbrechungen. Davon zu unterscheiden ist dagegen die Versicherung von immateriellen Schäden (wie z. B. Datenverlust) und von Schäden, die durch logische Fehler oder Angriffe verursacht werden. Diese werden in der Versicherungswirtschaft als eine neue Art von Risiko bezeichnet und sind (momentan) entsprechend schwer zu versichern [Ins04, Duf02, KMY04].

Schadenkorrelationen sind grundsätzlich auch für die Versicherung herkömmlicher Risiken relevant: Damit lokal verankerte Versicherungsunternehmen trotz geographischer Korrelationen von bspw. Sturm- und Hochwasserschäden existieren können, findet ein Ausgleich auf einer übergeordneten Ebene in Form von Rückversicherungen statt. Dieser Schutz wird weltweit von wenigen Unternehmen angeboten, die durch internationale Diversifikation ihre Risiken dekorrelieren. IT-Risiken sind dagegen vermutlich global ähnlich geartet, so dass übergeordnete Ausgleichsbestrebungen keine fundamentale Verbesserung der Situation nahe legen. Nach [Duf02] haben viele Erstversicherer Anfang 2002 Schäden durch Computerviren auf Druck ihrer Rückversicherer aus klassischen Schadenversicherungspolicen ausgeschlossen, weil Letztere einen globalen „Cyber-Hurricane" nicht decken können. Deshalb werden Rückversicherungen hier nicht weiter betrachtet.

2.3 Grundlagen der Finanz- und Versicherungsmathematik

Im Versicherungsvertrag (*Police*) verpflichtet sich das Versicherungsunternehmen gegen einen festen, im voraus fälligen Geldbetrag (*Prämie*), bei Eintritt von vertraglich definierten ungewissen Ereignissen (*Schäden*) bestimmte Zahlungen zu leisten, die wiederum meistens von der Höhe des Schadens abhängen. Damit übernimmt das Versicherungsunternehmen ungewisse Zahlungen in der Zukunft gegen eine feste Prämie in der Gegenwart.

Grundlagen zur Versicherungsökonomie finden sich bei [BA92]. Als Kernthemen werden drei Phänomene behandelt: *Adverse Selection* (schlechte Risiken fragen eher Versicherungsschutz nach als gute), *Moral Hazard* (Nachlässigkeit der Versicherungsnehmer, da Schaden nicht selbst getragen werden muss) sowie die *Prämienberechnung*. Letztere ist Gegenstand einer umfangreichen Literatur zur Versicherungsmathematik [PW92, Sch02]. Dieses Gebiet wird wiederum in die Lebensversicherungsmathematik und die an dieser Stelle relevante Schadenversicherungsmathematik [Mac97] eingeteilt.

Allerdings wird in der Versicherungsmathematik häufig die Unabhängigkeit von Schadenereignissen vorausgesetzt [Mac97, S. 24] – eine Annahme, die gerade für die Betrachtung von IT-Risiken nicht plausibel erscheint. Die Betrachtung eines Bestandes korrelierter Risiken hat dagegen unter dem Begriff *Portfolio* in der Kreditrisikoforschung bereits Tradition [SA02, DS03, Hus04]. Deshalb wird das hier vorgestellte Modell mit Methoden aus der Kreditrisikomessung kombiniert.

3 Ein Schadenversicherungsmodell für Computersysteme

In der Versicherungsmathematik werden nicht Policen, die u. U. mehrere Risiken umfassen, sondern einzelne Risiken betrachtet. Diese werden als Zufallsvariablen R_i mit einer nicht-negativen Verteilung der Schadenhöhe modelliert. Eine Anzahl n gleichartiger Risiken wird dann zu einem *Bestand* zusammengefasst. Ein Bestand $B_n = (R_1, R_2, \ldots, R_n)$ ist dann ein Zufallsvektor der Länge n.

Die folgende Argumentation beschränkt sich auf die Betrachtung einer Periode (z. B. ein Jahr). Dazu wird angenommen, dass die Risiken einer Bernoulli-Verteilung mit dem Parameter p als Eintrittswahrscheinlichkeit folgen. Die Schadenhöhe im Schadenfall wird

konstant angenommen und auf den Wert 1 normiert.[3] Also gilt

$$\mathrm{P}(R = r) = \mathrm{P}(r) = p^r \cdot (1-p)^{1-r}, \qquad r \in \{0, 1\}. \tag{1}$$

Diese Verteilungsannahme bewirkt, dass in jeder Periode die Schadenzahl x gleich dem Gesamtschaden eines Bestands ist: $S = \sum_{i=1}^{n} R_i$. Wenn die Risiken $R_1, R_2, \ldots, R_n$ unabhängig sind, dann ist $S \sim \mathbf{B}(n; p)$ binomial verteilt. Die Verteilungsfunktion ist

$$\mathrm{P}(S = x) = W_p^n(x) = \binom{n}{x} p^x \, (1-p)^{n-x}, \tag{2}$$

ihr Erwartungswert $\mathrm{E}(S) = np$ und ihre Varianz $\mathrm{Var}(S) = np(1-p)$.

