Meldepflichten für IT-Sicherheitsvorfälle: Ein Prinzipal-Agent-Ansatz

Stefan Laube*, Rainer Böhme

Institut für Wirtschaftsinformatik, Westfälische Wilhelms-Universität Münster
{Stefan.Laube,Rainer.Boehme}@uni-muenster.de

Zusammenfassung. Gesetzgeber in vielen Ländern planen, auf mangelnde IT-Sicherheit in der Privatwirtschaft mit der Einführung von Meldepflichten für IT-Sicherheitsvorfälle zu reagieren. Dieser Beitrag betrachtet Meldepflichten in einem Prinzipal-Agent-Modell. Marktteilnehmer (Agenten) haben wenig Anreize, IT-Sicherheitsvorfälle unilateral zu melden. Dem könnte der Staat (Prinzipal) durch Audits, gekoppelt mit Sanktionen, begegnen. Allerdings können Audits nicht zwischen strategischem Verschweigen und ehrlicher Unwissenheit der Agenten differenzieren. Deshalb könnte es schwierig werden, die Sanktionen so zu justieren, dass sich insgesamt ein positiver Wohlfahrtseffekt einstellt. Die Einführung von Meldepflichten ist zudem nur unter optimistischen Annahmen zur Verwertung gemeldeter IT-Sicherheitsvorfälle sinnvoll.

Schlüsselwörter: Meldepflichten für IT-Sicherheitsvorfälle, Interdependenz, Informationsasymmetrie, Prinzipal-Agent-Theorie, IT-Sicherheitsaudits

1 Motivation

Die kanonischen Schutzziele für informationstechnische Systeme lauten Vertraulichkeit, Integrität und Verfügbarkeit. IT-Sicherheitsvorfälle sind Ereignisse, bei denen eines oder mehrere dieser Schutzziele verletzt werden [18]. Sie können sowohl die Datensicherheit als auch den Datenschutz betreffen [13]. Angriffe auf Informationssysteme nehmen seit Jahren zu. Dadurch treten mehr IT-Sicherheitsvorfälle ein und es entstehen hohe Kosten für die betroffenen Unternehmen [34].

IT-Sicherheitsvorfälle verursachen sowohl direkte als auch indirekte Kosten [9]. Direkte Kosten ergeben sich z. B. durch das Entfernen von Schadprogrammen. Indirekte Kosten schließen immaterielle Kosten mit ein und betreffen z. B. Reputationsverluste durch die Veröffentlichung von Informationen über IT-Sicherheitsvorfälle. Um die indirekten Kosten zu quantifizieren, analysieren Cavusoglu et al. [9] den Einfluss der Veröffentlichung von Vorfällen börsennotierter Unternehmen auf deren Marktwert. Die Ergebnisse zeigen, dass IT-Sicherheitsvorfälle in den ersten zwei Tagen nach ihrer Veröffentlichung zu einem Verlust von (im Durchschnitt) 2.1% des Marktwerts führen. Diese Kosten schreiben Cavusoglu et al. vor allem Vertrauensverlusten der Kunden zu. Ihre Studie kommt zu der Einschätzung, dass nach Veröffentli-

12th International Conference on Wirtschaftsinformatik,
March 4-6 2015, Osnabrück, Germany

Laube, S.; Böhme, R. (2015): Meldepflichten für IT-Sicherheitsvorfälle: Ein Prinzipal-Agent-Ansatz, in: Thomas. O.; Teuteberg, F. (Hrsg.): Proceedings der 12. Internationalen Tagung Wirtschaftsinformatik (WI 2015), Osnabrück, S. 1146-1162

chung eines Vorfalles die indirekten Kosten höher ausfallen als die direkten, welche auch ohne Veröffentlichung entstanden wären.

IT-Sicherheitsvorfälle erzeugen jedoch nicht nur Kosten bei unmittelbar Betroffenen. Es besteht eine gegenseitige Abhängigkeit vernetzter Informationssysteme von Marktteilnehmern in einer Ökonomie, wodurch sich Vorfälle ausbreiten können [24]. Mangelhafte IT-Sicherheit führt somit zu negativen Externalitäten, die sich in IT-Sicherheitsvorfällen materialisieren. Kritische Infrastrukturen sind aus mehreren Gründen besonders exponiert [2,6].

Die Interdependenz von Informationssystemen rechtfertigt Regulierungsbestrebungen zur Senkung der durch IT-Sicherheitsvorfälle anfallenden Kosten [21]. Eine Verringerung dieser sozialen Kosten kann zu einer Steigerung der sozialen Wohlfahrt führen [32]. Es existieren unterschiedliche Regulierungsansätze [3]. Einer davon ist die Einführung von Meldepflichten für IT-Sicherheitsvorfälle. Es fehlt jedoch an wissenschaftlichen Untersuchungen zur Wirksamkeit solcher Meldepflichten. Diese Arbeit präsentiert ein Prinzipal-Agent-Modell, dessen Analyse zur Schließung dieser Forschungslücke beitragen soll.

Der Beitrag gliedert sich von nun an wie folgt: In Kapitel 2 folgt eine qualitative Beschreibung des Forschungsgegenstandes sowie die Formulierung unserer Forschungsfrage. Kapitel 3 beinhaltet einen Überblick über die mit unserem Beitrag verwandten Arbeiten. In Kapitel 4 stellen wir unser Modell vor und identifizieren dessen Gleichgewichte. Anschließend, in Kapitel 5, interpretieren wir die ermittelten Gleichgewichte. Der Beitrag schließt in Kapitel 6 mit einer Erörterung von Schlussfolgerungen, die sich aus der Analyse ergeben sowie einem Ausblick.

2 Ausgangslage und Forschungsfrage

In diesem Kapitel besprechen wir bestehende und aktuell diskutierte Meldepflichten für IT-Sicherheitsvorfälle. Wir weisen auf die Schwierigkeit der Anreizkompatiblität von Meldepflichten hin (Abschnitt 2.1) und erörtern Kontrollmechanismen zur Einhaltung von Meldepflichten (Abschnitt 2.2). Zuletzt leiten wir die Forschungsfrage aus einer aktuell diskutierten Meldepflicht ab (Abschnitt 2.3).

2.1 Meldepflichten für IT-Sicherheitsvorfälle

Meldepflichten für IT-Sicherheitsvorfälle wurden bereits in vielen Ländern eingeführt. Beispiele sind unter anderem die „California Civil Code Section § 1798.29“ in den USA [8], diese zielt auf IT-Sicherheitsvorfälle mit Datenschutz-Relevanz ab, und deren Nachfolger in anderen US-Bundesstaaten [29] sowie die Privacy Amendments (Privacy Alerts) Bill 2013 in Australien [30]. In Europa bestehen seit 2007 eine Richtlinie zur Veröffentlichung von IT-Sicherheitsvorfällen für den Telekommunikationssektor [11] sowie branchenspezifische Regelungen in der EU-Verordnung Nr. 611/2013 und der Richtlinie 2002/58/EG.

Im Februar 2013 stellte die Europäische Kommission eine Netz- und Informationssicherheits-Richtlinie (NIS-Richtlinie) [12] vor, die eine Meldepflicht für IT-Sicherheitsvorfälle in der Privatwirtschaft vorsieht. Das EU-Parlament stimmte im

März 2014 mit großer Mehrheit für die Umsetzung dieser Richtlinie, die Zustimmung des Rates steht noch aus. Parallel dazu wird in Deutschland seit März 2013 ein Referentenentwurf für ein IT-Sicherheitsgesetz diskutiert, das Meldepflichten vorsieht. Die aktuelle Auflage dieses Referentenentwurfs stammt aus dem August 2014 [7].

