Studie zum Stand der gegenwärtigen Wahrnehmung von Cyberrisiken in deutschen Unternehmen

INTERNATIONALE VERSICHERUNGSMAKLER UND RISK CONSULTANTS

INHALTSVERZEICHNIS

VORWORT

Im Cyberspace verschwimmen die Grenzen zwischen Kontinenten, Kulturen und Sprachen. Schon heute sind Milliarden Privatpersonen, Unternehmen und Regierungen global miteinander vernetzt. Besonders für die Wirtschaft hat diese Entwicklung ganz unterschiedliche Gesichter — sowohl im Hinblick auf Chancen als auch auf Risiken.

Welche Cyberrisiken werden von Unternehmen als besonders bedrohlich wahrgenommen? Wird der Risikotransfer durch Cyber-Versicherungsprodukte, die einige größere Industrieversicherer anbieten, genutzt oder präferieren Unternehmen vielmehr präventive Maßnahmen der Risikosteuerung?

Ziel dieser bundesweiten sowie branchenübergreifenden aus zwölf Fachfragen bestehenden Umfrage ist es zu untersuchen, wie deutsche Unternehmen Cyberrisiken wahrnehmen und wie hoch die potenzielle Gefahr für die Unternehmen durch einzelne dieser Risiken und die Konsequenzen ihres Eintritts eingeschätzt wird. Darüber hinaus soll auch die Auseinandersetzung mit Cyberrisiken und deren Steuerung in den Unternehmen untersucht werden. Die Befragung erfolgte online und anonym in der Zeit vom 18. Februar bis 6. März 2014.

Der Fokus der Untersuchung liegt hierbei auf dem Steuerungsinstrument der Cyberrisiko-Versicherung: Während präventive Steuerungsmaßnahmen wie Verhaltensrichtlinien und Restriktionen oder die Optimierung des unternehmensweiten IT-Sicherheitskonzepts in den einzelnen Unternehmen eine sehr unterschiedliche Effektivität, Intensität und Ausgestaltung annehmen können, ist eine Cyberrisiko-Versicherung als eher reaktive Steuerungsmaßnahme im Prinzip überall gleich.

Zwar sind individuell gestaltbare Deckungsbausteine und -konzepte möglich, Prämiensätze, Versicherungssummen und Selbstbehalte von Fall zu Fall verschieden, das Funktionsprinzip jedoch ist immer dasselbe: Gegen Erbringung eines an Deckungssumme und Risiko orientierten Versicherungsbeitrags bietet das Versicherungsunternehmen für den versicherten Schadenfall eine Entschädigung in vertraglich bestimmter Höhe. Insbesondere vor dem Hintergrund, dass die Cyberrisiko-Versicherung relativ neu am Markt ist, soll im Zuge dieser Untersuchung eruiert werden, ob und inwieweit dieses Versicherungsprodukt von Unternehmen als sinnvoll erachtet wird, welche Anforderungen gestellt werden und in welchem Rahmen sich Deckungsbedarf und Zahlungsbereitschaft bewegen.

Unser Dank richtet sich an Julian Meister, der mit dieser Umfrage – die die Grundlage für die Ergebnisse dieser Studie ist – den akademischen Grad Bachelor of Arts der HSBA, Hamburg School of Business Administration, im August 2014 erlangte.

Insbesondere danken wir an dieser Stelle den 405 Unternehmen, die sich an der Befragung beteiligt haben. Durch die große Resonanz ist es uns möglich, erstmals fundierte Aussagen zum aktuellen Stand der Wahrnehmung von Cyberrisiken im deutschen Mittelstand zu treffen.

Wir wünschen eine spannende Lektüre!

Hendrik F. Löffler
Geschäftsführer Funk RMCE

ZUSAMMENFASSUNG DER ERGEBNISSE

- Interne Cyberrisiken sind für deutsche Unternehmen überwiegend bedrohlicher als externe Cyberrisiken.

- Die Frequenz versuchter Cyberangriffe wird als hoch beschrieben, hierdurch eintretende nachweisbare Schädigungen der Unternehmen sind jedoch vergleichsweise selten.

- Wird die Integrität von Daten Dritter verletzt, ist dies für die Unternehmen in Deutschland vielfach kritischer als potenzielle Eigenschäden.

- Mit Blick auf die Risikosteuerung befürworten die befragten Unternehmen primär aktive Risikoprävention.

- Reaktive Steuerungsmaßnahmen wie z. B. die Cyberrisiko-Versicherung werden von den befragten Unternehmen als relativ intransparent bewertet. Es herrscht teilweise Unklarheit darüber, was eine Cyberrisiko-Versicherung aktuell leistet. Der Bedarf und das Interesse an einer Versicherungslösung sind daher bisher noch gering.

1. DEFINITION DES CYBERRISIKOS

Um den Begriff des Cyberrisikos einzugrenzen, bedarf es der Klärung der Begriffsherkunft. Das Cyberrisiko ist ein Risiko im Bereich des Cyberspace.

Als Cyberspace lässt sich eine globale Sphäre innerhalb der Informationsumwelt beschreiben. Diese Sphäre basiert auf interdependenten Netzwerken innerhalb der In-frastruktur von Informationssystemen. Hierzu gehören u. a. das Internet, Telekommunikationsnetzwerke, Computersysteme und eingebundene Prozessoren und Steuerungselemente.[1]

Cyberrisiken bedrohen die Sicherheit im Cyberspace, also die Cyber Security. Diese lässt sich mit der Fähigkeit umschreiben, die Nutzung des Cyberspace vor Cyberangriffen zu schützen und zu verteidigen.[2]

Cyberangriffe beschreiben Angriffe über den Cyberspace, die auf die Nutzung des Cyberspace durch ein Unternehmen gerichtet sind und auf eine Unterbrechung, Blockierung, Zerstörung oder böswillige Kontrolle der hierzu verwendeten Umwelt und Infrastruktur der Datenverarbeitung abzielen. Weitere Ziele können in der Zerstörung der Integrität oder dem Diebstahl von sensiblen Daten und Informationen liegen.[3]

Neben gezielten Angriffen werden aber auch Aktionen berücksichtigt, die unter Verwendung von Computernetzwerken stattfinden und einen unmittelbar oder potenziell negativen Effekt auf ein Informationssystem und/oder die darin befindlichen Informationen und Daten haben, jedoch keiner böswilligen Absicht unterliegen.[4] Nutzt ein Mitarbeiter beispielsweise sein Firmen-Notebook, auf dessen Festplatte sich vertrauliche Unternehmensdaten befinden, auch privat, ist dies kein gezielter Cyberangriff, aber durchaus eine Gefährdung der Cyber Security des Unternehmens.

Zusätzlich zum „klassischen" Hackerangriff und dem unvorsichtigen Umgang mit Unternehmensdaten lassen sich im Kontext Cyberkriminalität und -risiken „auch der Verlust oder die Zerstörung von Daten durch eigene Mitarbeiter, Urheber- oder Persönlichkeitsverletzungen durch die ungewollte Veröffentlichung von Daten, Betriebsunterbrechungen infolge des Zusammenbruchs der Automationssoftware, Industriespionage, Computer-Betrug oder Cyber-Erpressung (…)"[5] nennen.

