Kommunikation der IT-Sicherheitslage: Ein Index der Cyber-Sicherheit für den deutschsprachigen Raum (Position Paper)

Sebastian Lorkowski

Juniorprofessur für Wirtschaftsinformatik, insbesondere IT-Sicherheit
Westfälische Wilhelms-Universität Münster
Leonardo-Campus 3
48149 Münster
sebastian.lorkowski@wi.uni-muenster.de

Abstract: Die steigenden Zahl von Angriffen auf IT-Systeme in Europa hat die EU veranlasst, einen Vorschlag zur Meldepflicht von Cyberangriffen einzureichen. Die Begründung liegt im Mangel verlässlicher Kennzahlen und verwertbaren Daten. Datenlieferanten sind meist Institutionen, wie Hersteller von Sicherheitssoftware, deren Vorgehen teilweise intransparent und Interessen abhängig von den Ergebnissen sind. Nicht nur die EU, sondern auch andere Entscheidungsträger, wie Risikomanager und Sicherheitsbeauftragte sind von diesem Mangel betroffen. Die Medien- und unternehmensinterne Kommunikation erfolgt auf Basis der vorhandenen Daten. Eine Folge ist, dass bei Konsumenten der Eindruck steigender Cyberbedrohungen entsteht. Der Index der Cybersicherheit (ICS) ist eine monatlich erhobene Kennzahl, die die wahrgenommenen Risiken von IT-Sicherheitsexperten misst. Die Teilnehmer stellen durch eine monatlichen Umfrage ihr IT-Sicherheitsempfinden des Vormonats dar. Das Ergebnis der Umfrage wird auf den Indexwert abgebildet. Das ICS Projekt wurde in den USA von Daniel E. Geer und Mukul Pareek entwickelt und ist dort im April 2011 gestartet. Angelehnt an Konzepten und Vorbildern anerkannter Finanzindikatoren bildet der Index einen robusten Indikator, der die Anonymität der Unternehmen bewahrt und viele Ansprüche der Märkte erfüllt. Der Index kann als unabhängiger Benchmark für Entscheidungen und in der internen Unternehmenskommunikation verwendet werden.

1 Einleitung

Am 07. Februar 2013 veröffentlichte die Europäischen Kommission und die Hohe Vertreterin der Union für Außen- und Sicherheitspolitik eine Pressemitteilung, in der die Forderung nach einer Meldepflicht von Cyberangriffen auf Unternehmen formuliert wird [MAK13]. Das Für und Wider wird inzwischen auch in Deutschland angeregt diskutiert. Als Grund für die Einführung der Meldepflicht wird ein Problem angeführt, auf das im Forschungsfeld der IT-Sicherheit immer wieder verwiesen wird: das Fehlen verlässlicher und konsistenter Daten, auf deren Basis Entscheidungen getroffen werden können, vgl. [BKA10, Seite 7]. Gleichzeitig besteht nach wie vor die Herausforderung, dass Unternehmen ihre IT-Sicherheitsvorkommnisse aus Angst vor bürokratischem Aufwand und Image-

verlust[1] nicht veröffentlichen wollen. Aktuell werden viele Mikrodaten für Statistiken von den Herstellern von Sicherheitssoftware erstellt. Das Hauptinteresse dieser Autoren ist jedoch, ihr Produkt zu verkaufen. Zusätzlich werden unabhängige Daten durch Institutionen wie bspw. das Computer Security Institute (CSI) oder Eurostat erhoben. Diese Daten sind für unsere Trendanalysen nicht verwendbar, weil sie nur einmalig zu einem bestimmten Thema von Interesse erhoben werden [Eur10] oder weil sie sich nicht auf den deutschen Markt beziehen [CSI10]. Deshalb ist ihre Prognosefähigkeit begrenzt. Neben den bereits genannten Studien basieren viele andere, wie bspw. die KES Studie[2], die KPMG-Studien zur Wirtschaftskriminalität[3] oder die Sicherheitsstudien der Information Week[4] auf Umfragen. Auf Grund Ihres jährlichen Turnus stehen Analyseergebnisse nicht zeitnah zur Verfügung. Um einen jährlichen Trend aus den verschiedenen Quellen herauszulesen, müssten die Umfragen der verschiedenen Anbieter detaillierter analysiert werden, wie bspw., ob die Zusammensetzung der Teilnehmer oder der Fragebogen geeignet sind, um Forschungsfragen zu beantworten.

Auf Grund des gestiegenen Interesses an IT-Sicherheit, informieren die Medien inzwischen direkt über die Ergebnisse der Sicherheitsberichte der Hersteller von Sicherheitssoftware. Die Medienkonsumenten, die in den letzten 12 Monaten zuvor etwas über Cyber-Kriminalität gehört haben, weisen eine höhere Besorgnis gegenüber denen auf, die nichts gehört haben [Eur12, Seite 60]. So ändern einige Konsumenten auf Grund des Gelesenen ihr Verhalten im Umgang mit Internetdienstleistungen [Eur12, Seite 28ff.]. Da die Unternehmen im Allgemeinen nicht gewillt sind, über Vorkommnisse Auskunft zu geben, sind die Medien auch auf die Daten angewiesen, die über Dritte an die Öffentlichkeit kommen, oder Statistiken von Herstellern, die an der erhöhten Besorgnis ihrer Kunden verdienen. Risikomanager und Sicherheitsbeauftragte sind neben den Daten Ihrer Organisation zur Analyse von Trends auch auf die externen Daten angewiesen. Dramatisierte Berichte und intransparente Mikrodaten führen hier zu Fehlentscheidungen und Verunsicherung. In vielen Branchen findet ein intensiver Austausch zwischen Unternehmen über IT-Sicherheit nicht statt, weil hier Ängste vor Imageverlust und Informationsweitergabe herrschen. Ein weiteres Problem dieser Sicherheitsreports ist, dass sie das gesamte Vorjahr betrachten und somit als Entscheidungsgrundlage für aktuelle Trends oder Vorfälle der IT-Sicherheit nicht verwendet werden können.