Damit ein Versicherungsunternehmen den mittleren Schaden pro Periode $\mathrm{E}(S)$ aus den Prämieneinnahmen begleichen kann, könnte $\mathrm{E}(S) = np$ als Prämie auf die n Risiken umgelegt werden. Das entspricht einer *Nettoprämie* von $H_\mathrm{N} = p$. Weil dieser Ansatz mit Punktschätzungen über den Erwartungswert argumentiert, würden die Prämieneinnahmen nach diesem Prinzip nur in der Hälfte der Fälle ausreichen, um alle Forderungen zu begleichen. Die Wahrscheinlichkeit für den *Ruin* des Versicherungsunternehmens wäre also mit $\mathrm{P}(S > n \cdot H_\mathrm{N}) = 0.5$ viel zu hoch [Sch02, S. 143]. Deshalb muss zusätzlich zu den Einnahmen aus den Nettoprämien $\mathrm{E}(S) = n \cdot H_\mathrm{N}$ Sicherheitskapital in Höhe c vorhanden sein, so dass $\mathrm{P}(S > n \cdot H_\mathrm{N} + c) \leq \epsilon$ eine gegebene Schranke für die maximale Ruinwahrscheinlichkeit unterschreitet.

Das notwendige Sicherheitskapital kann für ein gegebenes ϵ mit der Quantilfunktion Q der Binomial-Verteilung berechnet werden:

$$c = \lceil Q_p^n(1-\epsilon) \rceil - \mathrm{E}(S) = \lceil Q_p^n(1-\epsilon) \rceil - np \tag{3}$$

Da dieses Kapital im Mittel nicht verbraucht wird, müssen für seine Bereitstellung lediglich die Kosten in Form einer entgangenen Rendite in einer vergleichbaren Risikoklasse auf die Versicherungsprämien umgelegt werden. Weil alle Risiken gleichartig sind, erscheint eine paritätische Aufteilung des Schwankungszuschlags angebracht. Für die Bruttoprämie H_B gilt also:

$$H_\mathrm{B} = H_\mathrm{N} + A + z \cdot \frac{c}{n}, \tag{4}$$

wobei z den Marktzins für eine Anlage mit einem Risiko von minimal ϵ bezeichnet [Mac97, S. 27][4], und A eine Umlage der Verwaltungskosten darstellt, die im Folgenden als vernachlässigbar klein angenommen wird.

[3] Diese Modellannahme impliziert, dass ein Schaden in jeder Periode höchstens einmal entstehen kann. Das trifft bspw. bei Haftungsfällen durch Datenschutzverletzungen zu: Wenn kritische Informationen einmal öffentlich sind, verursacht eine weitere Verbreitung der selben Informationen keinen weiteren Schaden. Auch für anders geartete Risiken fällt die Vernachlässigung von Mehrfachschäden bei kleinen p kaum ins Gewicht, da Mehrfachschäden dann nur sehr selten vorkommen.

[4] ϵ ist eine Untergrenze, weil das Versicherungsunternehmen neben dem Schwankungsrisiko weiteren Unsicherheiten wie Markt- und operationellen Risiken ausgesetzt ist.