Insgesamt lassen sich die betrieblichen Cyberrisiken vier übergeordneten Kategorien zuordnen, die einschließlich der jeweils wieder untergeordneten Aspekte die möglichen Formen des Cyberrisikos zusammenfassen:

> „(1) actions of people,
> (2) systems and technology failures,
> (3) failed internal processes, and
> (4) external events."[6]

1 Vgl. CNSS 2010
2 Vgl. ebd.
3 Vgl. ebd.
4 Vgl. ebd.
5 Vgl. JUNG 2013, S. 55, Sp. 2
6 CEBULA/YOUNG 2010

2. RISIKOWAHRNEHMUNG

2.1 Top-Thema „Cyberrisiken“

Haben sich Mitarbeiter/Bereiche und/oder die Geschäftsführungsebene Ihres Unternehmens in den vergangenen Monaten aktiv mit dem Thema Cyberrisiken beschäftigt?

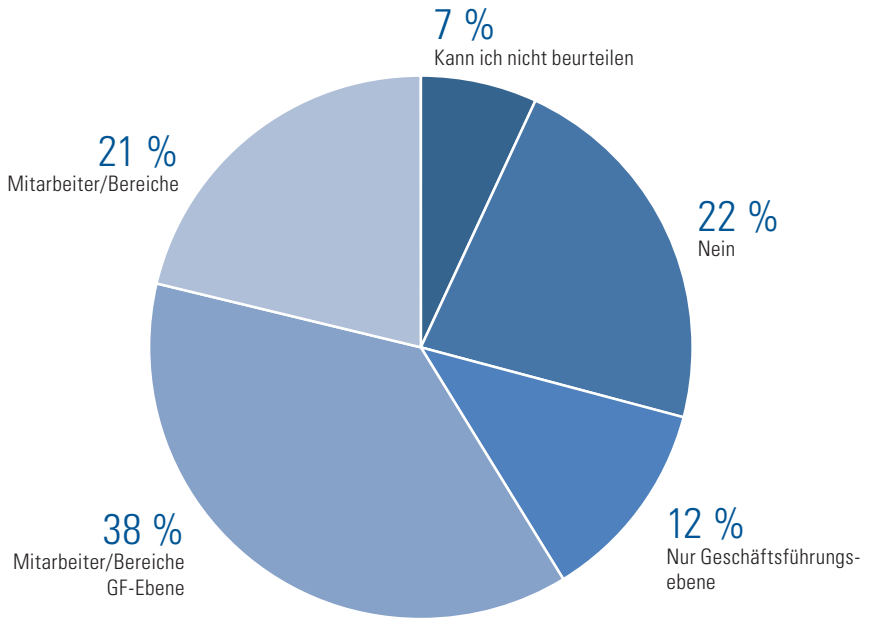

Abbildung 1

71 % der deutschen Unternehmen haben sich in den vergangenen Monaten aktiv mit Cyberrisiken auseinandergesetzt. In jedem zweiten Unternehmen sind Cyberrisiken mitunter in 12 % der Unternehmen ausschließlich Thema der Geschäftsführungsebene.

Trotz der medialen und politischen Aufmerksamkeit, die Themen wie Cyber Security, Cybercrime und Cyberrisiken momentan beikommt, haben sich 22 % der Unternehmen noch nicht aktiv hiermit beschäftigt.

7 % der Umfrageteilnehmer können nicht beurteilen, ob solche Themen in ihren Unternehmen aktuell behandelt werden. Gründe hierfür könnten in einer fehlenden internen Kommunikation liegen, aber auch darin, dass man sich hier noch nicht mit Cyberrisiken auseinandersetzt.

2.2 Cyberkriminalität in Deutschland

Was denken Sie, wie viele Fälle von Cyberkriminalität im deutschen Markt jährlich – in etwa – polizeilich erfasst werden?

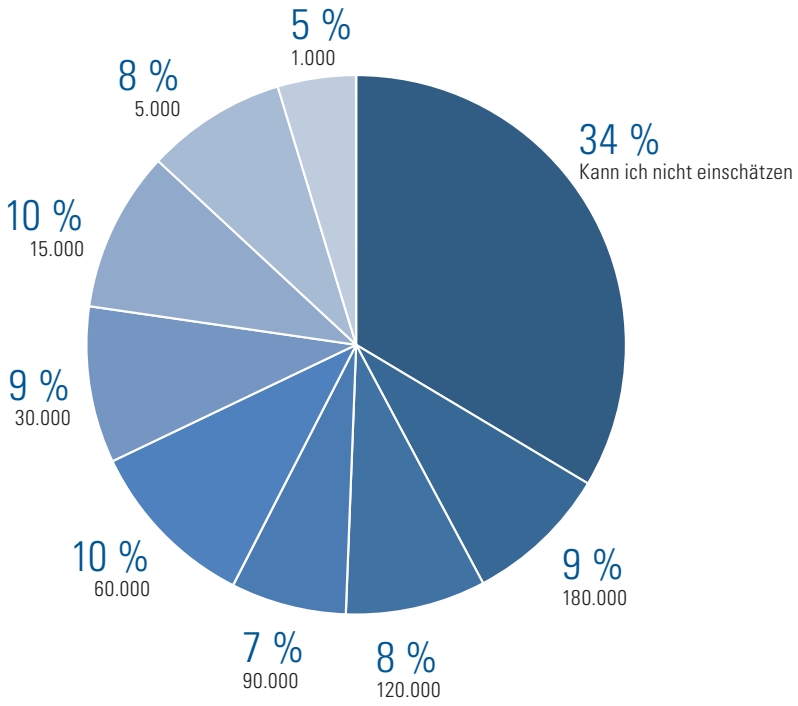

Abbildung 2

Laut dem BKA werden die meisten Fälle von Cybercrime überhaupt nicht polizeilich erfasst. Viele Delikte bleiben Versuche, andere werden nicht erkannt und insbesondere bei Straftaten gegen Unternehmen kommt es – um Reputationsrisiken vorzubeugen – meist gar nicht erst zur Anzeige. So ist die Dunkelziffer von Straftaten im Bereich Cyberkriminalität vermutlich groß[7]. Dennoch wurden in der polizeilichen Kriminalstatistik des Jahres 2012 63.959 Fälle von Cybercrime in Deutschland erfasst[8]. Nur ein Zehntel der deutschen Unternehmen kommt dieser Zahl mit einer Schätzung von etwa 60.000 jährlich erfassten Fällen nahe.

32 % der Unternehmen unterschätzen, 24 % überschätzen die Anzahl erfasster Straftaten. Tendenziell neigen Unternehmen also eher zum Unterschätzen von Cyberkriminalität. Dies kann u. U. zu schwerwiegenden Fehlentscheidungen in der unternehmerischen Planung führen. Der Anteil der Unternehmen, die eine richtige Einschätzung abgegeben haben, ist vergleichsweise gering. Knapp ein Drittel der Unternehmensrepräsentanten sieht sich nicht in der Lage, hier eine Einschätzung vorzunehmen. Das Ausmaß von Cybercrime scheint also schwer greifbar zu sein.