In dieser Hinsicht sind in Deutschland aktuelle wichtige Entwicklungen der Aufbau des Computer Emergency Response Team-Verbunds (CERT-Verbund)[5] und die Allianz für

[1] Siehe Zeitungsartikel aus: Die Welt, Wirtschaft lehnt Meldepflicht für Cyber-Angriffe ab, URL: `http://www.welt.de/wirtschaft/webwelt/article113456502/Wirtschaft-lehnt-Meldepflicht-fuer-Cyber-Angriffe-ab.html` (Stand: 25.04.2013) oder auch FAZ, Unternehmen wehren sich gegen Meldepflicht, URL: `http://m.faz.net/;fitScript=0/aktuell/sport/cyber-attacken-unternehmen-wehren-sich-gegen-meldepflicht-12054706.html` (Stand: 25.04.2013)

[2] Siehe unter `http://www.kes.info` (Stand: 28.06.2013)

[3] Studie für 2012 unter `http://www.kpmg.de/Themen/33581.htm` (Stand: 28.06.2013)

[4] Studie für 2013 unter `http://reports.informationweek.com/abstract/21/10696/Security/research-2013-strategic-security-survey.html` (Stand: 28.06.2013)

[5] Siehe unter `http://www.cert-verbund.de` (Stand 27.06.2013)

Cyber-Sicherheit (ACS)[6], ein Projekt des BSI mit mittlerweile mehr als 290 Teilnehmern [All13, Seite 4]. Beide Institutionen fördern mit ihrer Arbeit den Austausch über IT-Sicherheit mit den Unternehmen und präsentiert praktische Lösungsansätze. Der ICS als Kennzahl oder Indikator leistet keinen konkreten Vorschlag zur Verbesserung der IT-Sicherheit in einem Unternehmen. Ein wichtiger Unterschied zu diesen Projekten ist der Zusammensetzung der Teilnehmer zu erkennen.[7] Die ACS spricht Unternehmen an, die IT-Sicherheitsprodukte vertreiben, die aus den genannten Gründen die Aussagekraft des ICS schwächen könnten.

Daher ist der Bedarf nach unabhängigen Daten gegeben. Ob und wann die EU die Meldepflicht durchsetzen kann und für wen diese Daten dann zur Verfügung stehen, ist offen. Verbunden mit den Kommunikationshemmnissen der Unternehmen stellt sich jedoch die Frage: *Wie muss eine Kennzahl der IT-Sicherheit gestaltet sein, damit deutsche Unternehmen ihre IT-Sicherheit nach Außen kommunizieren und ein Mehrwert an Information entsteht?* Ein Grund, warum die Unternehmen in Zukunft die Kommunikation nach Außen angehen werden müssen, ist der Wandel der Priorität des Themas IT-Sicherheit in der Gesellschaft. Die Wichtigkeit in den Organisationen lässt sich aus den steigenden Investitionen [Pri13, Seite 7] ablesen, die auch gerechtfertigt werden müssen. Ein transparent gestalteter, stimmungsbasierter Index ist unser Ansatz, der die aufgeführten Anforderungen erfüllt und den Bedenken entgegen kommt. In diesem Paper möchten wir das ICS Projekt vorstellen, dass 2011 von Daniel E. Geer und Mukul Pareek in den USA gestartet[8] [Gee10, Gee11, GP12] und in diesem Jahr in Deutschland etabliert wird.[9] Der ICS ist ein stimmungsbasierter Index, der auf einer monatlichen Umfrage von deutschen IT-Sicherheitsexperten basiert [GP12]. Dan Geer bezeichnet den ICS als ein Standbein einer IT-Sicherheitsstrategie und als Kennzahl zum Messung der aktuellen IT-Sicherheitslage [Gee11, Seite 86].

Ein langfristig angelegtes Projekt, wie der ICS, bringt eine längere Begleitung der Teilnehmer mit sich. Wir möchten diesen Umstand auch dazu nutzen, um herauszufinden, inwiefern die Projektteilnahme Auswirkungen auf die Unternehmen hat. Die Umfrage wird von einem Mitarbeiter des Unternehmens ausgefüllt, der im Regelfall ein Mitarbeiter des höheren Managements ist, der die operativen Daten der Vorfälle nicht kennt und diese eventuell zur Beantwortung des Fragebogens erst anfordert. Andererseits ist eine top-down Kommunikation von Rückmeldungen aus dem ICS Projekt durch das Management möglich. Daraus schließt sich für uns die forschungsbegleitende Frage an: *Steigert die Teilnahme eines Unternehmens die interne Unternehmenskommunikation?*

In Kapitel 2 werden die Anforderungen an den Index erläutert und auf das allgemeine Design des ICS eingegangen. Daraus wird im Folgekapitel 3 die Berechnungslogik aus den Anforderungen abgeleitet. Da ein stimmungsbasierter Index stark von der Auswahl der Teilnehmer abhängig ist, gehen wir auf den Rekrutierungsprozess in einem eigenen Kapi-

[6] Siehe unter `https://www.allianz-fuer-cybersicherheit.de` (Stand 27.06.2013)

[7] Diese Aussage bezieht sich auf den Dialog von Entwicklern und Herstellern von IT-Sicherheitsprodukten mit den Nutzern; siehe unter `https://www.allianz-fuer-cybersicherheit.de/ACS/DE/allgemeineInformationen/Allianz/Akteure&Aktivitaeten/Teilnehmer/teilnehmer_node.html` (Stand 27.06.2013)

[8] Siehe US-Projekt unter `http://www.cybersecurityindex.org`

[9] Siehe deutsches Projekt unter `https://www.cybersecurityindex.de`

tel 4 gesondert ein. Das Design des Fragebogens, der den Teilnehmern zur Beantwortung vorgelegt wird, wird im Kapitel 5 erörtert. In Kapitel 6 wird auf die Abweichungen des ICS vom optimalen Vorgehen eingegangen. Der ICS wird für weitere Projekte Themen bieten, die wir als Ausblick in Kapitel 7 entwickeln. Das letzte Kapitel wird eine kritische Würdigung des ICS vornehmen und auf Randbedingungen aufmerksam machen, die für dieses Projekt gelten.

2 ICS Konzeption

> Das Furchtbarste so sagen, dass es nicht mehr furchtbar ist, dass es Hoffnung gibt, weil es gesagt ist. *Elias Canetti (1905-94)*

Kennzahlen haben in der Volks- und Betriebswirtschaft eine längere Tradition als in der IT-Sicherheit. Preißler beschreibt Kennzahlen als "Größe, die einen quantitativ messbaren Sachverhalt in konzentrierter Form wiedergibt, die in zusammenfassender, teilweise auch vergröbernder Weise Zusammenhänge der wirtschaftlichen Arbeitsweise eines Unternehmens erläutert und veranschaulicht" [Pre08, Seite 11]. Die Politik und die Entscheider in der Wirtschaft benötigen transparent und unabhängig erstellte Informationen, um ihre Entscheidungen begründen und evaluieren zu können. Daten über IT-Sicherheit können durch drei Akteure gewonnen werden, durch die Angreifer, die Opfer und Dritte. Zu den Dritten zählen die bereits erwähnten Hersteller von Sicherheitssoftware, wie auch Chatrooms, in denen z.B. Händler Hehlerware anbieten. Die Kommunikation mit Kriminellen birgt generelle Problematiken, wie das Auffinden, das Gewinnen von Vertrauen, um an Informationen zu gelangen, Glaubwürdigkeit der Informationen und rechtliche Risiken.[8] Dritte, die eine transparente, objektive und unabhängige Darstellung der aktuellen IT-Sicherheitslage vermitteln, sind uns aus besagtem Grund nicht bekannt. Deshalb sollen die Informationen aus den angegriffenen Unternehmen selbst kommen, wie es auch die Politik fordert.