Den neuen Meldepflichten ist gemein, dass sie Marktteilnehmern Informationspflichten bei IT-Sicherheitsvorfällen auferlegen. Zudem sehen die Gesetzentwürfe die Bestellung einer zentralen Instanz vor, an die Meldungen gerichtet werden müssen. Die Einführung von Meldepflichten wird oft auf Basis folgender unterstellter positiver Effekte für die Gesellschaft motiviert:

- Meldepflichten können die Komplexität der Definition von Sicherheitsvorkehrungen für Informationssysteme umgehen, indem sie bei Marktteilnehmern Anreize zur Prävention von IT-Sicherheitsvorfällen schaffen [3].
- Die zentrale Instanz kann Marktteilnehmer über bestehende IT-Sicherheitsvorfälle unterrichten oder ihnen bei der Reduktion von Schäden helfen [32].
- Die Weitergabe gemeldeter Informationen an betroffene natürliche Personen ist Voraussetzung zur Gewährung von Rechten wie z. B. dem Persönlichkeitsrecht. Durch einen Informationsaustausch mit Betroffenen, z. B. bei einer Datenschutzverletzung, können diese persönliche Schäden reduzieren [35].

Eine Meldepflicht geht jedoch ebenfalls mit potenziellen negativen Effekten für zur Meldung verpflichtete Marktteilnehmer einher. Durch Meldungen entstehen zusätzliche indirekte Kosten wie beispielsweise Reputationsschäden, Haftungs- und Schadensersatzansprüche betroffener natürlicher Personen, negative Reaktionen der Finanzmärkte oder Signale der Schwäche [14]. Demnach bedarf es an effektiven Anreizen, um Meldepflichten durchzusetzen [3].

2.2 Kontrollmechanismen zur Einhaltung von Meldepflichten

Bestehende und aktuell diskutierte Meldepflichten erzielen keinen Konsens darüber, welcher Anreizmechanismus eingeführt werden sollte. Winn [35] evaluiert Meldepflichten für IT-Sicherheitsvorfälle und stellt fest, dass die Einführung einer effektiven Meldepflicht nur unter Verwendung verschiedener, sich ergänzender politischer Instrumente möglich ist. Es bedarf zum einen an Strategien, die die freiwillige Einhaltung und Selbstregulierung fördern, d. h. Marktteilnehmer zur Investition in technische Kontrollmechanismen für IT-Sicherheitsvorfälle veranlassen. Zu diesen Strategien gehören unter anderem die Einführung von Subventionen, Haftungsregelungen und steuerlichen Anreizen. Zum anderen werden organisatorische Kontrollmechanismen benötigt, welche die technischen Kontrollmechanismen bei Marktteilnehmern unterstützen: Beispielsweise können Audits zur Überprüfung und Zertifizierung von Systemen, die einem gesetzlichen Standard entsprechen, genutzt werden [5].

Cavusoglu et al. [10] unterscheiden zwei Kategorien von technischen Kontrollmechanismen für IT-Sicherheitsvorfälle: Präventions- und Aufdeckungsmechanismen. Zu den Präventionsmechanismen gehören Techniken, die Informationssysteme abschirmen (wie z. B. Firewalls). Im Folgenden interpretieren wir Investitionen in Präventionsmechanismen als *IT-Sicherheitsinvestitionen*. Aufdeckungsmechanismen für

Angriffe sind z. B. Angriffserkennungssysteme. Der Betrieb dieser Systeme verursacht fixe und variable Kosten [22] und führt mitunter zu Fehlern erster Art (Warnung, obwohl kein Angriff vorliegt) sowie Fehlern zweiter Art (ausbleibende Warnung trotz eines Angriffs) [10].

Organisatorische Kontrollmechanismen können bei Marktteilnehmern Anreize zur Investition in IT-Sicherheit schaffen [1,10]. Die NIS-Richtlinie [12] schlägt z. B. Audits, gekoppelt mit Sanktionen, zur Überprüfung der Gesetzeskonformität von Marktteilnehmern vor. Das erklärte Ziel dabei ist, Informationsasymmetrien bzgl. IT-Sicherheitsvorfällen innerhalb der EU zu reduzieren und ein EU-weites Mindestniveau an IT-Sicherheit zu schaffen. Es bleiben jedoch Fragen der konkreten Umsetzung offen. Unsere Arbeitshypothese ist, dass Marktteilnehmer bei Verstößen gegen Meldepflichten mit Sanktionen belastet werden sollen. Bisherige Ansätze zur Abschätzung der Effektivität solcher Audits als Anreizmechanismus zur Durchsetzung von Meldepflichten sind uns nicht bekannt.

2.3 Forschungsfrage

Unsere Forschungsfrage motiviert sich aus der NIS-Richtlinie [12] und den potenziell aus dieser Richtlinie abgeleiteten Gesetzen:

Unter welchen Umständen steigern Meldepflichten für IT-Sicherheitsvorfälle (vgl. Abschnitt 2.1), die über Audits und Sanktionen durchgesetzt werden (vgl. Abschnitt 2.2), (a) das allgemeine IT-Sicherheitsniveau und (b) die soziale Wohlfahrt?

Diese Frage ist relevant für Marktteilnehmer, die Entscheidungen bzgl. der *Meldung von IT-Sicherheitsvorfällen* und *IT-Sicherheitsinvestitionen* zu treffen haben. Zudem ist sie relevant für Regulierer, die Entscheidungen bzgl. der *Wahrscheinlichkeit von Audits* sowie der *Höhe von Sanktionen* treffen müssen.

Zur Beantwortung müssen folgende Gegebenheiten berücksichtigt und modelliert werden: Die durch Meldepflichten entstehenden Kosten (vgl. Kapitel 1), die Interdependenz informationstechnischer Systeme (vgl. Kapitel 1), die Wirksamkeit von Gegenmaßnahmen durch eine zentrale Instanz (vgl. Abschnitt 2.1) sowie die Fehlerrate von internen Kontrollmechanismen (vgl. Abschnitt 2.2).

3 Verwandte Arbeiten

Die mit dieser Arbeit verwandte Literatur gliedert sich in zwei Bereiche: Prinzipal-Agent-Modelle, die zur Analyse der Wirksamkeit von Audits verwendet werden und ökonomische Arbeiten zum Austausch sicherheitsrelevanter Informationen.

Zu den ersten Wissenschaftlern, die Audits im Kontext von Prinzipal-Agent-Modellen verwenden, gehören Ng und Stoeckenius [31]. Sie beschreiben im Jahr 1979 ein Moral-Hazard-Problem zwischen Eigentümern (Prinzipal) und dem Management (Agent) eines Unternehmens. Dieser und vielen folgenden Arbeiten zur Lösung von Moral-Hazard- und Averse-Selektion-Problemen ist gemeinsam, dass

Audits durch den Prinzipal zur Überwindung von Informationsasymmetrien zwischen Prinzipal und Agent vertraglich geregelt werden (vgl. z. B. [25]). Wir untersuchen dagegen die Ausgestaltung einer gesetzlichen Regelung.

Theoretische Arbeiten, die sich mit dem Austausch von sicherheitsrelevanten Informationen befassen, beruhen vorwiegend auf dem Gordon-Loeb-Modell für IT-Sicherheitsinvestitionen [17] und beinhalten eine Modellierung interdependenter IT-Risiken. Gordon et al. [19] analysieren Kosten, die durch den Austausch von Informationen über IT-Sicherheit in einer Ökonomie entstehen. Sie zeigen, dass ein Informationsaustausch zur Senkung der Ausgaben für IT-Sicherheitsinvestitionen führen kann. Gal-Or und Ghose [14] analysieren den Preiswettbewerb konkurrierender Unternehmen, die sicherheitsrelevante Informationen miteinander austauschen. Im Gegensatz zu Gordon et al. [19] kommen sie zu dem Ergebnis, dass IT-Sicherheitsinvestitionen und Informationsaustausch strategische Komplemente sein können. Hausken [20] analysiert neben dem Informationsaustausch zwischen Unternehmen auch die Vorgehensweise eines strategischen Angreifers. Er zeigt, dass der Informationsaustausch in einer Ökonomie mit deren Interdependenz steigt. Lui et al. [27] zeigen, dass die Art der Informationsgüter, die von verschiedenen Unternehmen geschützt werden, eine entscheidende Rolle für den Austausch sicherheitsrelevanter Informationen spielt. Im Fall von komplementären Informationsgütern haben Unternehmen natürliche Anreize zum Austausch von Informationen. Im Fall von austauschbaren Informationsgütern werden hingegen Anreize benötigt, um einen Informationsaustausch hervorzurufen. Gao et al. [15,16] führen in zwei unterschiedlichen Beiträgen aus, unter welchen Bedingungen der Eingriff eines sozialen Planers in den Informationsaustausch wohlfahrtssteigernd ist. Allen Arbeiten ist gemein, dass der Austausch sicherheitsrelevanter Informationen wohlfahrtssteigernd wirken kann.