7 Vgl. BKA 2012, S. 5.
8 Vgl. BKA 2012, S. 3.

2.3 Cyberangriffe als tägliche Bedrohung

Was denken Sie, wie oft – in etwa – versucht wird, Ihr Unternehmen durch Cyberangriffe zu schädigen?

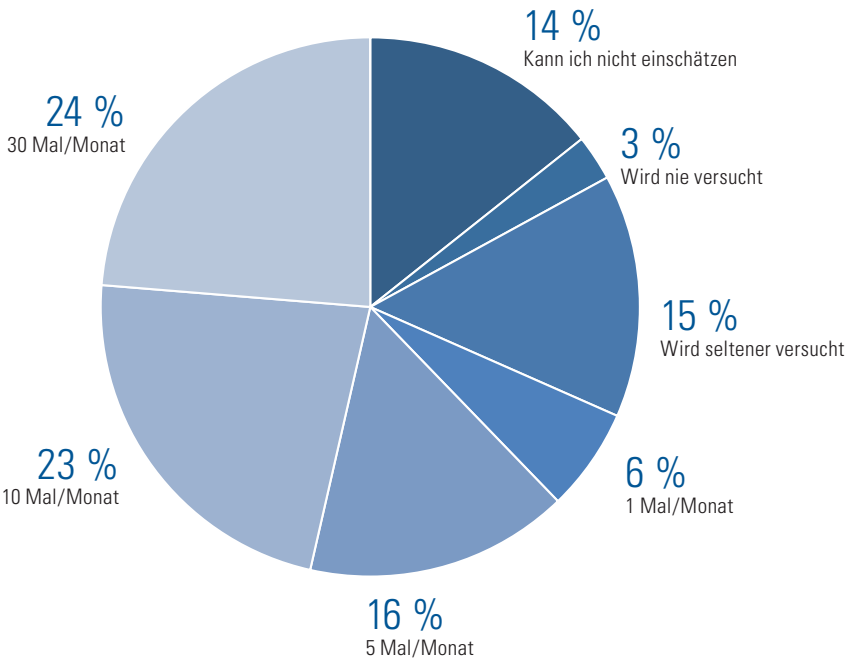

Abbildung 3

Fast die Hälfte der Unternehmen sieht sich mehreren Cyberangriffen in der Woche ausgesetzt. Knapp ein Viertel geht sogar davon aus, dass nahezu täglich eine Schädigung des Unternehmens durch Cyberangriffe versucht wird.

Angriffe im Cyberspace waren schon immer einfacher in der Durchführung, als sich dagegen zu verteidigen. Ein Angriff bedarf nur einer einzelnen Sicherheitslücke, die Verteidigung eines Systems hingegen bedarf der fortlaufenden Beseitigung und Prävention sämtlicher Schwachstellen.

Dementsprechend gehen auch nur 3 % der Unternehmen davon aus, dass sie nie Ziel von Cyberangriffen sind. Dieser Anteil ist im Vergleich zu den 83 %, die sich mehr oder minder regelmäßig in Gefahr sehen, verschwindend gering.

14 % der Umfrageteilnehmer können die Frequenz versuchter Cyberangriffe auf ihr Unternehmen nicht einschätzen.

2.4 Schädigung von Unternehmen durch Cyberangriffe

Wurde Ihr Unternehmen schon einmal durch einen Hacker- bzw. Cyberangriff geschädigt?

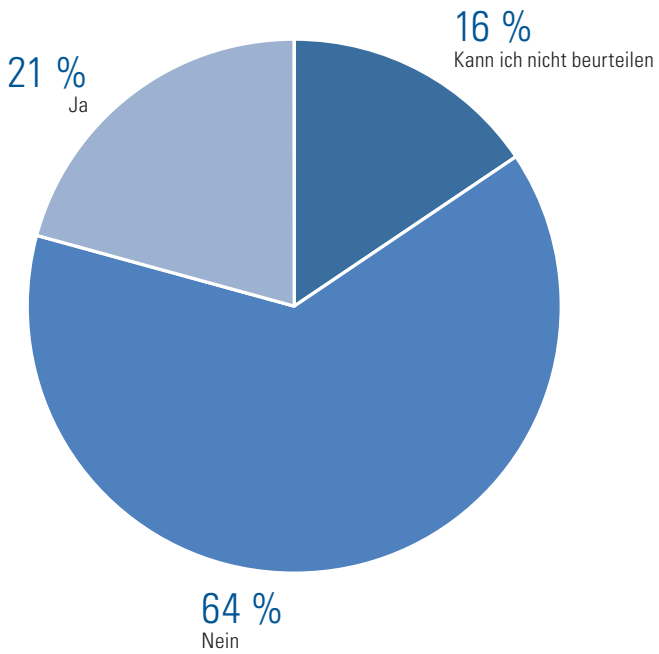

Abbildung 4

Etwa jedes fünfte deutsche Unternehmen wurde bereits durch einen Hacker- bzw. Cyberangriff geschädigt.

Im Vergleich zur polizeilich erfassten Anzahl an Delikten[9] ist dieser Anteil auffallend hoch. Geht man davon aus, dass nicht jede erfasste Straftat auch tatsächlich ein Unternehmen zum Ziel hatte bzw. überhaupt einen nennenswerten Schaden verursacht hat, wird der Eindruck umso mehr verstärkt, dass im Rahmen dieser Umfrage auffallend viele Unternehmen zugaben, bereits durch Cyberangriffe geschädigt worden zu sein. Grund für diese Offenheit kann sein, dass die Unternehmen aufgrund der anonymen Befragung keinerlei potenzielle Reputationsschäden befürchten mussten.

64 % der Unternehmen in Deutschland wurden noch nicht durch einen Hacker- bzw. Cyberangriff geschädigt und beweisen somit entweder ein hohes Maß an IT-Sicherheit oder konnten effektiven Angriffen bisher entgehen.

16 % können nicht beurteilen, ob bereits eine derartige Schädigung eingetreten ist.

9 Vgl. Frage 2, S. 8.

2.5 Cyberrisiken im Unternehmen: Die unterschätzte Gefahr

Wie hoch schätzen Sie die Gefahr für Ihr Unternehmen, dass eines der nachfolgenden Szenarien eintritt?