Bei Angriffen aller Art, auf rechtlicher Ebene wie auch bei Cyberangriffen, werden die Unternehmen zunächst als verantwortlich dargestellt, wodurch das Ansehen des Unternehmens Schaden nehmen kann [Ben97]. Die Konsequenz können aufwändige und kostenintensive Imagekampagnen zur Wiederherstellung desselbigen sein. Whistleblower oder Hacker legen immer wieder geheime Daten offen, bspw. Stratfor Daten in WikiLeaks durch das Hacker-Netzwerk Anonymous in 2012 [Han12]. Werden in Deutschland Kundendaten gestohlen, muss das Unternehmen nach §42a BDSG die betroffenen Kunden kontaktieren und somit die externe Kommunikation ohnehin aufnehmen. Damit die Organisationen bereit sind, die Information zu den Vorfällen zur Verfügung zu stellen, können Daten entweder anonymisiert erfasst werden oder nach der Erfassung unveröffentlicht bleiben. Um eine allgemeingültige Aussage über IT-Sicherheit zu fällen, muss der Vorfall aber nicht auf ein einzelnes Unternehmen zurückzuführen sein. Falls also die Mikrodaten der Kennzahl trotz jeglicher Vorkehrungen gestohlen werden, ist die Anonymisierung der Daten für das Design der Kennzahl die bessere Wahl, um die Unternehmen zur Teilnahme zu bewegen.

Zur Erstellung einer Kennzahl ist die Aggregation der Umfrageergebnisse notwendig. Verbreitet sind hier statistische Mittelwerte oder Extremwerte. Der Modalwert zeigt die IT-Sicherheit der Masse der Befragten an. Gezielte Angriffe auf Einzelunternehmen würden hier komplett entfallen. Der Modalwert ist deshalb, wie der Median, robust gegen Ausreißer. Der Median nimmt die Ausreißer erst ab einer erreichten Häufigkeit auf. Der einfache und gewichtete Durchschnitt ist empfindlich gegen Ausreißer, aber deshalb auch sensibel für Einzelvorfälle. Extremwerte kommen nicht in Betracht, da sie als Kennzahl eine Dramatisierung oder Beschönigung der IT-Sicherheitssituation bedeuten. Das statistisches Verfahren ist die Panelanalyse, da konstant die gleichen Individuen über einen längeren Zeitraum befragt werden. Der Median wäre die passende Wahl für die Kennzahl, wenn es sich um eine Einzelbefragung handeln würde, um durch die Ausreißer die Interpretation des Ergebnisses nicht zu verfälschen. Wir wählen jedoch den einfach gewichteten Durchschnitt, da die Aussage nicht auf einem einzelnen Kennzahlenwert liegt, sondern in der Interpretation des Trends im Zeitverlauf. Die Priorisierung und die Interpretation einer Frage ist für den einzelnen Teilnehmer für die Dauer des Projektes immer gleich. Eine Gewichtung des Durchschnittswertes könnte auf verschiedene Arten vorgenommen werden, z.B. eine Gewichtung der Fragen oder nach Unternehmensgröße. Wir gehen davon aus, dass unterschiedliche Branchen mit unterschiedlichen Sicherheitsproblemen zu kämpfen haben. Da die Kennzahl einen Querschnitt durch die deutsche Unternehmenslandschaft abbildet, und die Interpretation, die Priorität und Ausprägung einer Frage bspw. branchenspezifisch sein kann, sollen alle Vorkommnisse gleich gewichtet in die Kennzahl eingehen; vergleichbar mit dem ifo-Geschäftsklimaindex [ABS09, Seite 34].

Der ifo-Geschäftsklimaindex oder der europäische Purchasing Manager Index (PMI) sind in ihrer Konzeption ähnlich. Sie sind Panelbefragungen, in der Teilnehmer nicht-numerische Antworten auf Fragen zur Richtung einer Entwicklung ökonomisch relevanter Themen geben. Üblicherweise sind es ordinal skalierte Antworten, wie "gefallen", "unverändert" und "gestiegen". Durch einen Diffusionsindex werden die Antworten in einen Index transformiert, indem man den Antworten Zahlenwerte zuweist und diese zur Berechnung des Index heranzieht. Ein umfragebasierte Index hat darüber hinaus den Vorteil, dass aus jedem abgefragten Themenbereich ein Subindex erstellt werden kann. Die Vorgehensweise entspricht den von uns beschriebenen Anforderungen an eine Kennzahl. Abberger hat für den ifo-Geschäftsklimaindex gezeigt, dass der Index "starke Zusammenhänge mit Referenzreihen aus der amtlichen Statistik" [ABS09, Seite 34] aufweist, vgl. auch [SH02]. Zur Erlangung des Vertrauens der Teilnehmer soll die Konzeption des ICS sich an einem etablierten Verfahren orientieren. Ein Index repräsentiert die allgemeine IT-Sicherheitssituation gut, weil er nicht nur Vorkommnisse in einzelnen Unternehmen durch einen Durchschnitt glättet, sondern auch die Zeiträume repräsentiert, in denen keine Vorkommnisse auftreten oder neue Technologien Bedrohungen schmälern. Der Vorfall wird aber von seiner technologischen Basis abstrahiert, so dass auch zukünftige Angriffsszenarien durch das Konstrukt Bedrohung abgedeckt sind. Damit ist der ICS zukunftsfähig und ein breites Publikum ist in der Lage, die Bedrohung in ihrem Sinne zu interpretieren.

Zur Untersuchung eignen sich Längsschnitterhebungen, wie bspw. die Trendanalyse, sowie die Panelanalyse, von der die Kohortenstudie wiederum ein Spezialfall ist. Kopp

und Schäfers unterscheiden davon die Querschnittserhebungen, bei dem die Daten zu einem festen Zeitpunkt einmalig untersucht werden. Trend- und Panelanalyse unterschieden sich insofern, als dass bei der Trendanalyse die Teilnehmer für jede Untersuchung immer wieder neu zusammengestellt wird. Dadurch weisen Sie eine höhere Unabhängigkeit und Repräsentativität auf. Sie wird verwendet, wenn in einer Population nach allgemeingültigen Änderungen, d.h. Trends, gesucht werden [KS10, Seite 184ff.]. Bei der Panelanalyse bleiben die Teilnehmer die Gleichen, so dass die Möglichkeit entsteht, die Trends auf die individuellen Eigenheiten der Teilnehmer zurückzuführen [ER96, Seite 2]. Wenn Panelteilnehmer ein für die Analyse wichtiges Merkmal aufweisen, dass zu einem annähernd gleichem Zeitpunkt in deren Leben tritt, spricht man von einer Kohorte. Da die Teilnehmer jedoch kein persönliches Merkmal aufweisen, das wir untersuchen wollen, kann man beim ICS auch nicht von einer Kohorte sprechen. Die Rekrutierung von Teilnehmern für den ICS ist mit hohen Aufwänden verbunden, was auch auf die Sensibilität des Themas IT-Sicherheit zurückzuführen ist. Aus diesem Grund möchten wir die Analyse als Panel durchführen. Das wird auch die Möglichkeit bieten, bei der Auswertung auf individuelle oder Branchentrends einzugehen.