Eine Interpretation gesetzlicher Meldepflichten für IT-Sicherheitsvorfälle im Prinzipal-Agent-Modell ist uns nicht bekannt. Nachfolgend soll ein solches Modell aufgestellt werden, um die Forschungsfrage zu beantworten.

4 Modell

Das nachfolgende Modell setzt sich aus drei Komponenten zusammen: Einem Modell für IT-Sicherheitsinvestitionen einschließlich interdependenter Risiken (Abschnitt 4.1), einer Formalisierung von Meldepflichten (Abschnitt 4.2) sowie einer Formalisierung von Sicherheitsaudits (Abschnitt 4.3). Über diese Komponenten lassen sich das soziale Optimum (Abschnitt 4.4) des Modells sowie dessen Nash-Gleichgewichte (Abschnitt 4.5) bestimmen. Tabelle 1 im Anhang zu diesem Beitrag fasst alle in dem Modell verwendeten Symbole zusammen.

4.1 IT-Sicherheitsinvestitionen und Interdependenz

Betrachten wir einen rationalen Marktteilnehmer in einer Ökonomie, der in Sicherheit investiert $x \geq 0$, um die Wahrscheinlichkeit P von IT-Sicherheitsvorfällen zu reduzieren. Gordon und Loeb [17] charakterisieren diesen Zusammenhang $P(x)$: Die Vor-

fall-Wahrscheinlichkeit sinkt $P'(x) < 0$ in absteigendem Maße $P''(x) > 0$ bei zunehmender IT-Sicherheitsinvestition. Es gilt $\lim_{x\to\infty} P(x) \to 0$. Nachfolgend übernehmen wir die funktionale Form $P(x) = \beta^{-x}$ von Böhme [5]. Dabei stellt β die Sicherheitsproduktivität eines Marktteilnehmers dar, die wir auf $\beta = 20$ festlegen, um die Anzahl der Parameter überschaubar zu halten. Dies entspricht einer moderaten Sicherheitsproduktivität. Jeder Angriff auf ein ungeschütztes Informationssystem führt zu direkten Kosten $q_1 = 1$, sodass für die durch einen IT-Sicherheitsvorfall erwarteten Kosten eines Marktteilnehmers gilt:

$$c(x) = P(x) \cdot q_1 + x. \tag{1}$$

Wir nehmen vereinfachend an, dass eine Ökonomie aus insgesamt $n = 2$ symmetrischen und a priori homogenen, rationalen Marktteilnehmern besteht. Beide Teilnehmer $i \in \{0,1\}$ wählen die Höhe ihrer Investition x_i eigenständig. Nach Öğüt et al. [32] lautet die Wahrscheinlichkeit für einen IT-Sicherheitsvorfall bei einem Marktteilnehmer gegeben eines *Parameters für die Interdependenz informationstechnischer Systeme von Marktteilnehmern* $\gamma \in [0,1]$:

$$P_i(x_i, x_{1-i}) = 1 - \big(1 - P(x_i)\big) \cdot \big(1 - \gamma \cdot P(x_{1-i})\big). \tag{2}$$

4.2 Unscharfe Beobachtungen und Meldepflichten

Wir nehmen an, dass jeder Marktteilnehmer ein Eigeninteresse hat, IT-Sicherheitsvorfälle innerhalb seines Informationssystems aufzudecken. Die Realisierung der Zufallsvariable *SV* (IT-Sicherheitsvorfall) bei einem Marktteilnehmer sei durch $\alpha_i \in \{0,1\}$ gegeben, sodass $Pr(\alpha_i = 1) = P_i(x_i, x_{1-i})$. Zur Entdeckung von Vorfällen nutzen die Marktteilnehmer Angriffserkennungssysteme. Solche Systeme sind in der Praxis keine notwendige Voraussetzung dafür, Vorfälle zu entdecken. Wir führen Angriffserkennungssysteme als exemplarische interne Kontrollmechanismen ein und vernachlässigen die durch solche Systeme anfallenden Kosten, um die Parameteranzahl des Modells zu beschränken. Sei $\hat{\alpha}_i \in \{0,1\}$ die Realisierung der Zufallsvariable E (IT-Sicherheitsvorfall entdeckt). Es gelte $Pr(\hat{\alpha}_i = 1 | \alpha_i = 1) = 1 - \epsilon$, wobei $\epsilon \in]0,1]$ den *Parameter für die Wahrscheinlichkeit von Fehlern der Angriffserkennungssysteme* darstellt. Wir nehmen an, dass keine Fehler erster Art auftreten. Eine Studie von Lippmann et al [26] zeigt, dass selbst die besten Angriffserkennungssysteme nur eine Erkennungsrate von ca. 80 % haben. Für die folgenden Abbildungen setzen wir daher die Wahrscheinlichkeit eines Fehlers zweiter Art auf $\epsilon = 20$ % fest.

Meldepflichten veranlassen Meldeentscheidungen $\tilde{\alpha}_i \in \{0,1\}$ durch Marktteilnehmer. Eine Entscheidung gegen die Meldung eines gefundenen Vorfalls sei durch $\tilde{\alpha}_i = 0$ ausgedrückt. Vereinfachend nehmen wir an, dass Marktteilnehmer keine Vorfälle fingieren. Gesetzeskonformität sei durch $Pr(\tilde{\alpha}_i = 1 | \hat{\alpha}_i = 1 \wedge \alpha_i = 1) = t_i$ gegeben. Die zentrale Instanz, an die gemeldet wird, führt Gegenmaßnahmen bei Meldungen ein. Gemäß Öğüt et al. [32] können solche Maßnahmen durch eine Reduktion der Interdependenz $\eta(t)$ in einer Ökonomie beschrieben werden:

$$P_i(x_i, x_{1-i}, t_{1-i}) = 1 - \big(1 - P(x_i)\big) \cdot \big(1 - \gamma \cdot \eta(t_{1-i}) \cdot P(x_{1-i})\big). \tag{3}$$

Eigene Meldungen t_i eines Marktteilnehmers tragen dabei nicht zur Reduktion der Interdependenz zu anderen Marktteilnehmern bei. Dieser Anteil wird ohnehin vernachlässigbar wenn die Anzahl aller Marktteilnehmer steigt, d. h. $n \to \infty$.

Sei $b \in [0,1]$ der *Parameter für die Effektivität einer zentralen Instanz im Umgang mit gemeldeten Vorfällen*. Somit kann $\eta(t_{1-i})$ definiert werden als:

$$\eta(t_{1-i}) = 1 - b \cdot (1 - \epsilon) \cdot t_{1-i}. \tag{4}$$

4.3 Kosten und Audits

Die Meldung von Vorfällen geht mit zu erwartenden indirekten Kosten für Marktteilnehmer (z. B. Reputationsschäden) einher. Sie fallen an, wenn beispielsweise die zentrale Instanz Informationen über Vorfälle veröffentlicht. Sei $q_2 \in [0, \infty[$ der *Parameter für die Höhe der indirekten Kosten*. Die Gesamtkosten eines Marktteilnehmers (vgl. Gl. (6)) sind also abhängig von seinem Meldeverhalten t_i, das die Summe der indirekten und direkten Kosten $L_i(t_i)$ beeinflusst:

$$L_i(t_i) = (1 - \epsilon) \cdot t_i \cdot q_2 + q_1 \tag{5}$$

$$c_i(x_i, x_{1-i}, t_i, t_{1-i}) = P_i(x_i, x_{1-i}, t_{1-i}) \cdot L_i(t_i) + x_i. \tag{6}$$

Der Konflikt zwischen Marktteilnehmern und Regulierern kann als Prinzipal-Agent-Problem mit Moral-Hazard interpretiert werden: Ein Regulierer (Prinzipal) kann gesetzliche Meldepflichten für IT-Sicherheitsvorfälle einführen. Agenten tätigen IT-Sicherheitsinvestitionen und haben Informationen über Vorfälle. Der Prinzipal kann sich jedoch nicht sicher sein, dass Agenten im Sinne des Gesetzes handeln. Um für die Agenten Anreize zur Gesetzeskonformität zu schaffen, führt der Prinzipal Audits und Sanktionen ein.