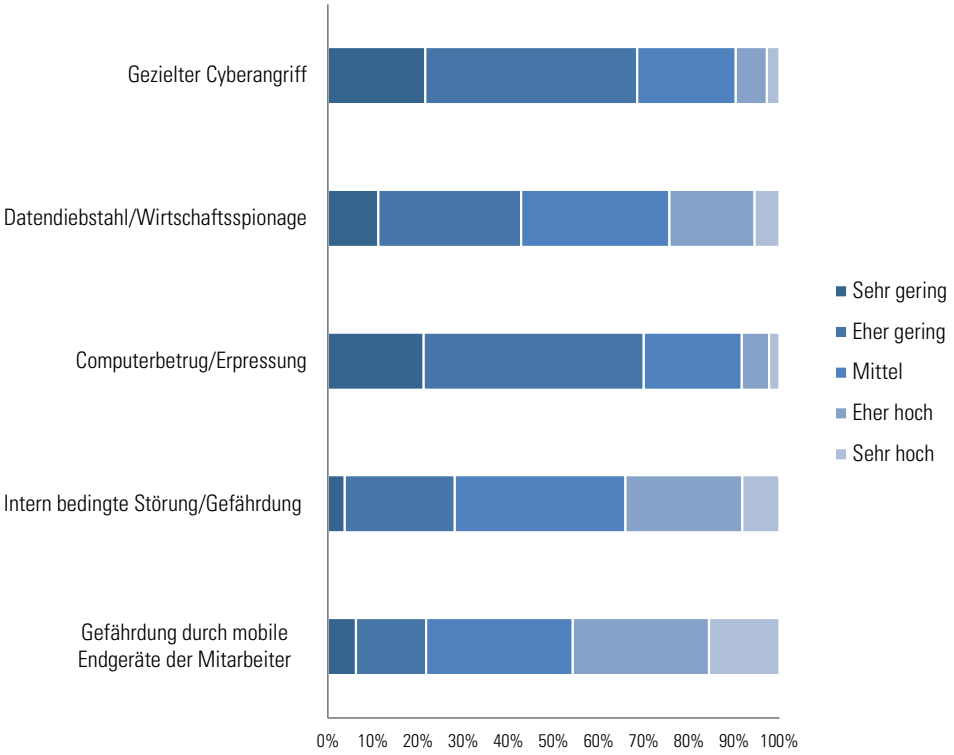

Abbildung 5

Durch die Möglichkeit, Risiken in Bezug auf ihre Gefahr zu bewerten, ergibt sich folgendes Gefahrenrating (eins entspricht „sehr gering", fünf entspricht „sehr hoch")[10]:

1.	Gefährdung durch mobile Endgeräte der Mitarbeiter	3,33
2.	Intern bedingte Störung/Gefährdung	3,10
3.	Datendiebstahl/Wirtschaftsspionage	2,76
4.	Gezielter Cyberangriff	2,22
5.	Computerbetrug/Erpressung	2,19

Im Kontext Cyberrisiken sehen sich deutsche Unternehmen vor allem durch interne Einflüsse bedroht. Hierzu gehören zum einen die Gefährdung der IT-Sicherheit, insbesondere durch eigene mobile Endgeräte der Mitarbeiter (Smartphones, Laptops, Tablets, USB-Sticks etc.) und zum anderen eine generelle intern bedingte Störung oder Gefährdung der IT-Sicherheit. 16 % der Unternehmen stufen die Eintrittsgefahr für eine Verletzung der Integrität ihrer Daten oder IT durch eigene mobile Endgeräte der Mitarbeiter als sehr hoch, 30 % als eher hoch ein. So geht knapp die Hälfte der Befragten davon aus, dass beispielsweise Smartphones von Mitarbeitern ein Sicherheitsrisiko darstellen und das Unternehmen bewusst gefährden können.

10 A. d. A.: Ein Rating von 3,33 entspricht etwa einer mittleren, tendenziell eher hohen Gefahr; Ein Rating von 2,19 entspricht etwa einer eher geringen, tendenziell mittleren Gefahr.

Neben der Gefahr, die mobile Endgeräte mit sich bringen, werden auch sonstige intern bedingte Störungen, wie beispielsweise die bewusste oder versehentliche Aktivierung schadhafter Software, als potenziell gefährlich eingestuft. 8 % der Umfrageteilnehmer bewerten die Eintrittswahrscheinlichkeit hier als sehr hoch, 26 % als eher hoch.

Opfer von Datendiebstahl und/oder Wirtschaftsspionage zu werden, halten deutsche Unternehmen für weniger wahrscheinlich, als durch interne Cyberrisiken Schaden zu nehmen. Die Gefahr erachten hier 24 % als hoch.

Die Gefahr, dass sie Opfer von Computerbetrug oder Erpressung werden, schätzen 70 % der Unternehmen hingegen als gering ein und messen diesem Cyberrisiko somit eine mäßige Bedeutung bei.

69 % der Unternehmen gehen ferner davon aus, dass die Wahrscheinlichkeit, Ziel eines böswilligen Cyberangriffs auf die Wertschöpfungskette zu werden, eher oder sehr gering ist.

Zwar vermuten viele Unternehmen eine hohe Frequenz derartiger Attacken.[11] An dessen Durchschlagskraft glauben sie aber offensichtlich nur in wenigen Fällen.

Insgesamt scheint die größte Bedrohung der IT-Sicherheit in den Unternehmen selbst zu liegen.

11 Vgl. Frage 3, S. 9 f.

2.6 Cyberrisiken und -angriffe: Gravierende Folgen

Bitte bewerten Sie die nachstehend genannten möglichen Konsequenzen eines Cyberrisikos/-angriffs im Hinblick auf die Bedeutung für Ihr Unternehmen.

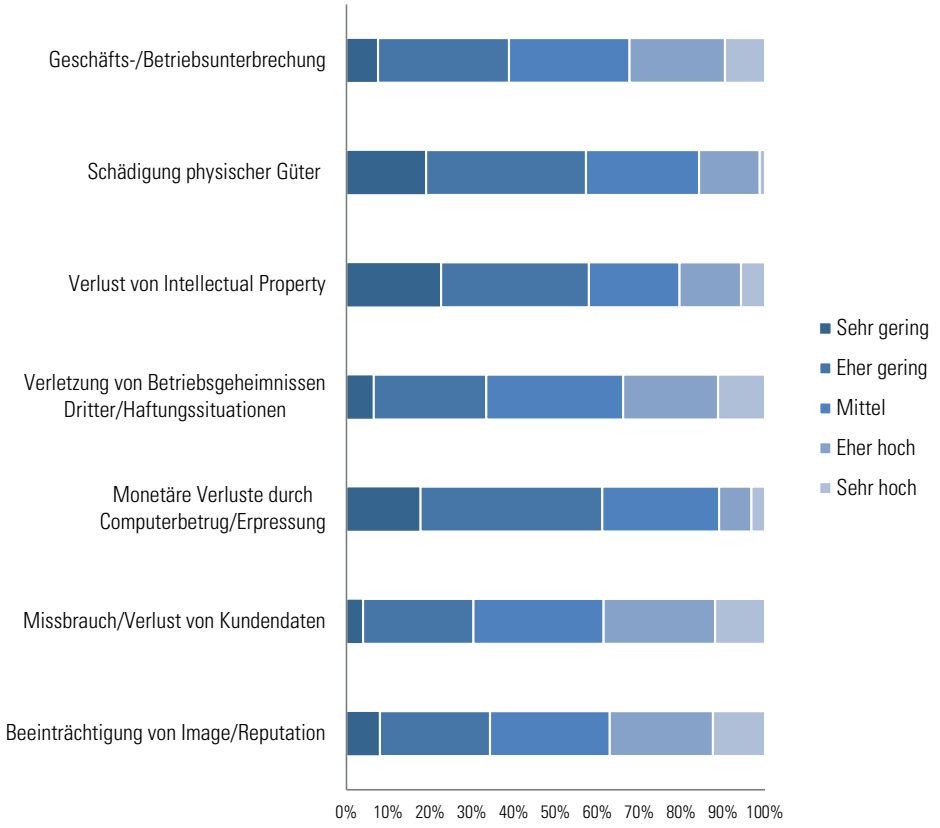

Abbildung 6

Unabhängig von der Bedrohung durch einzelne Cyberrisiken und -angriffe konnten Unternehmen die jeweiligen Konsequenzen eintretender Szenarien für den laufenden Betrieb bewerten.