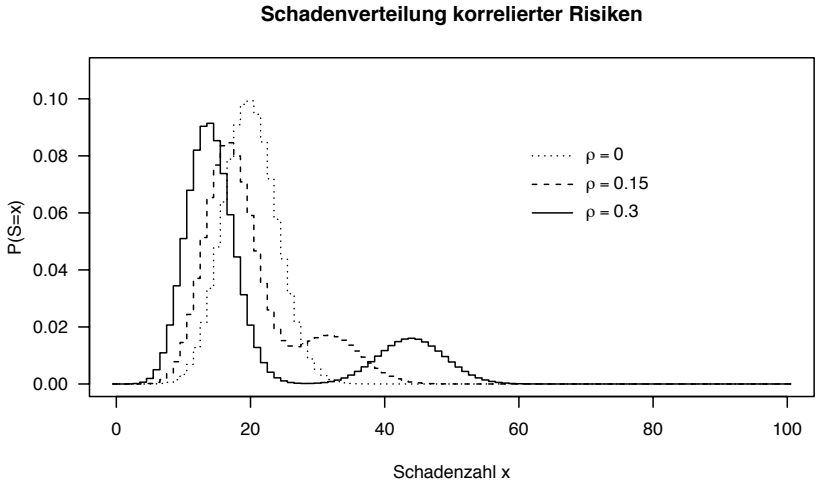

Abbildung 1: Schadenverteilung im Bestand in Abhängigkeit von ϱ mit $n = 100$ und $p = 0.2$

Ein konstituierendes Element der Versicherungsökonomie ist der *Ausgleich im Kollektiv*. Damit ist die durch den zentralen Grenzwertsatz begründete Degression des Schwankungszuschlags mit wachsender Anzahl *unabhängiger* Risiken in einem Bestand gemeint. Hier liegen also systembedingte Skaleneffekte vor: Versicherungsunternehmen mit großen Beständen können Deckung für neue Risiken zu günstigeren Bedingungen anbieten als solche mit kleinen Beständen.

Die Abhängigkeiten zwischen IT-Risiken werden über eine Korrelation ϱ der Einzelrisiken mit einer latenten Zufallsvariable modelliert, dem „systematischen Risiko" $R_0 \sim \mathbf{B}(1; p)$. Der Korrelationskoeffizient ϱ wird dazu als Produkt-Moment-Korrelation interpretiert:

$$\mathrm{Cor}(X, Y) = \frac{\mathrm{E}(XY) - \mathrm{E}(X)\mathrm{E}(Y)}{\sqrt{\mathrm{Var}(X)\mathrm{Var}(Y)}} \tag{5}$$

Speziell für die Bernoulli-Variablen R_0 und R_i gilt:

$$\varrho = \mathrm{Cor}(R_i, R_0) = \frac{\mathrm{P}(r_0 = 1 \wedge r_i = 1) - p^2}{p \cdot (1 - p)}, \qquad i = 1, \ldots, n \tag{6}$$

Daraus lassen sich die bedingten Wahrscheinlichkeiten für R_i in Abhängigkeit von R_0 formulieren:

$$p_{|0} = \mathrm{P}(r_i = 1 | r_0 = 0) = \frac{p - \mathrm{P}(r_i = 1 \wedge r_0 = 1)}{1 - p} = p - p \cdot \varrho \qquad \text{und} \tag{7}$$

$$p_{|1} = \mathrm{P}(r_i = 1 | r_0 = 1) = \frac{\mathrm{P}(r_i = 1 \wedge r_0 = 1)}{p} = p + (1 - p) \cdot \varrho\,. \tag{8}$$

Durch die Konstruktion der latenten Zufallsvariable R_0 ist die Verteilungsdichte des Gesamtschadens als Summe zweier Binomialverteilungen darstellbar:

$$\mathrm{P}(S = x) = p \cdot W^n_{p_{|1}}(x) + (1-p) \cdot W^n_{p_{|0}}(x) \tag{9}$$

mit der kumulierten Wahrscheinlichkeitsdichte

$$\mathrm{P}(S \leq x) = p \cdot \sum_{k=0}^{x} W^n_{p_{|1}}(k) + (1-p) \cdot \sum_{k=0}^{x} W^n_{p_{|0}}(k) \tag{10}$$

zur Berechnung des Schwankungszuschlags. Diese Verteilung ist für hohe Korrelationen bimodal und konvergiert im Grenzfall $\varrho = 0$ zur Binomial-Verteilung (s. Abbildung 1).

4 Ergebnisse

Im Folgenden wird das eben vorgestellte Schadenversicherungsmodell zur Beantwortung der Forschungsfragen verwendet. Dafür bedarf es zunächst einiger Annahmen über sinnvolle Parametervorgaben. Der Risikoparameter ϵ und die dazugehörige Kapitalverzinsung für das Sicherheitskapital z sind in der Praxis marktbestimmt und werden im Weiteren als $\epsilon = 0.005$ und $z = 0.1$ angenommen. Über die Stärke der Korrelation ϱ lassen sich bei der derzeitigen Datenlage keine validen Aussagen machen, so dass dieser Parameter in den weiteren Analysen mit verschiedenen Werten getestet wird. Auch die Bestandsgröße n soll nicht fixiert werden, da sie mitunter von der Marktdominanz der zu versichernden Plattform abhängt.