Die Realisierung der Zufallsvariable A (Audit) sei durch $\psi \in \{0,1\}$ gegeben, sodass $Pr(\psi = 1) = a$ die Wahrscheinlichkeit für einen durch den Prinzipal eingeleiteten Sicherheitsaudit darstellt. Vereinfachend soll im Folgenden jeder Audit jeden eingetretenen Vorfall mit Gewissheit entdecken. Audits seien damit per Definition viel zuverlässiger als Angriffserkennungssysteme.

Der Entscheidungsbaum in Abb. 1 stellt die für einen Agenten entstehenden Kosten durch einen IT-Sicherheitsvorfall (auf Basis seiner Entscheidungen sowie der des Prinzipals und der Natur) dar, wobei die Ungewissheit des Agenten durch gestrichelte Linien gekennzeichnet ist. Zunächst investiert der Agent x_i in Sicherheit. Daraufhin findet ein Angriff auf sein Informationssystem statt, der mit der Wahrscheinlichkeit $P_i(x_i, x_{1-i}, t_{1-i})$ erfolgreich ist. Vereinfachend gehen wir davon aus, dass in jedem Betrachtungszeitraum maximal ein IT-Sicherheitsvorfall vorliegen kann. Der Agent erkennt einen Vorfall mit der Wahrscheinlichkeit $1 - \epsilon$ und muss (unabhängig von der Realisation eines Vorfalls) eine Meldeentscheidung treffen. Falls kein Vorfall gemeldet wird, veranlasst der Prinzipal stichprobenartige Audits. Fehlverhalten des Agenten wird mit $S \in [0, \infty[$ sanktioniert.

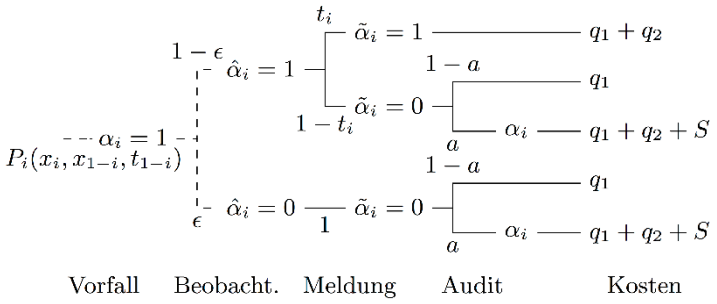


Abb. 1. Entscheidungsbaum

Aus Abb. 1 lassen sich die Kosten eines Marktteilnehmers im Falle eines Vorfalls nach Einführung einer gesetzlichen Meldepflicht, gegeben fixer Sanktionen, ablesen:

$$L_i(t_i, a) = (1 - \epsilon) \cdot [t_i \cdot q_2 + (1 - t_i) \cdot a \cdot (q_2 + S)] + \epsilon \cdot a \cdot (q_2 + S) + 1 \quad (7)$$

$$c_i(x_i, x_{1-i}, t_i, t_{1-i}, a) = P_i(x_i, x_{1-i}, t_{1-i}) \cdot L_i(t_i, a) + x_i. \quad (8)$$

Anhand des Entscheidungsbaums in Abb. 1 wird deutlich, dass der Prinzipal die zu wählende Audit-Wahrscheinlichkeit a und die Sanktionen S miteinander substituieren kann. Werden die Sanktionen unendlich hoch gewählt, entstehen immer Anreize zur Meldung von Vorfällen bei den Agenten – sofern Audits durchgeführt werden. Dieses Ergebnis ist trivial und steht dem Vergleich verschiedener Anreizmechanismen im Wege. Wir folgen daher Khouzani et al. [23] und fixieren die Sanktionen auf ein als durchsetzbar angenommenes Niveau von $S = 1$. (Das entspricht den direkten Kosten q_1.) Daraufhin lösen wir nach der Audit-Wahrscheinlichkeit auf.

4.4 Soziales Optimum

Soziale Kosten sind die Summe der Kosten aller Agenten in einer Ökonomie. Ein sozialer Planer mit Kontrolle über IT-Sicherheitsinvestitionen, Meldungen und Audits (die zur Anreizschaffung von IT-Sicherheitsinvestitionen und Meldungen gedacht sind und daher vom sozialen Planer nicht benötigt werden) hat folgendes Minimierungsproblem, basierend auf Gl. (6):

$$(x^*, t^*) = \arg\min_{x,t} 2 \cdot c_i(x, x, t, t, 0) = \arg\min_{x,t} c(x, x, t, t). \quad (9)$$

Die Substitution von x_i durch x ergibt sich aus der Symmetrieeigenschaft. Das Minimum von Gl. (9) ist durch Extremwerte oder Randwerte gekennzeichnet.

Aus der ersten und zweiten Ableitung der Gl. (9) nach t folgt, dass $t^*\big(x^*(t^*)\big) \in \{0,1\}$ einen Randwert darstellt. Ein sozialer Planer unterscheidet:

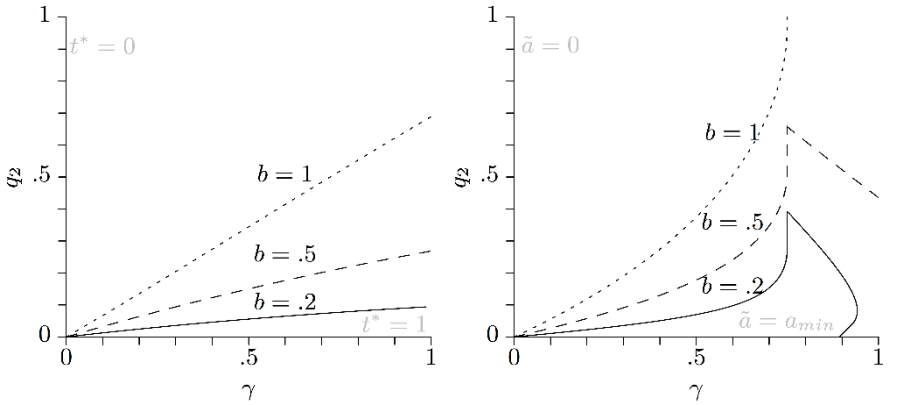
$$t^*\big(x^*(t^*)\big) = \begin{cases} 1, & \text{falls } c(x^*(0), x^*(0), 0,0) > c(x^*(1), x^*(1), 1,1) \\ 0, & \text{sonst.} \end{cases} \quad (10)$$

(Dies kann auch als Entscheidung über die Einführung von Meldepflichten unter der Annahme ehrlicher Agenten interpretiert werden.)

Die optimale IT-Sicherheitsinvestition $x^*(t^*)$ folgt aus der Nullstelle der ersten Ableitung von Gl. (9) nach x. Im sozialen Optimum gilt:

$$x^*(t^*) = -\frac{\log\left(\frac{\gamma\cdot\eta(t^*)+1}{4\cdot\gamma\cdot\eta(t^*)} - \sqrt{\frac{(\gamma\cdot\eta(t^*)+1)^2}{16\cdot\gamma^2\cdot\eta(t^*)^2} - \frac{1}{2\cdot\gamma\cdot\log(\beta)\cdot\eta(t^*)\cdot L(t^*,0)}}\right)}{\log(\beta)}. \tag{11}$$

Abb. 2 (a) visualisiert, wann ein sozialer Planer Meldepflichten einführt. Eine Interpretation der Abbildungen folgt in Kapitel 5.