Durch die Möglichkeit, Risiken in Bezug auf ihre Gefahr zu bewerten, ergibt sich folgendes Gefahrenrating (eins entspricht „sehr gering", fünf entspricht „sehr hoch")[12]:

1.	Missbrauch/Verlust von Kundendaten	3,16
2.	Beeinträchtigung von Image/Reputation	3,07
3.	Verletzung von Betriebsgeheimnissen Dritter/ Haftungssituationen	3,05
4.	Geschäfts-/Betriebsunterbrechung	2,95
5.	Verlust von Intellectual Property	2,46
6.	Schädigung physischer Güter	2,41
7.	Monetäre Verluste durch Computerbetrug/Erpressung	2,35

12 A. d. A.: Auch hier entspricht ein Rating von beispielsweise 3,16 etwa einer mittleren, tendenziell eher hohen Gefahr; Ein Rating von 2,46 entspricht etwa einer eher geringen, tendenziell mittleren Gefahr.

Gehen infolge eines Cyberrisikos/-angriffs Kundendaten verloren oder werden diese missbraucht, hat dies für deutsche Unternehmen eine eher (27 %) oder sehr hohe (12 %) Bedeutung. Dies ist nachvollziehbar, denn Kundendaten sind entscheidend für die Existenz und Betriebsfähigkeit vieler Unternehmen. Datenverluste können vielfältige Haftungssituationen bedeuten.

Auch die Beeinträchtigung von Unternehmensimage und -reputation als Folge eines Cyberrisikos hat für 37 % der deutschen Unternehmen eine eher bzw. sehr hohe Bedeutung.

Als ähnlich bedeutsam werden Risikofolgen wie die Verletzung von Betriebs- oder Geschäftsgeheimnissen Dritter und hiermit verbundene Haftungssituationen sowie eine eigene Geschäfts- oder Betriebsunterbrechung gesehen.

35 % der Unternehmen stufen die Bedeutung des Verlustes von eigenem Intellectual Property (Know-how, Patente, Lizenzen etc.) als eher gering und 23 % sogar als sehr gering ein. So ist der Verlust von eigenem Know-how für mehr als die Hälfte der Unternehmen wenig bedeutend. Werden Daten oder sensible Informationen Dritter gestohlen oder missbraucht, wird dies offensichtlich kritischer gesehen als der Diebstahl von Intellectual Property.

Ebenfalls interessant ist die Tatsache, dass die Beeinträchtigung der Reputation infolge eines Störfalls aus dem Bereich des Cyberspace von höherer Bedeutung für deutsche Unternehmen ist als der Betriebsstillstand infolge einer Unterbrechung der Wertschöpfungskette.

Dies ist erstaunlich: Oft zeigt die Praxis, dass ein Betriebsstillstand von nur wenigen Wochen zu einer Insolvenz des Unternehmens führen kann. Vielfach sind Wechselwirkungspotenziale innerhalb der Wertschöpfungskette den Unternehmen nicht bekannt. Dies kann in den meisten Fällen auf mangelnde Transparenz über entsprechende Risiken in den jeweiligen Unternehmen zurückgeführt werden.

3. RISIKOSTEUERUNG

3.1 Cyberrisiken steuern: Mitarbeiter sensibilisieren

Wurden in Ihrem Unternehmen bereits Maßnahmen zur Sensibilisierung der Mitarbeiter im Kontext Cyberrisiken ergriffen?

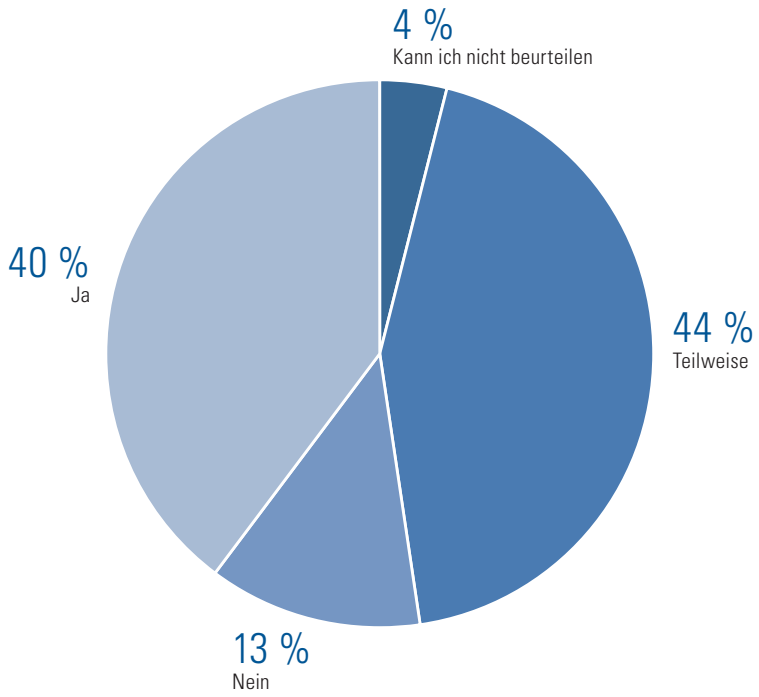

Abbildung 7

Cyberrisiken, die interner Natur sind, werden als besonders gefährlich eingestuft – dies haben die Ergebnisse im Bereich Risikowahrnehmung bereits gezeigt.

Dennoch haben 13 % der Unternehmen noch keine Maßnahmen ergriffen, um Mitarbeiter für Risiken aus dem Cyberspace zu sensibilisieren. 4 % der Umfrageteilnehmer können nicht beurteilen, ob derartige Maßnahmen in ihrem Unternehmen bereits ergriffen worden sind. Das deutet entweder darauf hin, dass dies nicht der Fall ist oder dass die ergriffenen Maßnahmen hier keine Wirkung zeigen.

40 % der deutschen Unternehmen sensibilisieren ihre Mitarbeiter für Cyberrisiken.

Fast die Hälfte der Befragten bestätigt außerdem, dass teilweise Maßnahmen zur Risikosensibilisierung getroffen wurden.

3.2 Maßnahmen zur Risikosteuerung: Effektivität bewerten

Wie bewerten Sie die Effektivität der nachfolgenden Maßnahmen zur Risikosteuerung vor dem Hintergrund einer erhöhten Bedrohung durch Cyberangriffe?