4.1 Versicherbarkeit von Monokulturen

Das vorgestellte Modell erlaubt für jeden Bestand B in Abhängigkeit von den Parametern n, p und ϱ die Berechnung einer Prämie, zu der Versicherungen angeboten werden können. Ob tatsächlich ein Markt für derartige Policen existiert, hängt demnach von der Nachfrageseite ab. Diese lässt sich durch ein einfaches Modell beschreiben, das die Gewinnerwartung eines nutzenmaximierenden, risikoaversen Wirtschaftssubjekts in zwei Zuständen gegenüberstellt (vgl. z. B. [Var99]). Dabei tritt der „Normalfall" mit einer Auszahlung von G_1 mit Wahrscheinlichkeit $1-p$ ein, und der „Schadenfall" mit $G_0 = G_1 - S$ mit Wahrscheinlichkeit p. Abbildung 2 visualisiert diese Auszahlungsstruktur.

Durch den Abschluss einer Versicherung zur vollständigen Deckung kann sich ein Wirtschaftssubjekt von Punkt N (keine Versicherung) zu Punkt V_{E} (Versicherung bei reiner Nettoprämie) auf ein höheres Nutzenniveau U_2 verbessern. Punkte mit gleichem Nutzen sind in der Abbildung als *Indifferenzkurven* gekennzeichnet. Dabei wird analog zu [KMY04] eine Nutzenfunktion der CRRA-Klasse[5] unterstellt. Diese streng monoton ansteigende Abbildung ordnet jeder Auszahlung y einen Nutzen zu

$$u(y) = \begin{cases} \frac{y^{1-\sigma}}{1-\sigma} & \text{für} \quad \sigma > 0, \sigma \neq 1 \\ \log(y) & \text{für} \quad \sigma = 1 \end{cases} \text{, so dass} \quad \sigma = -\frac{u''(y)}{u'(y)} \cdot y = const \tag{11}$$

[5] *Constant Relative Risk Aversion*, vgl. [Pra64]

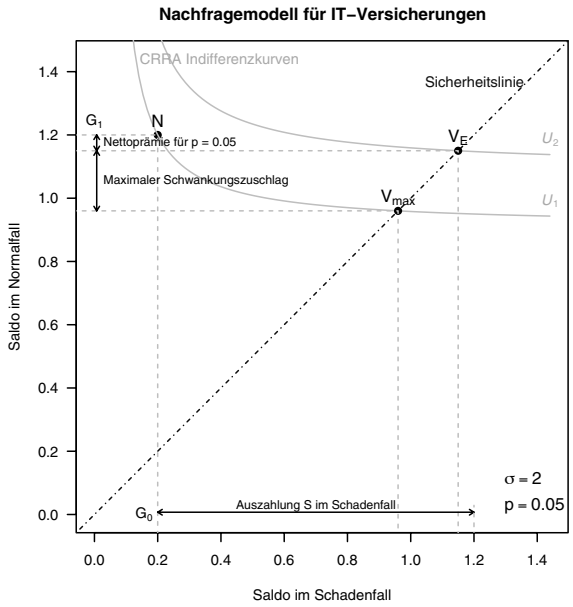

Abbildung 2: Modellierung im Zustandsdiagramm: Durch Abschluss einer Versicherung wird die Auszahlungsstruktur von Punkt N auf eine höheres Nutzenniveau im Punkt V_{E} gehoben. Die maximale Zahlungsbereitschaft für die Prämie ergibt sich am Schnittpunkt $V_{\max}$ der Sicherheitslinie mit der ursprünglichen Indifferenzkurve.

ein Maß der Risikoaversion ist. Ein Wirtschaftssubjekt wird solange (Teil-)Deckung nachfragen, wie es dadurch sein Nutzenniveau erhöhen kann. Eine obere Schranke für die Prämie ist durch Punkt $V_{\max}$ bestimmt, in dem sich die Sicherheitslinie mit der Indifferenzkurve U_1 durch N schneidet.

Durch eine Kombination des Nachfragemodells mit dem Schadenversicherungsmodell aus Kapitel 3 kann die maximale Korrelation ϱ für verschiedene Parameter numerisch berechnet werden. Tabelle 1 zeigt die Ergebnisse für 2×3 verschiedene Fälle: σ variiert dabei zwischen moderater Risikoaversion ($\sigma = 1$) und starker Risikoaversion ($\sigma = 3$). Die Auszahlung G_0 wird in drei Stufen verändert, nämlich hohe ($G_0 = 0.2$), mittlere ($G_0 = 1$) und geringe Schadeneinwirkung ($G_0 = 5$). Weil für dieses Szenario eine Monokultur angenommen wird, erfolgte die Berechnung der Wahrscheinlichkeitsdichte für $n \to \infty$ mit Hilfe einer Approximation.