(a) Fallunterscheidung aus Gl. (10) (b) Fallunterscheidung aus Gl. (17)

Abb. 2. Entscheidungen sozialer Planer (a) und Prinzipal (b)

4.5 Nash-Gleichgewicht

In der Praxis existiert jedoch kein sozialer Planer. Die Agenten verfolgen eigene Interessen, auf deren Basis sie ihre individuellen Kosten minimieren. Es bedarf somit einer spieltheoretischen Analyse der Nash-Gleichgewichte des Prinzipal-Agent-Spiels. Zur Lösung eines solchen Spiels kann nach Macho-Stadler und Pérez-Castrillo [28] zunächst das Gleichgewicht unter den Agenten ermittelt werden, bevor der Prinzipal die sozialen Kosten minimiert. Wir betrachten nur reine Strategien.

Agenten. Jeder Agent trifft simultan Investitions- und Meldeentscheidungen um seine Kosten aus Gl. (8) zu minimieren. Ein Agent hat somit das Minimierungsproblem:

$$(x_i^+, t_i^+) = \arg\min_{x_i, t_i} c_i(x_i, x_{1-i}, t_i, t_{1-i}, a). \tag{12}$$

Aus der ersten Ableitung der Kostenfunktion in Gl. (12) nach t_i folgt, dass die beste Antwort eines Agenten $t_i^+(x_i, x_{1-i}, t_{1-i}, a)$ ein Randwert ist. Über die gegenseitig besten Antworten beider Agenten lässt sich die Meldewahrscheinlichkeit im Gleich-

gewicht $\tilde{t}(\tilde{x}, a)$ ermitteln. Wenn marginal risikoaverse Agenten Meldepflichten bei Indifferenz einhalten, gilt im Gleichgewicht:

$$\tilde{t}(\tilde{x}, a) = \begin{cases} 1, & \text{falls } a \geq a_{min} \vee q_2 = 0 \\ 0, & \text{sonst.} \end{cases} \tag{13}$$

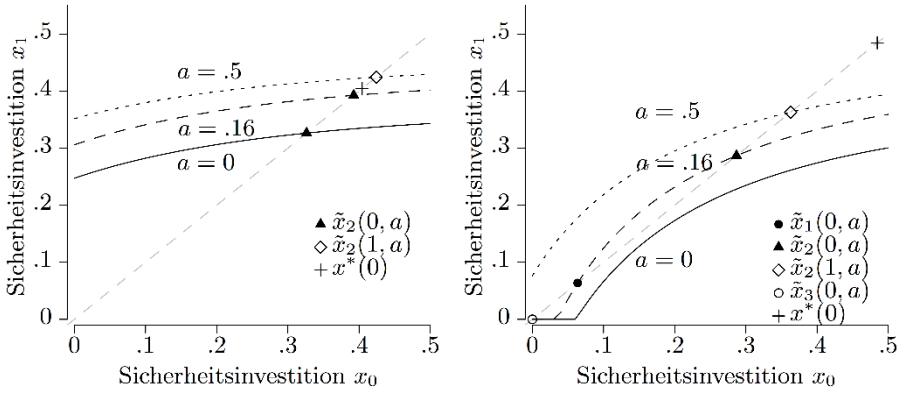
Die beste Antwort eines Agenten bzgl. der IT-Sicherheitsinvestition $x_i^+(x_{1-i}, t_i, t_{1-i}, a)$ entspricht der Nullstelle der ersten Ableitung der Kostenfunktion in Gl. (12) nach x_i:

$$x_i^+(x_{1-i}, t_i, t_{1-i}, a) = \sup\left\{-\frac{\log\left(\frac{1}{\log(\beta)\cdot L(t_i,a)\cdot(1-\gamma\cdot\eta(t_{1-i})\cdot\beta^{-x_{1-i}})}\right)}{\log(\beta)}, 0\right\}. \tag{14}$$

Über die Fixpunkte der besten Antworten beider Agenten ergeben sich drei Gleichgewichte:

$$\tilde{x}_{1,2}(\tilde{t}, a) = -\frac{\log\left(\frac{1}{2\cdot\gamma\cdot\eta(\tilde{t})} \pm \sqrt{\frac{1}{4\gamma^2\cdot\eta(\tilde{t})^2} - \frac{1}{\gamma\cdot\log(\beta)\cdot\eta(\tilde{t})\cdot L(\tilde{t},a)}}\right)}{\log(\beta)}; \tilde{x}_3(\tilde{t}, a) = 0. \tag{15}$$

Abb. 3 (a) und (b) zeigen alle interessanten Fälle für die beste Antwort eines Agenten auf eine IT-Sicherheitsinvestition des zweiten Agenten sowie auf Sicherheitsaudits durch den Prinzipal. Eine Interpretation beider Abbildungen findet in Kapitel 5 statt.



(a) Beste Antwort Agent 1 ($\gamma = .3$) (b) Beste Antwort Agent 1 ($\gamma = .8$)

Abb. 3. Beste Antwort von Agent 1 auf Agent 0 und den Prinzipal ($b = .2; q_2 = .2; a_{min} = .166$); Nash-Gleichgewichte liegen auf den Schnittpunkten mit der Winkelhalbierenden

Prinzipal. Der Prinzipal nutzt die höchste Gleichgewichts-Investition $\tilde{x}_2(\tilde{t}, a)$ als Anreizkompatibilitätsbedingung. Eine Partizipationsbedingung für die Agenten, wie sie in Prinzipal-Agent-Modellen üblich ist, entfällt, weil Meldepflichten rechtlich binden. Das Problem des Prinzipals lautet somit:

$$\tilde{a} = \arg\min_a 2 \cdot c(\tilde{x}_2(a), \tilde{t}(a), a) = \arg\min_a c(\tilde{x}_2(a), \tilde{t}(a), a). \tag{16}$$

Aus der Funktion in Gl. (8) wird ersichtlich, dass Audits und Sanktionen zu zusätzlichen Kosten bei einem Agenten führen. Gleichzeitig können Audits und Sanktionen als Anreize zur Meldung von IT-Sicherheitsvorfällen genutzt werden (vgl. Gl. (13)). Der Prinzipal sucht diejenige Audit-Wahrscheinlichkeit, unter der eine grundsätzliche Anreizschaffung a_{min} zum Austausch von Informationen existiert und die gleichzeitig die sozialen Kosten senkt. Andernfalls sind Audits ineffektiv:

$$\tilde{a} = \begin{cases} a_{min}, & \text{falls } c(\tilde{x}_2(0), \tilde{x}_2(0), 0,0) > c(\tilde{x}_2(a_{min}), \tilde{x}_2(a_{min}), 1,1) \\ 0, & \text{sonst.} \end{cases} \quad (17)$$

Abb. 2 (b) stellt den Parameterraum für Entscheidungen des Prinzipals dar. Wir interpretieren diese Abbildung im nächsten Kapitel.

5 Interpretation

Im Folgenden interpretieren wir die Abbildungen aus Kapitel 4. Zunächst erklären wir das Handeln eines sozialen Planers (Abschnitt 5.1). Dann diskutieren wir, unter welchen Bedingungen welche Gleichgewichte bei der Einführung von Meldepflichten für IT-Sicherheitsvorfälle entstehen (Abschnitt 5.2).

5.1 Soziales Optimum

Bei steigender Interdependenz γ steigen die durch einen sozialen Planer eingeführten IT-Sicherheitsinvestitionen. Dieses Ergebnis wird durch den Vergleich der Abb. 3 (a) mit der Abb. 3 (b) ersichtlich (Veränderung des $+$). Abb. 2 (a) zeigt, unter welchen Parameterkonstellationen ein sozialer Planer Meldungen von IT-Sicherheitsvorfällen einführt. Die Linien beschreiben Indifferenzen bzgl. der Fallunterscheidung in Gl. (10) bei unterschiedlicher Effektivität b einer zentralen Instanz. Die Fläche unter den Linien beschreibt $t^*\big(x^*(t^*)\big) = 1$ und vice versa. Bei steigender Fehlerquote ϵ, die nach Gl. (4) eine Steigerung von $\eta(t)$ zur Folge hat, sinken die Linien in Richtung Abszisse. Dann bleiben Vorfälle eher unentdeckt, was den Effekt der Reduktion interdependenter Risiken durch eine zentrale Instanz abschwächt.