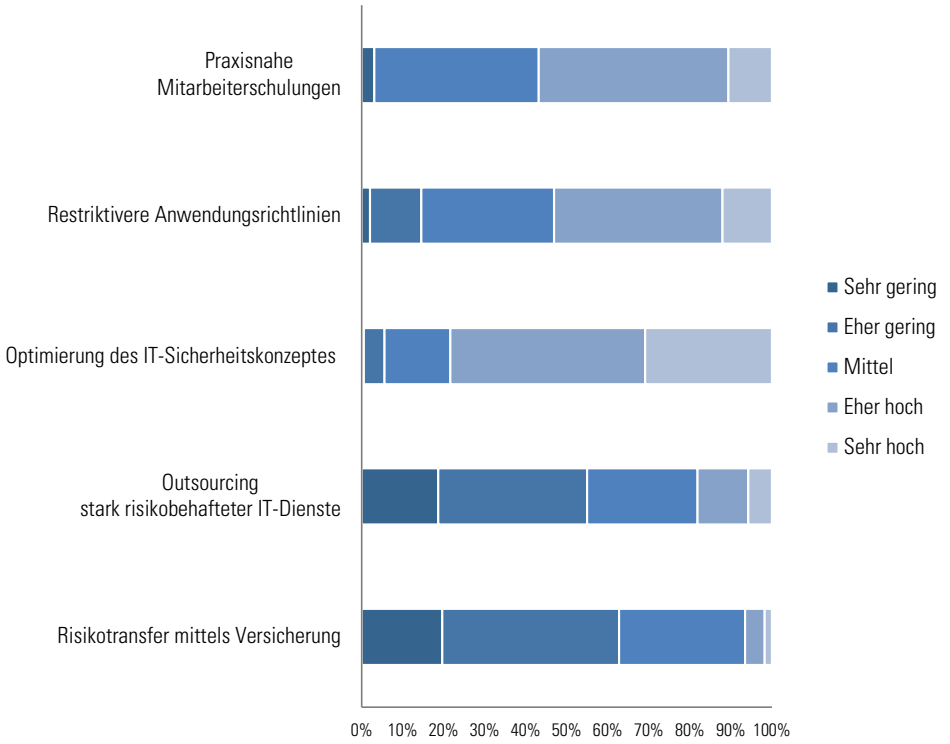

Abbildung 8

Die Effektivität der einzelnen Maßnahmen zur Risikosteuerung wurde folgendermaßen bewertet[13]:

1.	Optimierung des IT-Sicherheitskonzeptes	4,03
2.	Restriktivere Anwendungsrichtlinien für Mitarbeiter	3,49
3.	Praxisnahe Mitarbeiterschulungen	3,44
4.	Outsourcing stark risikobehafteter IT-Dienste	2,50
5.	Risikotransfer mittels Versicherung	2,26

Um einer erhöhten Bedrohung der IT-Sicherheit zu entsprechen und hier angesiedelte Risiken zu steuern, sollten Unternehmen ihr IT-Sicherheitskonzept sowohl im Bereich Software als auch im Bereich Hardware optimieren bzw. ausbauen – diese Ansicht vertreten 78 % der Unternehmen, indem sie die Effektivität einer solchen Maßnahme für eher hoch (47 %) oder sehr hoch (31 %) erklären.

13 A. d. A.: Ein Rating von beispielsweise 4,03 entspricht hier einer eher hohen Effektivität; Ein Rating von 2,26 hingegen entspricht einer eher geringen, tendenziell mittleren Effektivität.

Ebenfalls effektiv sind laut der befragten Unternehmen restriktivere Anwendungsrichtlinien und praxisnahe Schulungen für Mitarbeiter. Letztere bewerten 46 % der Umfrageteilnehmer im Hinblick auf ihre Effektivität als eher hoch, 11 % als hoch. Restriktivere Anwendungsrichtlinien, beispielsweise in Form von eingeschränktem Zugang zu sensiblen Daten oder zusätzlichen Passwörtern, halten 41 % für eher, 12 % für sehr effektiv.

Mehr als die Hälfte der Unternehmen hält das Outsourcing stark risikobehafteter IT-Dienste für wenig wirkungsvoll.

Die Cyberrisiko-Versicherung als Medium des Risikotransfers wird durch deutsche Unternehmen nicht nur relativ, sondern auch absolut als eher ineffektiv bewertet. Ein Fünftel der Umfrageteilnehmer schätzt die Wirksamkeit dieses Risikosteuerungselements als sehr gering ein, 43 % beurteilen diese als eher gering und lediglich 7 % als hoch.

4. CYBERRISIKO-VERSICHERUNG

4.1 Realität und Planung bei der Platzierung einer Cyberrisiko-Versicherung

Hat Ihr Unternehmen schon eine Versicherung gegen das mögliche Risiko eines Cyberangriffs abgeschlossen bzw. ist ein Abschluss innerhalb der nächsten 12 Monate geplant?

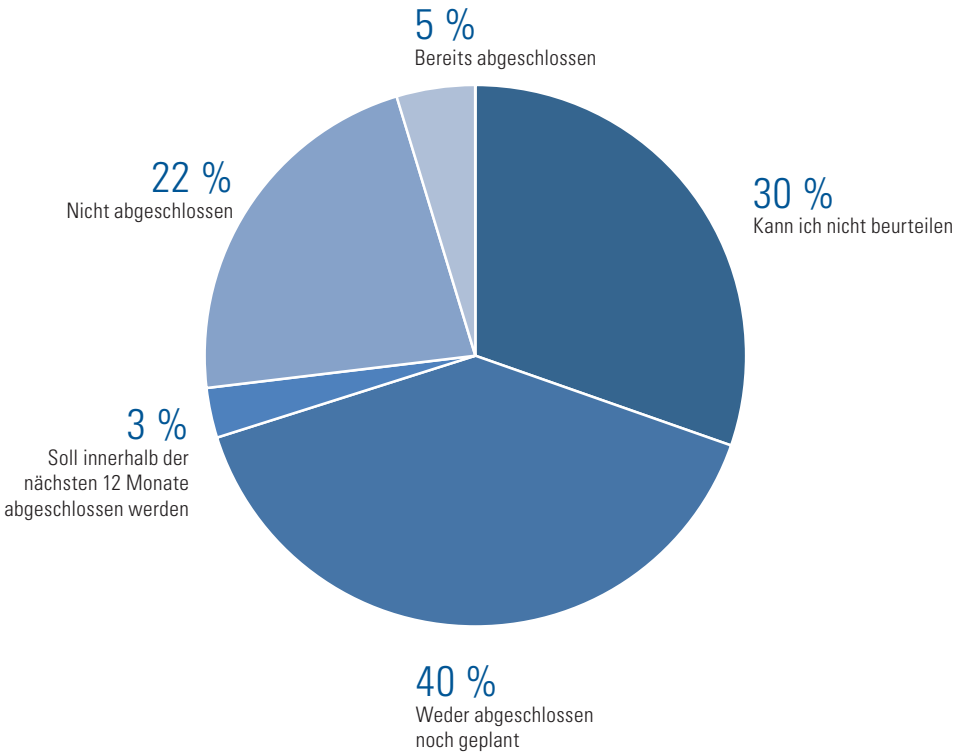

Abbildung 9

Der Anteil der Unternehmen, die bereits eine Versicherung gegen mögliche Cyberrisiken abgeschlossen haben, liegt bei lediglich 5 %. Vor dem Hintergrund der vorangegangenen Umfrageergebnisse verwundert dies nicht.

Nur 3 % der Unternehmen planen den Abschluss einer entsprechenden Police innerhalb der nächsten 12 Monate.