Nach Aussage der Europäischen Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik, nimmt die "Tragweite und Häufigkeit von Cybersicherheitsvorfällen" [MAK13] zu und nach Symantec, ein Hersteller von IT-Sicherheitssoftware, ist die Anzahl zielgerichteter Angriffe im Vorjahr um 42% gestiegen [Sym13]. Für die Angabe von Kosten gibt es in den Umfragen kein einheitliches Modell, welche Kosten aufgelistet werden und welche nicht [ABB$^+$12], doch ist durch den Trend steigender Kosten auch von einer steigenden Bedrohung auszugehen. Getz und Ulmer gehen auf die Möglichkeit ein, Diffusionsindizes monatlich, quartalsweise, halbjährig oder ganzjährig zu erstellen [GU90, Seite 17]. Um aus der Bedrohung den Trend ausreichend zu erfassen, wird die Umfrage den Teilnehmern, bestehend aus IT-Sicherheitsexperten deutscher Unternehmen, als monatlich wiederkehrender Fragebogen online zur Beantwortung vorgelegt.

Um den ICS zu etablieren, muss er für die Teilnehmer und Nutzer einen Mehrwert aufweisen. Der Mehrwert eines Index zeigt sich dann unter anderem durch die Nutzung der Kennzahl. Um das Vertrauen der Teilnehmer und der Nutzer zu gewinnen, soll der ICS transparent gestaltet werden. Ein Beispiel für Transparenz ist hierbei der DAX-30 Index, der aus den 30 größten und umsatzstärksten deutschen Unternehmen zusammengesetzt ist. In den Index fließen die Preise der Aktienkurse, die transparent an einem offenen Markt gehandelt werden, sowie Gewichtungen in Form von Streubesitzanteil-Marktkapitalisierung des Aktienbestands, die ebenfalls veröffentlicht werden, ein.[10] Darüber hinaus sind die Umsätze bekannt, so dass über die Zeit auch die umsatzstärksten deutschen Unternehmen transparent ermittelt werden können. Umgekehrt ist Subjektivität bei der Zusammensetzung der Teilnehmer kein Kriterium, das die Glaubwürdigkeit eines Index negativ beeinflusst. Der Dow-Jones-Index wird aus vom Wall-Street-Journal nach subjektiv ausgewählten Aktien zusammengesetzt. Der Schlüssel für den Erfolg eines Finanzindex ist die Transparenz und Konsistenz, so dass die Methode intersubjektiv nachvollzogen werden kann und somit Vertrauen schafft. Für den ICS folgt daraus, dass die vollständige

[10]Deutsche Börse, Selection Indices, URL: `http://www.boerse-frankfurt.de/en/basics+overview/indices/selection+indices` (Stand: 25.04.2013)

Berechnungslogik auf der Projektseite im Internet dargestellt wird. Für vollständige Nachvollziehbarkeit müssten auch die Mikrodaten veröffentlicht werden, was aber zur Wahrung der Anonymität der Teilnehmer nicht vorgesehen ist.

Ziel ist, den monatlichen ICS-Wert mit einer kurzen Erklärung auf der Webseite des Projektes zu publizieren. Diese Bekanntgabe ermöglicht auch Nichtteilnehmern die eingeschränkte Nutzung und unterstützt so die Verbreitung des ICS. Die Teilnehmer bekommen exklusiv eine detaillierte Analyse der Umfragedaten und die Subindizes der Kategorien zur Verfügung gestellt. Damit haben die Teilnehmer einen Benchmark, den sie zu ihrer eigenen Risikoabschätzung und für die interne Argumentation und Kommunikation nutzen können. Die Wirtschaftsprüfungsgesellschaft PricewaterhouseCoopers hat im aktuellen "Information Security Breaches Survey 2013" für Großbritannien herausgestellt, dass die ineffektive Kommunikation der Führung ein wichtiger Grund ist, warum Mitarbeiter nicht die richtigen Handlungen im Unternehmen vornehmen, um IT Risiken zu begegnen [Pri13, Seite 3]. Hier sehen wir auch den vorrangigen Nutzen bei den Subindizes, die sich konkret auf bestimmte Themen einschränken, da die Kommunikation in den Unternehmen sich konkret auf sicherheitsrelevante Bereiche bezieht und nicht die IT-Sicherheit allgemein. Die interne Nutzung des Index in den Unternehmen trägt ebenfalls zur Verbreitung bei und ist eine Möglichkeit, der Panelmortalität, d.h. dem Ausscheiden von Teilnehmern im Zeitverlauf, entgegen zu wirken.

3 Berechnung des ICS

Ausgangspunkt für die Berechnung des ICS ist ein Diffusionsindex, wie er bei den bekannten Finanzinstrumenten vorzufinden ist. Einfache Diffusionsindizes sind wertebereichgebunden, das heißt, sie bewegen sich in einem Wertebereich von bspw. 0 bis 100, vgl. [GU90, Seite 17].

$$index = 100\% * \text{\#gestiegen} + 50\% * (\text{\#unverändert}) \tag{1}$$

#gestiegen	Anzahl der Antworten, die auf eine Frage 'gestiegen' antworteten
#unverändert	Anzahl der Antworten, die auf eine Frage 'unverändert' antworteten

Wertebereich-gebundene Indikatoren werden verwendet, wenn das zu messende Konstrukt keinem Trend unterliegt. Der Indexwert bezieht sich dabei auf eine zeitliche Referenz, wie bspw. dem Vormonat. Sie werden häufig als Glättung für andere Indizes verwendet, um eine Glättung von Ausreißern vorzunehmen. Die alternative Darstellung des Diffusionsindex ist die Abbildung des Prozentwertes auf einen Zufallslauf. Zufallsläufe dienen der Trenddarstellung über längere Zeiträume. Problematisch ist hier die Deutung, weil der Indexwert selbst keine Aussage hat, da er auf einem willkürlich gewähltem Startwert basiert. Wichtig ist lediglich das Verhältnis der Kurve im Zeitverlauf. Ein unmittelbarer Trendvergleich von zwei Werten ist bei der absoluten Zahlendarstellung besser möglich, als bei wertebereich-gebundenen Indikatoren. Absoluten Zahlendarstellung benötigen einen Startwert, den wir willkürlich im Zeitpunkt t_0 bei 1000 festlegen.