Bei der Interpretation fällt auf, dass Versicherungsnehmer mit hoher Risikoaversion oder großen Schadenwahrscheinlichkeiten auf einem Versicherungsmarkt Deckung trotz möglicher Schadenkorrelation bekommen. Dies lässt sich durch das generell hohe Prämienniveau bei riskanten Unternehmungen bzw. durch die hohe Zahlungsbereitschaft risikoscheuer Wirtschaftssubjekte erklären: Die zusätzliche Belastung durch Schadenkorrelation fällt dann relativ nicht mehr so stark ins Gewicht.

Tabelle 1: Obergrenzen für Schadenkorrelationen ϱ

		Risikobereitschaft der Versicherungsnehmer					
		$\sigma = 1$			$\sigma = 3$		
Risiko p	$G_0 =$	0.2	1.0	5.0	0.2	1.0	5.0
0.01		0.11	0.04	0.01	1.00	0.20	0.03
0.05		0.55	0.19	0.05	1.00	0.89	0.16
0.10		1.00	0.37	0.09	1.00	1.00	0.31
0.20		1.00	0.73	0.18	1.00	1.00	0.60

Allerdings können bereits geringe Korrelationen in den orthogonalen Versicherungsprodukten eine Marktlösung verhindern. Gerade diese Produkte, kleine Policen gegen relativ unwahrscheinliche Schäden, könnten jedoch – bei hinreichendem Volumen – die Liquidität in diesem neuen Markt garantieren und somit zur Etablierung von IT-Versicherungen beitragen. Angesichts der eingangs dargestellten positiven Konsequenzen von IT-Versicherungen ist dieser Befund durchaus als dysfunktional zu bewerten.

4.2 Prämienstruktur als Anreiz zur Diversifizierung

Dieser Abschnitt beleuchtet die Auswirkung einer unterschiedlich starken Verbreitung von Systemplattformen auf die Prämien einer IT-Versicherung. Zu diesem Zweck werden zwei idealtypische Plattformen angenommen und jeweils in einem eigenen Bestand abgebildet: Die dominierende Plattform $\mathcal{D}$ ist durch einen großen Bestand ($n_\mathcal{D} \to \infty$) und eine Schadenkorrelation $\varrho_\mathcal{D} > 0$ gekennzeichnet. Die Alternativplattform $\mathcal{A}$ hat einen deutlich kleineren Bestand $n_\mathcal{A}$. Ihre Komponenten verursachen aber unkorrelierte Schäden. Diese Annahme ist plausibel, da sich bspw. ein Virus in einem heterogenen Netzwerk kaum ausschließlich über Komponenten von $\mathcal{A}$ verbreiten kann. Zudem haben Virenprogrammierer deutlich geringere Anreize eine wenig verbreitete Plattform zu berücksichtigen. Beide Plattformen seien gleich (un)sicher mit der Schadenwahrscheinlichkeit p.

Bei der Prämienberechnung ist nun interessant, ab welcher Korrelation $\varrho_\mathcal{D}$ die Alternativplattform $\mathcal{A}$ zu geringeren Kosten versichert werden kann, obwohl sie durch den kleinen Bestand nur einen unvollkommenen Ausgleich im Kollektiv erreicht. Abbildung 3 zeigt die Bedingungen für eine rechnerisch gleich hohe Bruttoprämie für verschiedene Schadenwahrscheinlichkeiten.

Alle Kombinationen $(n_\mathcal{A}, \varrho_\mathcal{D})$ rechts oberhalb der dargestellten Graphen führen zu einem Prämienvorteil für die Alternativplattform $\mathcal{A}$. Damit zeigt die quantitative Betrachtung von Sicherheitsaspekten erstmals einen Marktmechanismus auf, der im Gegensatz zu den bislang diskutierten softwareökonomischen Netzwerkeffekten keine Verbesserung der Kostenstruktur für den jeweiligen Marktführer impliziert. Inwieweit der hier entstehende Diversitätsbonus jedoch ausreicht, um die Kosten der Abweichung von der dominierenden Plattform zu kompensieren und somit den Automatismus zur „natürlichen Monokultur" zu durchbrechen, ist mit den an dieser Stelle getroffenen Annahmen und Modellen nicht entscheidbar.