22 % der Unternehmen verfügen derzeit nicht über eine Cyberrisiko-Versicherung und werden aussagegemäß auch innerhalb der nächsten 12 Monate keine abschließen. Die Möglichkeit einer zukünftigen Auseinandersetzung mit diesem Produkt schließt dieser Anteil aber nicht aus[14]. Anders ist es bei weiteren 40 % der Unternehmen in Deutschland: Diese verfügen über keine Versicherung gegen Cyberrisiken und haben auch nicht geplant, diesen Umstand künftig zu ändern.

14 A. d. A.: Hätten die Unternehmen diese Möglichkeit ausschließen wollen, wäre dies über die Antwort „Weder abgeschlossen noch geplant" realisierbar gewesen.

Rund ein Drittel der Umfrageteilnehmer kann nicht beurteilen, ob ihr Unternehmen bereits über eine Cyberrisiko-Versicherung verfügt. Eventuell fehlt es hier an Fachkenntnis, Interesse oder der Möglichkeit eines Einblicks in das Versicherungsportfolio des Unternehmens.

Ein Grund, warum Unternehmen nicht an einer Cyberrisiko-Versicherung interessiert sind, könnte ferner die Tatsache sein, dass diese ihre Cyberrisiken bereits über sonstige, schon bestehende Versicherungen abgedeckt sehen und glauben, hier keine zusätzliche, spezielle Versicherungslösung zu benötigen:

4.2 Cyberrisiken als Deckungsbaustein bereits bestehender Versicherungen

Glauben Sie, dass die Cyberrisiken Ihres Unternehmens bereits über eine sonstige, schon bestehende Versicherung abgedeckt sind?

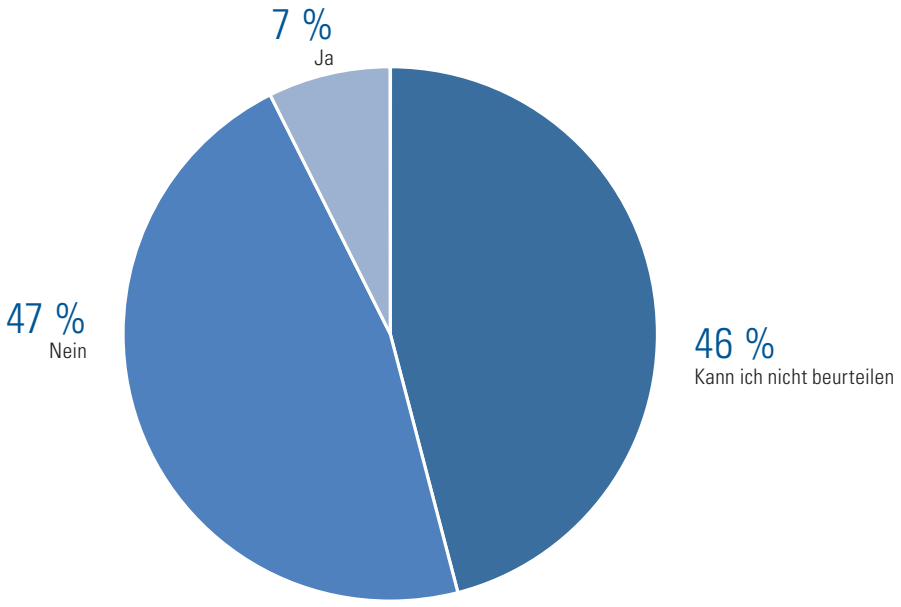

Abbildung 10

Der Anteil der Unternehmen, die der Meinung sind, ihre Cyberrisiken seien bereits über eine sonstige Versicherung abgedeckt, liegt im Rahmen dieser Umfrage bei 7 %. Genannt werden hier Betriebsunterbrechungs- (13 %), Elektronik- bzw. Hardware- (17 %) sowie D & O- und Rechtsschutz-Versicherungen (7 %). Der Großteil dieser Unternehmen (63 %) nennt hier explizit keine sonstigen Versicherungslösungen.

47 % der Unternehmen glauben nicht, dass ihre Cyberrisiken bereits anderweitig versichert sind und 46 % können nicht beurteilen, ob dies der Fall ist.

Knapp die Hälfte der Umfrageteilnehmer, die angeben, bereits eine Cyberrisiko-Versicherung abgeschlossen zu haben, wollen ihre Risiken ebenfalls über eine sonstige, schon bestehende Versicherung abgedeckt wissen. Sinn macht eine derartige Kombination der Antworten auf die Fragen 9 und 10 nur, wenn man davon ausgeht, diese Umfrageteilnehmer bezeichneten ihre sonstige, schon bestehende Versicherung als Cyberrisiko-Versicherung. Ob dieser Erkenntnis ist es wahrscheinlich, dass der tatsächliche Anteil der Unternehmen, die angeben, bereits eine Cyberrisiko-Versicherung abgeschlossen zu haben, um etwa die Hälfte geringer ist.

26 % der deutschen Unternehmen haben aktuell keine Cyberrisiko-Versicherung, und haben nicht geplant, eine solche abzuschließen und glauben ebenfalls nicht, dass ihre Cyberrisiken bereits über eine sonstige, schon bestehende Versicherung abgedeckt sind. Drei Viertel der Unternehmen, die Antworten in dieser Kombination abgegeben haben, bewerten die Effektivität des Risikotransfers mittels Versicherung im Rahmen der Frage acht als eher bzw. sehr gering.

4.3 Cyberrisiken – mögliche Deckungskomponenten

Was sollte durch eine Cyberrisiko-Versicherung für Ihr Unternehmen abgedeckt sein? Bitte wählen Sie die entsprechenden Elemente aus.

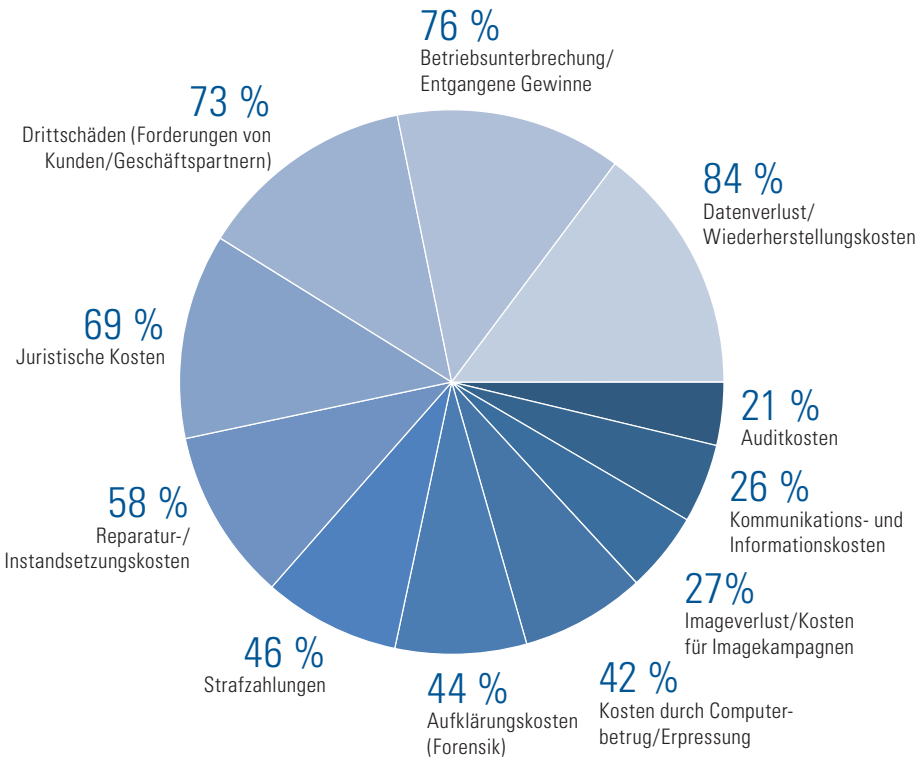

Abbildung 11

Insgesamt wird deutlich, dass einige Elemente für den Großteil der Unternehmen unerlässlich sind.
Hierzu gehören neben den Wiederherstellungskosten bei einem Datenverlust (84 %) und Kosten, die durch eine Betriebsunterbrechung infolge eines Cyber-Störfalls entstehen (76 %), auch Drittschäden (73 %) und juristische Kosten (69 %).