Rensis Likert hat die 1932 ein Skalierungsverfahren vorgeschlagen, in dem Zustimmungs-

fragen mittels Rating-Skalen beantwortet werden [CD94, Lik32]. Da der ICS die Meinung der IT-Sicherheitsexperten zur Bedrohungsentwicklung des Vormonat messen soll, wird für die Beantwortung der Fragen eine 5-stufige Rating-Skala mit den Antwortmöglichkeiten "stark gefallen" (=-20%), "gefallen" (=-7,5%), "unverändert" (=+0%), "gestiegen" (=+7,5%) und "stark gestiegen" (=+20%) verwendet. Nach positiven Erfahrungen von Dillman bei Umfragen möchten wir ebenfalls die Antwortmöglichkeit "weiß nicht" (=0%) vorgeben [Dil99]. Diesen Antworten weisen wir die prozentualen Gewichtungen zu. Diese sind Erfahrungswerte aus dem US Projekt und werden zunächst in Deutschland übernommen. Wie die Teilnehmer die Antworten interpretieren und dementsprechend Vorfälle in ihrem Unternehmen, ist den Teilnehmern selbst überlassen. Da jedoch das Panel im Laufe der Zeit nur langsam wechselt, bleibt auch die Interpretation der Antwortmöglichkeiten relativ stabil.

Eine weitere Anforderung, die wir an den ICS haben, ist, dass sich konträre Antworten gegenseitig aufheben sollen. Diese Anforderung resultiert aus der einheitlichen Gewichtung aller Antworten. Die Verwendung von diskreten Raten in der Berechnungsformel des ICS erfüllt diese Anforderung nicht. Wendet man bei der Berechnung eines Monats die exakt inversen Antworten des Vormonats an, wird der Indexwert des Vormonats nicht erreicht.

$$ICS_t = ICS_{t-1} * (1 + s_t) \tag{2}$$

ICS_t ist der ICS zum Zeitpunkt t
s_t repräsentiert die in Prozentzahlen umgewandelten Antworten des Monats

Damit Antworten in unterschiedlichen Berechnungsperioden gleich gewichtet werden, wechselt die Berechnung von diskreten Raten auf kontinuierlichen Wachstumsraten. Deshalb wird die allgemeine Formel zur Berechnung des ICS wie folgt aussehen.

$$ICS_t = ICS_{t-1} * e^{s_t} \tag{3}$$

ICS_t ist der ICS zum Zeitpunkt t
s_t repräsentiert die in Prozentzahlen umgewandelten Antworten des Monats

4 Teilnehmer

Die Teilnehmerauswahl für einen stimmungsbasierten Index ist, wie auch für Umfragen generell, ein wichtiger Teil der Konzeption und Voraussetzung für die Glaubwürdigkeit [Gro89, Seite 81ff.]. Die möglichen Teilnehmer müssen bzgl. IT-Sicherheit einen breiten Überblick über ihr Unternehmen haben. In Bezug eines Rollenmodells betrifft das sowohl die höhere Managementebene, die im Falle eines größeren Vorfalls informiert wird, als auch die operativ arbeitenden Mitarbeiter, die bspw. die Aufnahme, Abwehr und Behebung von Schäden vornehmen. Andererseits gehen die Fragen von dem Faktor Bedrohung als Mittelpunkt aus und nicht von den konkreten Vorfällen. Der potentielle Teilnehmer muss in der Lage sein, den konkreten Vorfall in ein generisches Risiko für das Unternehmen zu abstrahieren. Die klassische Aufgabe der Bewertung von Risiken auf Basis aggregierter Kennzahlen liegt bei der Managementebene. Die operativ arbeitenden Mitarbeiter haben wahrscheinlich ein größeres Detailwissen, was in dieser Umfrage

jedoch nicht abgefragt wird. In größeren Unternehmen findet häufig auch eine höhere Spezialisierung der Mitarbeiter statt, so dass die gänzliche Übersicht nicht mehr durch Administratoren abgedeckt wird. Deshalb sind IT-Sicherheitsexperten in diesem Projekt in erster Linie Informationssicherheitsbeauftragte und Risikomanager. Analog zum ifo-Geschäftsklimaindex gehen wir bei Führungspersonen davon aus, dass sie "zeitnah über möglichst viele Informationen verfügen" [ABS09, Seite 39]. In kleineren Unternehmen kann es sein, dass diese Aufgabe klassischerweise vom Leiter der Administration ebenfalls ausgefüllt wird. Da aber speziell in größeren Unternehmen nicht davon ausgegangen werden kann, dass diese sich Zeit für eine monatliche Umfrage nehmen, sind auch die Mitarbeiter im Fokus, die direkt an diese Vorgesetzten berichten. Als weitere Gruppe möchten wir Forscher ansprechen, die sich praktisch im Feld bewegen und auch Entwicklungsleiter der Hersteller von Sicherheitsanwendungen.

Eine reine Zufallsauswahl aus einer Grundgesamtheit von deutscher Unternehmen würde zu Lasten der Teilnahme gehen und wird nicht umgesetzt. Die zufällige Auswahl von Teilnehmern aus verschiedenen IT-Sicherheitsbeauftragten ist in den meisten Unternehmen auch nicht möglich, da oft nur wenige auf die uns vorgegebenen Eigenschaften passen. Auch eine Fokussierung auf bestimmte Branchen oder Unternehmensgrößen erfolgt nicht.

Die Rekrutierung der Teilnehmer erfolgt durch ein Schneeballverfahren, das durch Kontakte der Organisatoren und deren Besuche von Konferenzen und Workshops initiiert wird. Die Interessenten können sich dann über die Webseite informieren, sich selbst über die Kontaktdaten bei den Teammitgliedern melden und ihren Teilnahmewunsch äußern. Eine Selektion bestimmter Unternehmen mit definierten Eigenschaften wird nicht vorgenommen. Außerdem werden die Rolle und Aufgaben der Person im Unternehmen, das Jahr, in dem der Teilnehmer im Unternehmen begonnen hat, die Größe des Unternehmens und die Branche erhoben. Darüber hinaus erfassen wir, ob es sich bei dem Unternehmen um einen Anbieter von IT Dienstleistungen handelt oder nicht. Auf Basis der Rolle bzw. den Aufgaben im Unternehmen wird vom Projektteam entschieden, ob die oben genannten Teilnahmebedingungen erfüllt sind. Die anderen Eigenschaften erfassen wir als sozioökonomische Faktoren, die zur Einschätzung der Repräsentativität des Panels und Berechnung von Trends als statistische Bedingung herangezogen werden.

Langfristig wird eine Teilnehmerzahl von 300 angestrebt. Vorbild für diese ist der Institute of Supply Management's (ISM) PMI, ein umfragebasisierter Index, dessen Umfrage von Einkaufsleitern in 300 Unternehmen beantwortet wird und in den USA eine hohe Reputation hat. Sobald 100 Unternehmen die Zusage zur Teilnahme erhalten haben, werden die Umfragen und die Erstellung des Index starten.