5.2 Nash-Gleichgewicht

Reaktion der Agenten auf Audits. Ohne Audits und bei positiven indirekten Kosten sind Meldepflichten für Agenten wirkungslos (vgl. Argumentation zu Gl. (25)). Abhängig von der Interdependenz (vgl. Argumentation zu Gl. (30)) können dann bis zu drei Gleichgewichte $(a = 0, \tilde{t} = 0, \tilde{x}_{1,2,3}(0,0))$ bestehen. Diese liegen unter dem sozialen Optimum (vgl. Abb. 3), gegeben $x^*(t^*) \neq 0$. Sollten Marktteilnehmer trotz fehlender Anreize Vorfälle melden, so entstehen für sie indirekte Kosten (vgl. Gl. (6)). Eine Audit-Wahrscheinlichkeit $a < a_{min}$ kann Anreize für IT-Sicherheitsinvestitionen schaffen, denn Audits und Sanktionen steigern die erwarteten Kosten durch Vorfälle bei den Agenten (vgl. Gl. (7) und Gl. (8)). Solange $a < a_{min}$ werden jedoch keine Vorfälle gemeldet (vgl. Gl. (13)).

Bei geringer Interdependenz (vgl. Abb. 3 (a)) liegt ohne Audits nur das Gleichgewicht $\left(0{,}0{,}\tilde{x}_2(0{,}0)\right)$ vor. Meldungen können durch $a \geq a_{min}$ erwirkt werden. Wenn $a \gg a_{min}$, dann steigen die IT-Sicherheitsinvestitionen der Agenten über ein sozial optimales Niveau hinweg (vgl. $+$ und Quadrat in Abb. 3 (a)).

Bei hoher Interdependenz (vgl. Abb. 3 (b)) liegt ohne Audits nur das Gleichgewicht $(0{,}0{,}0)$ vor, indem Agenten nicht in Sicherheit investieren. Audits können in diesem Fall am effektivsten sein. Bei einer Audit-Wahrscheinlichkeit $a < a_{min}$ entstehen zwei weitere Gleichgewichte $(a, 0, \tilde{x}_{1,2}(0, a))$, die immer gemeinsam vorliegen (vgl. Argumentation zu Gl. (30)). Mit Audits $a \geq a_{min}$ werden Meldepflichten durchgesetzt. Es existiert dann nur noch das Gleichgewicht $\left(a, 1, \tilde{x}_2(1, a)\right)$.

Gleichgewichte des Spiels. In der Fläche unter den Linien in Abb. 2 (b) existiert das Gleichgewicht $\left(\tilde{a} = a_{min}, \tilde{t} = 1, \tilde{x}_2(1, a_{min})\right)$. Hier werden Audits, die grundsätzliche Anreize zur Meldung von Vorfällen schaffen, eingeführt (vgl. Gl. (17)). **Meldepflichten mit Audits und Sanktionen lohnen sich insbesondere bei hoher Interdependenz, geringen indirekten Kosten, hoher Effektivität von zentralen Instanzen sowie geringer Fehler-Wahrscheinlichkeit von Angriffserkennungssystemen.** Wenn Agenten aufgrund hoher Interdependenz keine Anreize zur Investition in Sicherheit haben (starke Steigung der Linien in Abb. 2 (b) für $\gamma = .749$), stimulieren Audits IT-Sicherheitsinvestitionen.

In der Fläche über den Linien in Abb. 2 (b) werden keine Audits eingeführt. Es bestehen bis zu drei Gleichgewichte (vgl. letzter Abschnitt). Verglichen mit einem sozialen Planer ist der Prinzipal eher bereit, Meldepflichten zu realisieren (vgl. die Flächen in Abb. 2 (a) und (b), in denen $t^* = \tilde{t} = 1$ gilt).

Die Audit-Wahrscheinlichkeit a_{min} steigt mit den indirekten Kosten q_2 (vgl. Gl. (26)). Eine Steigerung der Fehlerrate ϵ senkt die Linien in Abb. 2 (b) Richtung Abszisse: Weniger Vorfälle werden gefunden und gemeldet (vgl. Abb. 1). Hierdurch steigen die erwarteten Sanktionen bei den Agenten. Beides reduziert die Effektivität von Audits.

6 Diskussion

Unser Prinzipal-Agent-Modell deckt wichtige Bestandteile von Meldepflichten für IT-Sicherheitsvorfälle in einer Ökonomie ab (Kapitel 2), jedoch kann es die Realität nicht vollständig abbilden. Dennoch lassen sich aus unserem Vier-Parameter-Modell erste Ergebnisse zur Beantwortung der von uns identifizierten Forschungsfrage ableiten. Diese Ergebnisse und die daraus zu ziehenden Schlussfolgerungen werden im nächsten Abschnitt zusammengefasst (Abschnitt 6.1). Anschließend geben wir einen Ausblick zur Erweiterung unseres Beitrags, um die modellierte Situation noch realistischer darzustellen (Abschnitt 6.2).

6.1 Schlussfolgerungen

Meldepflichten *ohne* Audits (unabhängig von Sanktionen) erzeugen kaum Anreize zur Meldung von IT-Sicherheitsvorfällen durch Marktteilnehmer, solange Meldungen mit potenziellen indirekten Kosten einhergehen. In diesem Fall tätigen Marktteilnehmer IT-Sicherheitsinvestitionen im Eigeninteresse. Diese Investitionen liegen unter dem sozial optimalen Niveau. Negative Externalitäten werden vereinzelt bei denjenigen Marktteilnehmern internalisiert, die den Meldepflichten trotz fehlender Anreize nachkommen, und hierdurch entstehende indirekte Kosten tragen.

Meldepflichten *mit* Audits *und* Sanktionen ändern die Anreizsituation und können zur Steigerung von IT-Sicherheitsinvestitionen in einer Ökonomie führen. Dabei können die IT-Sicherheitsinvestitionen von Marktteilnehmern bis über ein sozial optimales Niveau hinweg steigen. Angenommen die Sanktionen entsprächen der Höhe der direkten Kosten eines IT-Sicherheitsvorfalls, dann ist die optimale Audit-Wahrscheinlichkeit von den indirekten Kosten eines Vorfalls abhängig. Bei gleich hohen indirekten Kosten, direkten Kosten sowie Sanktionen, muss die Audit-Wahrscheinlichkeit in einer Ökonomie auf 50 % justiert werden, um Anreize zur Einhaltung von Meldepflichten zu erzeugen. Gemäß dem statistischen Bundesamt existierten in Deutschland im Jahr 2012 ca. 80 000 Unternehmen mit mehr als 50 Mitarbeitern [33]. Zählen alleine diese Unternehmen zu den betroffenen Marktteilnehmern, so würden Meldepflichten in Deutschland ca. 40 000 Audits – in einem zu definierenden Zeitraum – erfordern. Wenn durch diese Audits alle betroffenen Marktteilnehmer IT-Sicherheitsvorfälle melden, dann werden negative Externalitäten von allen Betroffenen internalisiert.

Will man die Anzahl der Audits senken, müssen die Sanktionen erhöht werden. Damit schadet man aber Marktteilnehmern, die ihre IT-Sicherheitsvorfälle aus reiner Unwissenheit nicht melden. Anreize zur Einhaltung von Meldepflichten wirken also nicht in jedem Fall wohlfahrtssteigernd. Aus unserer Analyse geht hervor, dass Audits die über eine grundsätzliche Anreizschaffung zur Meldung von Vorfällen hinausgehen zu negativen Wohlfahrtseffekten führen. Im Modell wurde bislang kein Over-Reporting berücksichtigt, das jedoch vorstellbar (und von anderen Meldepflichten bekannt) ist und der Informationsqualität schadet.