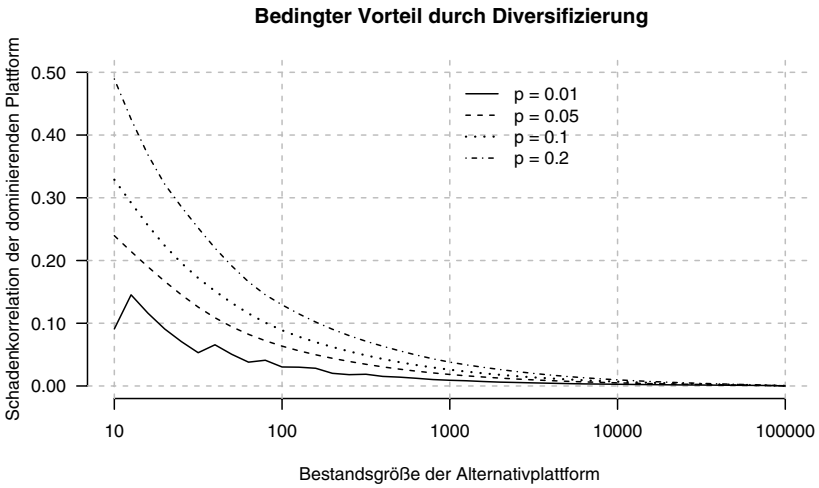

Abbildung 3: Punkte mit konstanter Bruttoprämie für die Systeme $\mathcal{D}$ und $\mathcal{A}$

Aus Abbildung 3 ist ebenfalls ersichtlich, dass immer eine gewisse Mindestbestandsgröße überschritten werden muss, bevor $\mathcal{A}$ günstiger zu versichern ist als $\mathcal{D}$. Außerdem ist zu erwarten, dass die Schwelle zusätzlich ansteigt wenn Verwaltungskosten A berücksichtigt werden, denn die Sicherheit jeder neuen Plattform muss vor einem Vertragsabschluss zunächst eingehend evaluiert werden. Diese Markteintrittsbarriere könnte eine Verschiebung der Gleichgewichtssituation von einer dominanten Plattform $\mathcal{D}$ zu einer Anzahl diverser Plattformen $\mathcal{A}_1 \ldots \mathcal{A}_m$ effektiv verhindern.

5 Diskussion

Der ökonomische Zugang zu Fragestellungen der Informationssicherheit allgemein, und speziell die Idee der Versicherung von immateriellen Risiken, sind viel versprechende Ansätze zur Schaffung einer zuverlässigeren Infrastruktur für die Informationsgesellschaft. Der vorliegende Beitrag soll jedoch darauf hinweisen, dass bewährte Konzepte aus der „Offline-Ökonomie" nicht unverändert in die „Online-Ökonomie" übertragen werden können. Durch Sicherheitslücken verursachte IT-Schäden dürfen wegen der Schadenkorrelationen bei der heutigen Struktur installierter Systeme nicht nach den Prinzipien der klassischen Schadenversicherungsmathematik behandelt werden.

5.1 Mögliche Konsequenzen

Die Existenz eines Versicherungsmarktes für IT-Risiken hat eine Reihe positiver Konsequenzen: Der Sicherheitsgewinn durch technische Maßnahmen wird monetär quantifizier-

bar, es entstehen zusätzliche Anreize zum sicheren Betrieb installierter Systeme sowie zur Entwicklung sicherer Systeme, und Anbieter alternativer Lösungen werden durch niedrigere indirekte Kosten zu Innovationen motiviert. Eine abschließende Bewertung dieser Konsequenz in Bezug auf die zu erwartenden Wohlfahrtseffekte bleibt dabei Aufgabe für weitere Forschung.

Bevor sich jedoch diese wünschenswerten Effekte realisieren lassen, sind einige Bedingungen zu erfüllen. *Erstens* ist eine rechtsverbindliche Haftungsregelung für immaterielle Schäden Grundvoraussetzung für die Entstehung eines breiten Marktes für IT-Versicherungen [Var00]. *Zweitens* zeigt die vorliegende Analyse, dass selbst dann Versicherungsschutz für einen beträchtlichen Teil des Bedarfs nicht angeboten werden könnte, weil strukturbedingte Schadenkorrelationen drohen. Möglicherweise können die positiven Folgen für den Gesamtmarkt also nur durch ergänzende Subventionen einzelner Teilmärkte erreicht werden. Diese Art von regulatorischen Eingriffen wird in den USA bereits diskutiert, dort allerdings aus anderen Gründen [KMY04].