5 Der Fragebogen

Der Fragebogen, siehe Anhang A, ist in sechs Themenblöcke aufgeteilt: Angreifer, Methoden, Motivation des Angreifers, Angriffsziel, Verteidigung und Allgemeine Wahrnehmung. Vergleichbar mit der Dekomposition bei der Inhaltsanalyse nach Früh [Frü07, Seite 88], wird das Konstrukt IT-Sicherheit in Indikatoren zerlegt. Anforderung an die korrekte Zer-

legung sind Vollständigkeit, Trennschärfe und Exklusivität der Indikatoren [Frü07, Seite 89]. Bei der Auswahl der Frageblöcke musste jedoch ein Kompromiss zwischen Themenabdeckung und Aufwand zur Beantwortung eingegangen werden. Deshalb erhebt diese Dekomposition keinen Anspruch auf absolute Vollständigkeit. Ziel ist, dass jede dieser Kategorien einen eigenen Subindex bildet und diese mit dem Index des Vormonats zu dem Gesamtindex des jeweiligen Monats aggregiert werden.

Der deutsche Fragebogen wurde aus dem US Projekt übernommen. Bei der Übersetzung der Fragen ist darauf geachtet worden, dass die Fragen jeweils durch den Block "Im Vergleich zum Vormonat" eingeleitet werden, vgl. mit Dillman [Dil99] und Tourangeau et al.[TRR00, Seite 104]. Die Voranstellung des Zeitbezugs soll dem Antwortenden bei der Rekapitulation des Vormonats unterstützen.

Der Fragebogen ist nicht lang und eine Navigation durch den Fragebogen, die auf Grund vorangegangener Antworten nötig wäre, ist nicht möglich, da die Fragen voneinander inhaltlich unabhängig sind. Um eine Logik bei der Beantwortung der Fragen aufzubauen, wird der Angreifer als Thema nach vorne gestellt, da wir ihn als Kern und Hintergrund von IT-Sicherheit sehen. Die folgenden Fragen sind durch die Hintergründe eines Sicherheitsvorkommnisses motiviert und bauen auf der ersten Frage auf, was zu den angegriffenen Ressourcen führt. Die Ressourcen werden zur Erbringung des Geschäfts benötigt und sind Teil des Unternehmens. Das Unternehmen ist Teil der Gesellschaft und so schließt der Fragebogen mit allgemeingültigen Fragen zu dieser ab [Dil99, Seite 86ff.].

Beim Diffusionsindex entscheidet der Teilnehmer den Trend des Index, indem er als Antwort eine Richtung des Trends bestimmt. Die Antworten, die der Teilnehmer aus der Auswahl wählt, schließt die Antwort als vollständigen Satz ab, vgl. mit [Dil99, Seite 68, Bild 2.16, revision 13]. Der Halbsatz, der der Antwort vorangestellt ist, dient auch als Erklärung und Hilfestellung, wie die Fragestellung zu interpretieren ist. Als Anzahl gibt der Fragebogen 5 Antworten vor, um die Symmetrie bei der Anzahl der positiven und negativen Antworten zu erhalten und Teilnehmer hier eine höhere Zufriedenheit bei der Beantwortung der Fragen aufweisen [Dil99, Seite 57f.]. Nach Empfehlung von Dillman [Dil99, Seite 58f.] wird die neutrale Antwort "weiß nicht" ans Ende der Antwortmöglichkeiten gestellt, damit der Leser die Chance nutzt, alle werthaltigen Antwortmöglichkeiten zu lesen, bevor er diese wählt. In Zukunft möchten wir das Panel dazu nutzen, auch Fragestellungen mit aktuellem Bezug einzubringen, die nicht unbedingt eine Antwort vorgeben, sondern auch Freitexte ermöglichen.

Kerneigenschaft des Fragebogens ist, dass hier keine konkreten Vorfälle abgefragt werden. Bei der Formulierung der Fragen werden absichtlich unscharfe Begriffe wie bspw. "Bedrohung" und "Risiko" verwendet, die in jedem Unternehmen und jeder Branche anders interpretiert werden. Die Begriffe und Fragen werden bewusst nicht zusätzlich erklärt. Wie beim ifo-Geschäftsklimaindex wird dem Unternehmen selbst überlassen, wie sie diese definieren. Die Unternehmen wählen "die für sie relevanten Faktoren. [...] Durch die Flexibilität der Fragestellungen lassen sich die Antworten der Befragungsteilnehmer über verschiedenste Wirtschaftsbereiche hinweg zu einem Gesamtindikator zusammenfügen" [ABS09, Seite 34].

6 Einschränkungen

Der ICS ist kein theoretisches Konstrukt, sondern sucht den Kontakt zur Praxis. Wesentliche Einschränkungen müssen wir deshalb in den Bereichen machen, in denen den teilnehmenden Unternehmen hohe Aufwände jeglicher Art aufgelastet werden oder das Projekt aus organisatorischen Gründen für uns nicht mehr durchführbar ist.

Die Rekrutierung von Teilnehmern für den ICS erfolgt in einem schwierigen Umfeld. Wesentliche Aspekte des ICS-Designs basieren auf begründeten Überlegungen. Das Schneeballverfahren beinhaltet in diesem Zusammenhang sowohl die Fortführung der Rekrutierung durch bereits gewonnene Teilnehmer, als auch deren Empfehlungen von Interessenten. Bei der Rekrutierung der Teilnehmer müssen wir hier Abstriche machen. Für die statistische Repräsentativität für eine gesamtdeutsche Aussage zur IT-Sicherheit würde eine Population von 300 Teilnehmern nicht ausreichen. Für eine langfristige Stimmungsanalyse mit stabiler Population ist dieser Umstand allerdings nicht bedeutsam, da der Fokus nicht auf der Aussagekraft eines einzelnen Umfragemonats liegt. Folgerichtig haben die Daten einer einzelne Umfrage keine für Gesamtdeutschland repräsentative Aussagekraft.

Es ist nicht ausgeschlossen, dass gerade die Unternehmen, die von Cyberangriffen am Häufigsten betroffen sind, auch die sind, die aus Imagegründen am wenigsten bereit sind, teilzunehmen. Wir können nur auf die Unternehmen zurückgreifen, die sich auch bereit erklären, an der Umfrage teilzunehmen. Den Bedenken der Organisationen wirkt das transparente Konzept durch das Auslassen konkreter Vorfälle in der Befragung entgegen. Dieser Umstand hat auf Grund der langfristigen Durchführung jedoch wenig Aussagekraft, weil Rückschlüsse auf die Teilnehmer nur zum Zeitpunkt der Teilnahme gelten. Die IT-Sicherheitssituation der Teilnehmer kann sich im Laufe der Teilnahme verändern.