Unter den im Modell getroffenen Annahmen lassen sich Meldepflichten am ehesten bei starker Interdependenz zwischen IT-Systemen in einer Ökonomie begründen. Es stellt sich zudem heraus, dass die Einführung von Meldepflichten nur unter optimistischen Annahmen über die Wirkung einer gut informierten zentralen Instanz sinnvoll ist. Diesen Annahmen fehlt es jedoch an wissenschaftlicher Evidenz, sodass Forschungsbedarf besteht. Es ist beispielsweise fraglich, wie effektiv die Weitergabe eines von einer zentralen Instanz erstellten Lagebildes über Vorfälle an die Marktteilnehmer sein kann. Außerdem sollten die durch eine Einbeziehung der Öffentlichkeit in den Verteilungsprozess von Vorfällen entstehenden Effekte evaluiert werden [3,4]. Regulierer, die Meldepflichten einführen wollen, sind hier in der Bringschuld, die Wirksamkeit der Meldepflichten zu belegen.

6.2 Ausblick

Um die Kernaussagen von Meldepflichten für IT-Sicherheitsvorfälle zu ermitteln, haben wir unser Modell bewusst einfach gehalten. Wir nutzen Sicherheitsaudits und Sanktionen, um Anreize für Meldungen durch Marktteilnehmer zu schaffen. Dieses Vorgehen ist aus der aktuell diskutierten NIS-Richtlinie [12] begründet.

Es sind verschiedene Erweiterungen unseres Modells denkbar. Zum einen könnte die Meldung von IT-Sicherheitsvorfällen und deren effektive Verwertung nicht als Reduktion der Interdependenz, sondern als Senkung der Vorfall-Wahrscheinlichkeit interpretiert werden [32]. Die ließe sich z. B. durch einen Effekt auf die Produktivität von IT-Sicherheitsinvestitionen in das Modell aufnehmen. Offen bleibt auch, welche Ergebnisse sich aus einer Modellierung endogener Investitionen in technische oder organisatorische Kontrollmechanismen für IT-Sicherheitsvorfälle ergeben.

Nicht zuletzt könnten die über unser Modell bestimmten Kombinationen aus Audit-Wahrscheinlichkeiten und Sanktionen, die zu effektiven Meldepflichten führen, einem Realitätscheck unterzogen werden. Ein Vergleich mit den Bußgeldvorschriften aus § 149 Abs. 2 TKG liegt nahe, um Aufschluss über die Durchsetzbarkeit der aktuell diskutierten NIS-Richtlinie und den potenziell aus dieser Richtlinie abgeleiteten Gesetzen zu bekommen.

Literatur

1. Anderson, R.: Why information security is hard – An economic perspective. In: 17th Annual Computer Security Applications Conference, New Orleans, S. 358–365 (2001)
2. Anderson, R.: Security engineering: A guide to building dependable distributed systems. Wiley (2008)
3. Anderson, R., Böhme, R., Clayton, R., Moore, T.: Security economics and the internal market. European Network and Information Security Agency (2008)
4. Anderson, R.: EU cyber security directive considered harmful, https://www.lightbluetouchpaper.org/2013/02/08 (Abgerufen: 04.12.2014)
5. Böhme, R.: Wann sind IT-Security-Audits nützlich? In: Proceedings of the Wirtschaftsinformatik, Zürich, S. 385–394 (2011)
6. Böhme, R., Laube, S.: Das IT-Sicherheitsgesetz. In: Baetge, J., Kirsch, H. (Hrsg.) Mittelstand im Blick: Compliance und Risikomanagement, IDW Verlag, Düsseldorf, S. 17–36 (2014)
7. Bundesministerium des Innern: Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme. (Stand: 18.08.2014)
8. California State Senate: Assembly Bill 700. (2002)
9. Cavusoglu, H., Mishra, B., Raghunathan, S.: The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. IJEC 9 (1), S. 70–104 (2004)
10. Cavusoglu, H., Mishra, B., Raghunathan, S.: The value of intrusion detection systems in information technology security architecture. ISR 16 (1), S. 28–46 (2005)
11. European Commission: Report on the outcome of the review of the EU regulatory framework for electronic communications networks and services in accordance with Directive 2002/21/EC and summary of the 2007 reform proposal. COM (2007) 696 rev 1 (2007)

12. European Commission: Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. COM (2013) 48 final (2013)
13. Fischer-Hübner, S.: IT-Security and privacy. Springer, Berlin et al. (2001)
14. Gal-Or, E., Ghose, A.: The economic incentives for sharing security information. ISR 16 (2), S. 186–208 (2005)
15. Gao, X., Zhong, W., Mei, S.: A game-theoretic analysis of information sharing and security investment for complementary firms. JORS 65 (11), S. 1682–1691 (2013)
16. Gao, X., Zhong, W., Mei, S.: Security investment and information sharing under an alternative security breach probability function. Inf Syst Front, S. 1–16 (2013)
17. Gordon, L., Loeb, M.P.: The economics of information security investment. ACM Transactions on Information and System Security (TISSEC) 5 (4), S. 438–457 (2002)
18. Gordon, L., Loeb, M.P., Zhou, L.: The impact of information security breaches: Has there been a downward shift in costs? JCS 19 (1), S. 33–56 (2011)
19. Gordon, L., Loeb, M.P., Lucyshyn, W.: Sharing information on computer systems security: An economic analysis. JAPP 22 (6), S. 461–485 (2003)
20. Hausken, K.: Information sharing among forms and cyber attacks. JAPP 26 (6), S. 639–688 (2007)
21. Hiller, J.S., Russell, R.S.: The challenge and imperative of private sector cybersecurity: An international comparison. CLSR 29 (3), S. 236–245 (2013)
22. Iheagwara, C.: The effect of intrusion detection management methods on the return on investment. Computer & Security 23 (3), S. 213–228 (2004)
23. Khouzani, M., Pham, V., Cid, C.: Incentive engineering for outsourced computation in the face of collusion. In: Workshop on the Economics of Information Security, Pennsylvania State University (2014)
24. Kunreuther, H., Heal, G.: Interdependent security. J Risk Uncertain 26 (2/3), S. 231–249 (2003)
25. Laffont, J., Martimort, D.: The theory of incentives: The principal-agent model. Princeton University Press, Princeton (2002)
26. Lippmann, R., Haines, J., Fried, D., Korba, J., Das, K.: The 1999 DARPA off-line intrusion detection evaluation. Comput Netw 34 (4), S. 579–595 (2000)
27. Liu, D., Ji, Y., Mookerjee, V.: Knowledge sharing and investment decisions in information security. DSS 52 (1), S. 95–107 (2011)
28. Macho-Stadler, I., Pérez-Castrillo, D.: Principal-agent models. In: Meyers, R. (Hrsg.) Encyclopedia of complexity and systems science, Volume 1., Springer, New York, S. 6977–6990 (2009)
29. National Conference of State Legislatures: State security breach notification laws, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (Abgerufen: 04.12.2014)
30. Neilsen, M.: Privacy Amendment (Privacy Alerts) Bill 2013. Bill Digest No. 146 (2013)
31. Ng, D., Stoeckenius, J.: Auditing: Incentives and truthful reporting. JAR 17, S. 1–24 (1979)
32. Öğüt, H., Memon, N., Raghunathan, S.: Cyber insurance and IT security investment: Impact of interdependent risk. In: Workshop on the Economics of Information Security, Harvard (2005)
33. Statistisches Bundesamt: Statistisches Jahrbuch: Deutschland und Internationales. Statistisches Bundesamt, Wiesbaden (2013)
34. Symantec: Internet security threat report 2014. Technischer Report, Symantec (2014)
35. Winn, J.: Are better security breach notification laws possible? BTLJ 24 (3) (2009)