Außerdem zeigen diese Überlegungen, dass die Entwicklung eines IT-Versicherungsmarktes – ob selbsttragend, subventioniert oder durch Versicherungspflichten durchgesetzt – von Verschiebungen in der Marktstruktur begleitet wird. Nicht zuletzt werden auch die Hersteller der neuen Situation begegnen und ihre Produkte anpassen: Durch technische Maßnahmen könnten Computersysteme gezielt diversifiziert angelegt werden, so dass die Wahrscheinlichkeit von gleichzeitigen Schäden architekturbedingt gesenkt werden kann. Hier bieten sich interessante Verbindungen zum Gebiet der Fehlertoleranz (*Safety*).

5.2 Grenzen des Modells

Angesichts der Vielfalt an möglichen Implikationen, die sich aus den vorgestellten Befunden ergeben, ist eine kritische Würdigung der verwendeten Methodologie besonders wichtig. Das verwendete Modell ist zu einfach. Es bildet einige wichtige Aspekte der Realität überhaupt nicht ab; so z. B. unterschiedliche Schadenhöhen und verschiedene Schadenwahrscheinlichkeiten für systematisches Risiko und individuelle Risiken. In der Literatur ist zudem grundsätzlich umstritten, ob der auf historischen Daten beruhende Versicherungsansatz für die Modellierung von Schäden durch strategische Angreifer, wie bspw. Virenprogrammierer, geeignet ist [Sch04a].

Auch das in Abschnitt 4.1 verwendete Nachfragemodell beinhaltet einige starke Annahmen, die kritisch hinterfragt werden müssen. Zum Beispiel sollte die Robustheit der Ergebnisse beim Einsatz anderer Nutzenfunktionen untersucht werden. Ähnliches gilt für die Berücksichtigung von Wirtschaftssubjekten, die nur eine Teildeckung nachfragen.

Beim Vergleich der Plattformen $\mathcal{A}$ und $\mathcal{D}$ (Abschnitt 4.2) ist unrealistisch, dass beide Plattformen eine gleiche totale Schadenwahrscheinlichkeit aufweisen. So könnten unterschiedliche finanzielle Ressourcen für F&E zu weiteren Korrelaten zwischen Marktstruktur und Schadenwahrscheinlichkeit führen. Auch die Berücksichtigung von Transaktionskosten zur Verwaltung und Informationsbeschaffung könnte die hier aufgezeigten Zusammenhänge (vermutlich zugunsten des Marktführers) verändern.

Zu einer umfassenden Betrachtung fehlt zudem die Berücksichtigung von weiteren Aspek-

ten, insbesondere der Informationsökonomie, wie *Moral Hazard*, *Adverse Selection* und Regulierung [BA92]. Die Interpretation und Verallgemeinerung der vorgestellten Ergebnisse sollte deshalb immer unter Vorbehalt der hier genannten Einschränkungen passieren. Gleichzeitig bietet diese Aufzählung auch eine Reihe interessanter Ansatzpunkte für weiterführende interdisziplinäre Forschung.

5.3 Fazit

Eine vorsichtige Interpretation der noch mit methodischen Einschränkungen behafteten Befunde legt nahe, dass Schadenkorrelationen die Entwicklung eines Marktes für IT-Versicherungen durchaus behindern können. Wer IT-Versicherungen fördern will, muss also zugleich eine Diversifizierung der Systeme fördern. Regulatorische Eingriffe im Sinne einer Versicherungspflicht – auch für bestimmte Bereiche – implizieren eine Veränderung der bestehenden Marktmechanismen, insbesondere im Softwarebereich, und könnten zu einer Neuordnung der Marktstruktur führen. Vor diesem Hintergrund bekommt das von Ross Anderson in [And94a] formulierte Prinzip eine neue Bedeutung:

"A trusted component or system is one which you can insure."

Literatur

[Adk04] Roger Adkins. An Insurance Style Model for Determining the Appropriate Investment Level against Maximum Loss arising from an Information Security Breach. In *Workshop of Economics and Information Security*, Minneapolis, MN, 2004. Online verfügbar unter `http://www.dtc.umn.edu/weis2004/adkins.pdf`.

[And94a] Ross J. Anderson. Liability and Computer Security: Nine Principles. In Dieter Gollmann, (Hrsg.), *Computer Security (ESORICS '94)*, LNCS 875, S. 231–245, Berlin Heidelberg, 1994. Springer Verlag.

[And94b] Ross J. Anderson. Why Cryptosystems Fail. *Communications of the ACM*, 33(11):32–40, 1994.