Der Umfang des Fragebogens ist eine Abwägung zwischen Informationsgehalt und Zeitaufwand. Mit steigendem Zeitaufwand wären die Teilnehmer weniger bereit gewesen, den Fragebogen monatlich auszufüllen. Insbesondere, da unsere Zielpopulation Entscheider auf höherer Managementebene sind. Die wesentlichen Aspekte der IT-Sicherheit sind unseres Erachtens nach aufgeführt. Einen Anspruch auf Vollständigkeit erheben wir hier aber nicht. Das bedeutet, dass der Index nur Aussagekraft für die Aspekte der IT-Sicherheit erhebt, die auch als Kategorie aufgenommen werden.

Die bisher gewählten Gewichtungen der Antworten sind Erfahrungswerte aus dem US Projekt. Es ist nicht ausgeschlossen, dass diese Werte im Laufe des deutschen Projektes an das deutsche Panel angepasst werden müssen, wenn der Index zu stark von Ausreißern betroffen ist. Die Anpassungen sollten jedoch in den ersten Monaten erfolgen, um die Aussage des Index nicht zu verfälschen. Panels bauen darauf auf, dass die Messverfahren und Teilnehmer im Umfragezeitraum relativ stabil bleiben. Falls eine solche Adaption vorgenommen werden muss, müssen die Konsequenzen in die Analyse und eventuell in einer noch zu bestimmenden Weise den Indexwert einfließen.

Manche Aspekte, wie die Unterschiede von Finanzprodukten und IT-Sicherheit, konnten in diesem Positionspapier nicht berücksichtigt werden. Hier verweisen wir auf die Projektseite `https://www.cybersecurityindex.de`, die auf Hintergründe eingeht.

7 Ausblick

Das aktuelle Projekt beinhaltet in erster Linie die Akquisition von Teilnehmern und Etablierung des ICS. Hauptsächlich möchten wir den Index, seine Subindizes und die Möglichkeit, Fragen mit aktuellem Bezug unterzubringen, als eine valide und langfristige Datenquelle für zukünftige Forschungsvorhaben nutzen. Ein Projekt wird hierbei sein, die Meinung der IT-Experten mit den Informationen aus anderen Informationsquellen, wie z.B. Massenmedien, Fachzeitschriften oder Konsumentenumfragen zu vergleichen. Darüber hinaus streben wir an, gewonnene Erkenntnisse auf Konferenzen zu präsentieren.

Analog zum ifo-Geschäftsklimaindex ist es wichtig, die Ergebnisse des ICS zu hinterfragen. So wäre es wichtig, den ICS an anderen IT-Sicherheitsstatistiken zu messen. Umgekehrt kann der ICS auch dazu verwendet werden, die veröffentlichten Trends der Hersteller von Sicherheitsprodukten auf Validität zu prüfen.

Stand heute ist der ICS der einzige uns bekannte Sicherheitsindex, der monatlich berechnet wird. Es denkbar, dass IT-Sicherheit saisonalen Schwankungen unterliegt. Dieser Umstand müsste weiter untersucht werden und bei Bedarf behoben werden. So wird bspw. der ifo-Geschäftsklimaindex durch das ASA-II Verfahren bereinigt.

Außerdem sind Rückmeldungen von den Teilnehmern zu erwarten, wie es auch beim US Projekt geschehen ist. Diese müssen bewertet werden und gehen eventuell auch als Ideen in das Verfahren oder die Berechnung des ICS ein. Dazu wäre es interessant zu erfahren, welche Fragen für die Teilnehmer besonders wichtig sind und welche die Organisationen gar nicht betreffen.

Um die Teilnehmer über den langen Zeitraum im Projekt zu halten, ist es wesentlich, den Teilnehmern Anwendungsmöglichkeiten zu unterbreiten. Es ist denkbar, diese mit einzelnen Teilnehmern zu entwickeln und dann zu veröffentlichen. Für erste Verwendungsmöglichkeiten können die existierenden Finanzindizes evaluiert werden.

8 Zusammenfassung

Dieses Positionspapier stellt den ICS vor, der von Unternehmen als Benchmark als Kommunikationsbasis für die eigenen Risiken oder zur Rechtfertigung der IT-Sicherheitsinvestitionen verwendet werden kann. Ausgangspunkt ist die Feststellung, dass nach heutiger Kenntnis ein solcher Index, als aggregierte Kennzahl nicht existiert. Allerdings erstellen abhängige Sicherheitsprodukthersteller oder unabhängige Institutionen mit einem speziellen Fokus auf ein spezifisches IT-Sicherheitsthema jährlich Sicherheitsreports. Wir haben dargestellt, warum diese durch Organisationen nur mit Vorsicht verwendbar sind.

Der Aufbau des Papers geht von der Frage aus, wie das Design einer Kennzahl aussehen muss, damit Manager sie für ihre Entscheidungen verwenden und welche Voraussetzung erfüllt sein müssen, dass Unternehmen gewillt sind, Informationen über ihre IT-Sicherheitslage bereitzustellen. Um diese Herausforderung praktisch umzusetzen, ist im April 2013 das deutsche ICS Projekt gestartet, dessen Konzeption hier vorgestellt worden

ist. Der ICS ist ein stimmungsbasierter Index, der sich auf einer Umfrage von deutschen IT-Sicherheitsbeauftragten begründet. Den Teilnehmern wir eine monatlich identische Umfrage zur Beantwortung vorgelegt und nach Abschluss erhalten sie eine detaillierte Analyse des berechneten Index. Der Indexwert selbst wird auf der Webseite des Projektes veröffentlicht. Basis für die Erstellung dieses Index sind Diffusionsindizes, wie sie in der Finanzbranche bereits seit langer Zeit verwendet werden. Die Rekrutierung, als wesentlicher Punkt einer Panel-Umfrage, und der Fragebogen sind umrissen worden. Transparenz, Objektivität und Unabhängigkeit sind Quelle für alle Entscheidungen zum Entwurf des Index. Um jedoch die praktische Umsetzbarkeit und die Anonymität der Teilnehmer nicht zu gefährden, sind bei der Repräsentativität der Teilnehmerauswahl und dem Umfang der Befragung Abstriche gemacht worden.

Neben dem Mehrwert für die Teilnehmer ist der ICS auch eine Datengrundlage für weitere Forschungen. Voraussetzung für alle weiteren Planungen ist die erfolgreiche Einführung des Index und die Erstellung erster Indexwerte. In einem zweiten Schritt ist die Aussagekraft des Index gegen schon bestehende Berichte der IT-Sicherheit zu verifizieren.

References

[ABB+12] Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michael van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. Measuring the Cost of Cybercrime. In *WEIS*, 2012.

[ABS09] Klaus Abberger, Manuel Birnbrich, and Christian Seiler. Der Test des Tests im Handel - eine Metaumfrage zum ifo Konjunkturtest. *Ifo Schnelldienst*, 62(21):34–41, 2009.

[All13] Allianz für Cyber-Sicherheit. Jahresbericht 2012/2013, 2013.