7 Anhang

Tabelle 1. Symbolverzeichnis

Sym.	Typ	Bedeutung	Sym.	Typ	Bedeutung
x_i	Wahlm.	IT-Sich.-investition	L	Funktion	Summe Kosten
t_i	Wahlm.	Meldungs-Wkt.	η	Funktion	Reduktion von γ
a	Wahlm.	Audit-Wkt.	P	Funktion	Vorfall-Wkt.
S	Wahlm.	Sanktionen	c	Funktion	Kostenfunktion
q_2	Parameter	Indirekte V.-Kosten	SV	ZV	Sicherheitsvorfall
γ	Parameter	Interdependenz	E	ZV	Vorfall entdeckt
ϵ	Parameter	Fehlerrate AES	A	ZV	Sicherheitsaudits
b	Parameter	Eff. bei Meldungen	α_i	Real. ZV	Real. von SV
n	Konstante	Anzahl Agenten	$\hat{\alpha}_i$	Real. ZV	Realisation von E
q_1	Konstante	Direkte V.-Kosten	$\tilde{\alpha}_i$	Real.	Vorfall-Meldung
β	Konstante	Sich.-produktivität	ψ	Real. ZV	Realisation von A

(Sym.: Symbol; Sich.: Sicherheits-; Wahlm.: Wahlmöglichkeit; Wkt.: Wahrscheinlichkeit; ZV: Zufallsvariable; AES: Angriffserkennungssystem; Real.: Realisation; V.: Vorfall; Eff.: Effektivität zentrale Instanz)

7.1 Soziales Optimum

$$\text{Aus Gl. (9): } (x^*, t^*) = \arg\min_{x,t} c(x, x, t, t). \tag{18}$$

Meldewahrscheinlichkeit. Erste und zweite Ableitung von Gl. (18):

$$\frac{\partial c}{\partial t} = (1-\epsilon)\cdot\ P(x^*)\cdot((1-\ P(x^*))\cdot(\gamma\cdot q_2\cdot\eta(t) - b\cdot\gamma\cdot L(t)) + q_2) \tag{19}$$

$$\frac{\partial^2 c}{\partial t^2} = -2\cdot b\cdot\gamma\cdot q_2\cdot(1-\epsilon)^2\cdot\big(1-P(x^*)\big)\cdot P(x^*) < 0. \tag{20}$$

Aus Gl. (20) ergibt sich, dass die Kostenfunktion unabhängig von x^* für $b > 0$ und $\gamma > 0$ konkav in t verläuft. Es existiert ein lokales Maximum, sodass $t^*(x^*) \in \{0{,}1\}$ gilt. Hierdurch ist Gl. (10) motiviert.

IT-Sicherheitsinvestition. Über die erste Ableitung von Gl. (18):

$$\frac{\partial c}{\partial x} = \big[\gamma\cdot\eta(t^*)\cdot\big(1-P(x)\big) + \big(1-\gamma\cdot\eta(t^*)\cdot P(x)\big)\big]\cdot L(t^*, 0)\cdot P'(x) + 1. \tag{21}$$

Über die Nullstelle der Ableitung ergibt sich ein lokales Minimum (vgl. Gl. (11)):

$$x^*(t^*) = -\frac{\log\left(\frac{\gamma\cdot\eta(t^*)+1}{4\cdot\gamma\cdot\eta(t^*)} - \sqrt{\frac{(\gamma\cdot\eta(t^*)+1)^2}{16\cdot\gamma^2\cdot\eta(t^*)^2} - \frac{1}{2\cdot\gamma\cdot\log(\beta)\cdot\eta(t^*)\cdot L(t^*,0)}}\right)}{\log(\beta)}. \tag{22}$$

7.2 Nash-Gleichgewicht

$$\tilde{a}(\tilde{x}, \tilde{t}) = \arg\min_{a} c(x_i^+, x_{1-i}^+, t_i^+, t_{1-i}^+, a) \text{ u. d. B.:} \tag{23}$$

$$(x_i^+, t_i^+) = \arg\min_{x_i, t_i} c_i(x_i, x_{1-i}, t_i, t_{1-i}, a) \text{ wobei } x_{i,1-i} \geq 0. \quad (24)$$

Meldewahrscheinlichkeit Agenten: Beste Antwort und Gleichgewicht.
Ansatz aus Gl. (24). Die erste Ableitung nach t_i lautet:

$$\frac{\partial c_i}{\partial t_i} = \underbrace{P_i(x_i, x_{1-i}, t_{1-i})}_{>0} \cdot \underbrace{(1-\epsilon) \cdot (q_2 - a \cdot (q_2 + S))}_{\text{abhängig von } a,S \text{ und } q_2}. \quad (25)$$

Falls $a = 0 \wedge q_2 > 0$ hat kein Agent Bereitschaft zu melden: $\partial c_i / \partial t_i > 0$. Im Gleichgewicht (gegenseitig beste Antworten) gilt dann der Randwert $\tilde{t}(\tilde{x}, 0) = 0$. Für $a = 0 \wedge q_2 = 0$ folgt $\partial c_i / \partial t_i = 0$ und Agenten sind indifferent bzgl. der Meldung. Für $a > 0 \wedge q_2 > 0$ kann ein Agent Anreize zur Meldung bekommen. Sei $a = a_{min}$. Über die Nullstelle des zweiten Teils aus Gl. (25) folgt:

$$0 = (1-\epsilon) \cdot \left(q_2 - a_{min} \cdot (q_2 + S)\right) \Leftrightarrow a_{min} = \frac{q_2}{q_2 + S}. \quad (26)$$

Falls $a_{min} \geq \frac{q_2}{q_2+S}$ sind Anreize zur Meldung vorhanden, d. h. $\tilde{t}(\tilde{x}, a_{min}) = 1$. Aus dieser Argumentation folgt die Fallunterscheidung in Gl. (13).

IT-Sicherheitsinvestition Agenten: Beste Antwort und Gleichgewicht.
Ansatz aus Gl. (24). Die erste Ableitung lautet:

$$\frac{\partial c_i}{\partial x_i} = \left(1 - \gamma \cdot \eta(t_{1-i}) \cdot P(x_{1-i})\right) \cdot L_i(t_i, a) \cdot P'(x_i) + 1. \quad (27)$$

Über die Nullstelle der ersten Ableitung ergibt sich die beste Antwort:

$$x_i^+(x_{1-i}, t_i, t_{1-i}, a) = \sup\left\{ -\frac{\log\left(\frac{1}{\log(\beta) \cdot L(t_i, a) \cdot (1 - \gamma \cdot \eta(t_{1-i}) \cdot \beta^{-x_{1-i}})}\right)}{\log(\beta)}, 0 \right\}. \quad (28)$$

Dieser Ausdruck entspricht Gl. (14). Die IT-Sicherheitsinvestition im Gleichgewicht entspricht den gegenseitig besten Antworten $\tilde{x}(\tilde{t}, a) = x_i^+(\tilde{x}, \tilde{t}, a)$:

$$\tilde{x}_{1,2}(\tilde{t}, a) = -\frac{\log\left(\frac{1}{2 \cdot \gamma \cdot \eta(\tilde{t})} \pm \sqrt{\frac{1}{4 \cdot \gamma^2 \cdot \eta(\tilde{t})^2} - \frac{1}{\gamma \cdot \log(\beta) \cdot \eta(\tilde{t}) \cdot L(\tilde{t}, a)}}\right)}{\log(\beta)}; \tilde{x}_3(\tilde{t}, a) = 0. \quad (29)$$

Diese drei Gleichgewichte entsprechen Gl. (15). Existenz von $\tilde{x}_1(\tilde{t}, a)$ und $\tilde{x}_3(\tilde{t}, a)$:

$$-\frac{\log\left(\frac{1}{2 \cdot \gamma \cdot \eta(\tilde{t})} + \sqrt{\frac{1}{4 \cdot \gamma^2 \cdot \eta(\tilde{t})^2} - \frac{1}{\gamma \cdot \log(\beta) \cdot \eta(\tilde{t}) \cdot L(\tilde{t}, a)}}\right)}{\log(\beta)} \geq 0$$

$$-\frac{\log\left(\frac{1}{\log(\beta) \cdot L(t_i, a) \cdot (1 - \gamma \cdot \eta(t_{1-i}) \cdot \beta^{-0})}\right)}{\log(\beta)} \geq 0. \quad (30)$$

Beide Bedingungen sind für $\gamma \geq \frac{\log(\beta) \cdot L(\tilde{t}, a) - 1}{\log(\beta) \cdot \eta(\tilde{t}) \cdot L(\tilde{t}, a)}$ erfüllt.