[And01] Ross J. Anderson. Why Information Security is Hard – An Economic Perspective, 2001. Online verfügbar unter `http://www.cl.cam.ac.uk/~rja14/econsec.html`.

[BA92] Karl H. Borch und Knut K. Aase. *Economics of Insurance*. North-Holland, Amsterdam, 1992.

[CW00] Jean L. Camp und Catherine Wolfram. Pricing Security. In *Proc. of the CERT Information Survivability Workshop*, S. 31–39, Boston, MA, October 24–26 2000. Online verfügbar unter `http://www.cert.org/research/isw/isw2000/papers/54.pdf`.

[DS03] Darrell Duffie und Kenneth J. Singleton. *Credit Risk. Pricing, Measurement, and Management*. Princeton University Press, 2003.

[Duf02] Daintry Duffy. Safety at a Premium. *CSO Magazine*, December 2002. Online verfügbar unter `http://www.csoonline.com/read/120902/safety.html`.

[Eco03] The Economist. Fighting the Worms of Mass Destruction. *The Economist*, November 27th, 2003. Online verfügbar unter `http://www.economist.co.uk/science/displayStory.cfm?story_id=2246018`.

[GL02] Lawrence A. Gordon und Martin P. Loeb. The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, 5(4):438–457, 2002.

[GLS03] Lawrence A. Gordon, Martin P. Loeb und Tashfeen Sohail. A Framework for Using Insurance for Cyber-Risk Management. *Communications of the ACM*, 46(3):81–85, 2003.

[Hus04] Stefan Huschens. *Dreizehn Korrelationen in Kreditrisikomodellen*. Nr. 41 in Dresdner Beiträge zu Quantitativen Verfahren. Technische Universität Dresden, 2004.

[Ins04] Insurance Information Institute. Computer Security-Related Insurance Issues, 2004. Online verfügbar unter `http://www.iii.org/media/hottopics/insurance/computer/`. (Abgerufen am 1. Oktober 2004).

[KMY04] Jay P. Kesan, Ruperto P. Majuca und William J. Yurcik. The Economic Case for Cyberinsurance. *Illinois Law and Economics Working Paper Series*, 2004. Online verfügbar unter `http://ssrn.com/abstract=577862`.

[KY94] Robert Kneuper und Bruce Yandle. Auto Insurers and the Air Bag. *Journal of Risk and Insurance*, 61:107–116, 1994.

[Mac97] Thomas Mack. *Schadenversicherungsmathematik*. Nr. 28 in Schriftenreihe Angewandte Versicherungsmathematik. Verlag Versicherungswirtschaft, Karlsruhe, 1997.

[Ozm04] Andy Ozment. Bug Auctions: Vulnerability Markets Reconsidered. In *Workshop of Economics and Information Security*, Minneapolis, MN, 2004. Online verfügbar unter `http://www.dtc.umn.edu/weis2004/ozment.pdf`.

[Pra64] John W. Pratt. Risk Aversion in the Small and in the Large. *Econometrica*, 32:122–136, 1964.

[PW92] Harry H. Panjer und Gordon E. Willmot. *Insurance Risk Models*. Society of Actuaries, Schaumburg, IL, 1992.

[SA02] Anthony Saunders und Linda Allen. *Credit Risk Measurement*. Wiley, New York, 2002.

[Sch02] Klaus D. Schmidt. *Versicherungsmathematik*. Springer Verlag, Berlin Heidelberg, 2002.

[Sch04a] Stuart E. Schechter. *Computer Security Strength & Risk: A Quantitative Approach*. Dissertation, Harvard University, Cambridge, MA, 2004.

[Sch04b] Bruce Schneier. Hacking the Business Climate for Network Security. *IEEE Computer*, S. 87–89, April 2004.

[SV98] Carl Shapiro und Hal R. Varian. *Information Rules. A Strategic Guide to the Network Economy*. Harvard Business School Press, 1998.

[Var99] Hal Varian. *Intermediate Microeconomics – A Modern Approach*. W. W. Norton & Company, New York, 5. Auflage, 1999.

[Var00] Hal Varian. Managing Online Security Risks. *New York Times*, June 1st, 2000. Online verfügbar unter `http://www.nytimes.com/library/financial/columns/060100econ-scene.html`.

[YD02] William Yurcik und David Doss. CyberInsurance: A Market Solution to the Internet Security Market Failure. In *Workshop on Economics and Information Security*, Berkeley, CA, 2002. Online verfügbar unter `http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurit%y/`.