[Ben97] William L. Benoit. Image Repair Discourse and Crisis Communication. *Public Relations Review*, 23(2):177 – 186, 1997.

[BKA10] BKA. Cybercrime - National Situation. Technical report, Bundeskriminalamt (BKA), 2010.

[CD94] Dennis L. Clason and Thomas. J. Dormody. Analyzing Data Measured by Individual Likert-Type Items. *Journal of Agricultural Education*, 35(4):31–35, 1994.

[CSI10] CSI. *2010/2011 CSI Computer Crime and Security Survey*. CSI Computer Crime and Security Survey. Computer Security Institute, 2010.

[Dil99] Don Dillman. *Mail and Internet Surveys; The Tailored Design Method*. Wiley John + Sons, 1999.

[ER96] Uwe Engel and Jost Reinecke. *Analysis of Change: Advanced Techniques in Panel Data Analysis*. Walter De Gruyter Incorporated, 1996.

[Eur10] Eurostat. Enterprises - ICT Security Policy, Incidents and Measures Taken, 2010.

[Eur12] European Commission. Eurobarometer 390 - Cyber Security Report, 2012.

[Frü07] Werner Früh. *Inhaltsanalyse: Theorie und Praxis*. UTB. Uni-Taschenbücher. UVK, 2007.

[Gee10] Daniel E. Geer. An Index of Cybersecurity. *IEEE Security & Privacy*, 8(6):96, 95, 2010.

[Gee11] Daniel E. Geer. New Measures. *IEEE Security & Privacy*, 9(3):86–87, 2011.

[GP12] Daniel E. Geer and Mukul Pareek. ICS Update. *Security Privacy, IEEE*, 10(3):93–95, 2012.

[Gro89] Robert M. Groves. *Survey Errors and Survey Costs*. Wiley series in probability and mathematical statistics: Applied probability and statistics. Wiley, 1989.

[GU90] Patricia M. Getz and Mark G. Ulmer. Diffusion Indexes: A Barometer of the Economy. *Monthly Labor Review*, 13:13 – 21, 1990.

[Han12] Andrew Hansen. Research Note: Trends in Data Breaches. *Annie Searle Associates LLC*, 6273, 2012.

[KS10] Johannes Kopp and Bernhard Schäfers. *Grundbegriffe der Soziologie*. Springer, 2010.

[Lik32] Rensis Likert. A Technique for the Measurement of Attitudes. *Archives of Psychology*, 22(140):1–55, 1932.

[MAK13] Cecilia Malmström, Catherine Ashton, and Neelie Kroes. Cybersicherheitsplan der EU für ein offenes, freies und chancenreiches Internet / EU Cybersecurity Plan to Protect Open Internet and Online Freedom and Opportunity, February 2013.

[Pre08] Peter R. Preißler. *Betriebswirtschaftliche Kennzahlen: Formeln, Aussagekraft, Sollwerte, Ermittlungsintervalle*. BWL Starter Kit. Oldenbourg Wissensch.Vlg, 2008.

[Pri13] PricewaterhouseCoopers GB. Information Security Breaches Survey. Technical report, PricewaterhouseCoopers GB, 2013.

[SH02] Michael Schröder and Felix P. Hüfner. Forecasting economic activity in Germany: how useful are sentiment indicators? ZEW Discussion Papers 02-56, ZEW - Zentrum für Europäische Wirtschaftsforschung / Center for European Economic Research, 2002.

[Sym13] Symantec Corporation. *Internet Security Threat Report*, volume 13. Symantec Corporation, 2013.

[TRR00] Roger Tourangeau, Lance J. Rips, and Kenneth Rasinski. *The Psychology of Survey Response*. Cambridge University Press, 2000.

A Fragebogen

1. Angreifer

Im Vergleich zum Vormonat, wie hat sich aus Ihrer Sicht die Bedrohung für Ihre Organisation durch die folgenden Angreifer entwickelt? [stark gefallen, gestiegen, unverändert, gestiegen, stark gestiegen, weiß nicht]

1.1 Insider: Das Risiko durch böswillige Interne (mit Gelegenheit und Motivation) ist

1.2 Strategische Rivalen: Die Wahrscheinlichkeit, dass Angriffe existieren, welche explizit auf wirtschaftlich wertvolle Daten Ihrer Organisation abzielen, ist

1.3 Aktivisten/Hacktivisten: Ihre Gefährdung durch politisch oder ideologisch motivierte Aktivitäten (aus dem In- und Ausland) ist

1.4 Kriminelle: Die Bedrohung für Ihre Organisation durch kriminell motivierte Angreifer ist
1.5 Staaten: Der Grad, zu dem Ihre Organisation Ziel von nationalen Akteuren ist, ist

2. Methoden
Im Vergleich zum Vormonat, wie hat sich die Bedrohung durch folgende Angriffsmethoden entwickelt?
2.1 Botnetze
2.2 Allgemeine Schadsoftware
2.3 Exploits von Sicherheitslücken
2.4 Phishing / Social Engineering
2.5 Gezielte Angriffe auf Ihre Organisation

3. Motivation des Angreifers
Im Vergleich zum Vormonat, wie hat sich das Risiko durch die unten genannten Angriffsanreize entwickelt?
3.1 Datendiebstahl (Vertraulichkeit)
3.2 Datenänderung (Integrität)
3.3 Unterbrechung der Geschäftstätigkeit (Verfügbarkeit)

4. Angriffsziele
Im Vergleich zum Vormonat, wie hat sich das Risiko durch die folgenden Angriffsziele für Ihre Organisation entwickelt?
4.1 Webbasierte Anwendungen / Webseiten
4.2 Geräte mit Internetzugang
4.3 Arbeitsplatzrechner / Desktops
4.4 Mobile Geräte
4.5 Öffentliche Infrastrukturen, von denen Sie abhängig sind (inklusive Cloud-Dienste)
4.6 Geschäftspartner (wie z.B. Hersteller), die rechtmäßigen Zugriff auf Ihre Daten haben

5. Verteidigung
Im Vergleich zum Vormonat, wie hat sich Ihre Einschätzung bezüglich der folgenden Bedrohungen entwickelt?
5.1 Die Verwundbarkeit von verfügbaren Verteidigungsmaßnahmen durch bekannte Bedrohungen ist
5.2 Die Verwundbarkeit von verfügbaren Verteidigungsmaßnahmen durch unbekannte Bedrohungen ist

6. Allgemeine Wahrnehmung
Im Vergleich zum Vormonat, wie hat sich Ihre Einschätzung bezüglich der folgenden Themen entwickelt?
6.1 Die Wahrnehmung von Cyber-Risiken, die die allgemeine Bevölkerung betreffen, ist in den Medien und der Öffentlichkeit
6.2 Ihr persönliches Risiko durch Online-Aktivitäten, inklusive kommerzieller Tätigkeiten, ist
6.3 Der allgemeine Informationsaustausch in Ihrer Branche oder Region ist