Deutlich weniger wichtig scheint die Übernahme von Kosten für einen Imageverlust durch einen Versicherer, obwohl die befragten Unternehmen der Beeinträchtigung ihrer Reputation die zweithöchste Bedeutung unter den Konsequenzen eines Cyberangriffs/-risikos beimessen[15]. Möglicherweise sind sich viele Unternehmen im Klaren, dass die Folgen eines Imageverlusts nur schwer zu monetarisieren sind.

So führt einer der Umfrageteilnehmer unter Sonstiges aus: „Wäre schön, wenn die unteren 5 auch durch eine Versicherung abzudecken wären, aber hier ergeben sich gesetzliche oder Bewertungsprobleme[16]."

Weitere Umfrageteilnehmer lassen an dieser Stelle verlauten, dass der Risikotransfer auf ein Versicherungsunternehmen der falsche Weg sei. Risikoprävention in Form aktiver Identifikation und Beseitigung von Risiken sei der bessere Ansatz. Solche Ausführungen decken sich mit den Ergebnissen aus dem Bereich Risikosteuerung, nach denen präventive Maßnahmen deutlich effektiver als reaktive Maßnahmen sind.

Zusätzlich genannt wurde die Einhaltung des Bundesdatenschutzgesetzes (BDSG) als versicherter Tatbestand. Nach § 42a BDSG haben nicht öffentliche Stellen, zu denen nach § 2 Absatz 4 BDSG auch private Unternehmen gehören, eine Informationspflicht gegenüber Einzelpersonen, sollten Dritte unrechtmäßig zur Kenntnis ihrer Daten kommen und „schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen" drohen.

15 Vgl. Frage 6, S. 25 - 27.

16 A. d. A.: Untere fünf Antwortmöglichkeiten in der Online-Ansicht des Fragebogens: Strafzahlungen, Kommunikations- und Informationskosten, Imageverlust / Kosten für Imagekampagnen, Aufklärungskosten (Forensik), Auditkosten.

4.4 Cyberrisiko-Versicherung – Risikotransfer: Eine Frage des Preises

Vorausgesetzt, eine Cyberrisiko-Versicherung wird den individuellen Anforderungen Ihres Unternehmens gerecht: Was wäre Ihnen der Risikotransfer wert? Bitte geben Sie an, in welchem Rahmen sich die Jahresprämie in Abhängigkeit von der entsprechenden Versicherungssumme (VS) bewegen dürfte.

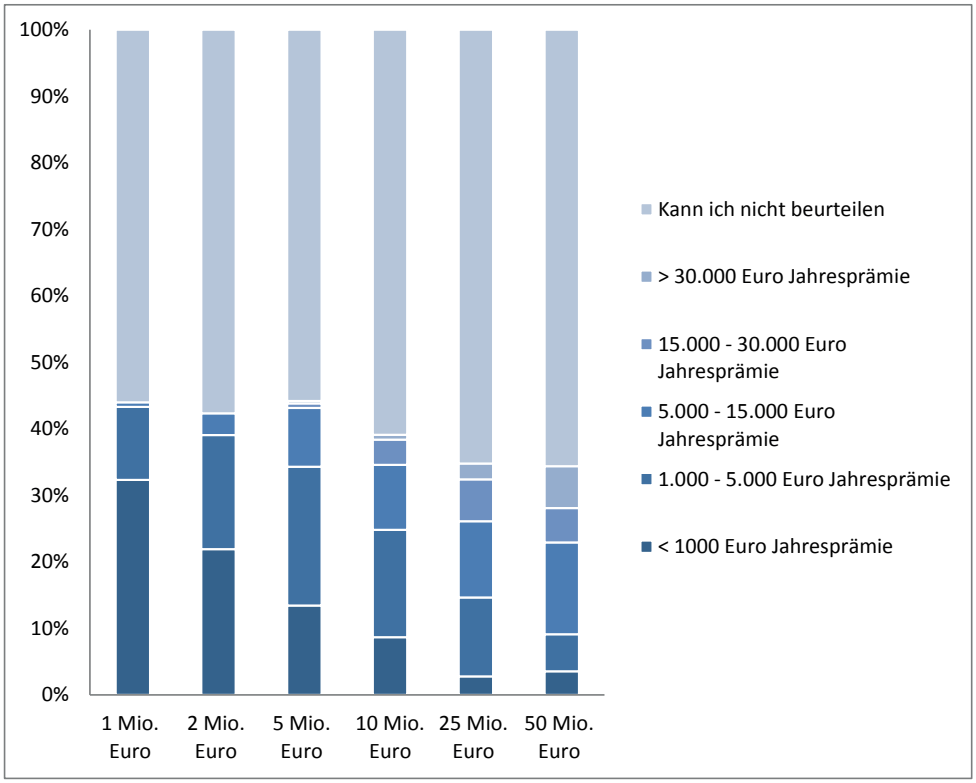

Abbildung 12

Durchschnittlich 60 % der Umfrageteilnehmer können nicht beurteilen, in welchem Rahmen sich die Zahlungsbereitschaft für Cyberrisiko-Versicherungen in ihrem Unternehmen bewegt. Cyberrisiken sind nur schwer greifbar und eine monetäre Bewertung möglicher Schäden und nötiger Absicherung fällt vielen Unternehmen scheinbar schwer.

Die Antworten zeigen, dass mit steigender Deckungssumme auch die Höhe der Prämien steigt, die Groß- und mittelständische Unternehmen zu zahlen bereit sind, um Cyberrisiken auf eine Versicherungsgesellschaft transferieren zu können.

Die Ergebnisse zeigen aber auch, dass lediglich 1 % der befragten Unternehmen bereit ist, für eine eigenständige Cyber-Versicherung mit adäquatem Deckungsumfang (z. B. 10 Mio. Euro) mehr als 30.000 Euro Jahresprämie zu zahlen. Die aktuelle Lage auf den Versicherungsmärkten zeigt hier eine große Diskrepanz im Kontext „Zahlungsbereitschaft vs. angebotenem Deckungsumfang“: Die Versicherungswirtschaft ist damit gefordert, an einer Weiterentwicklung der heutigen Konzepte zu arbeiten.

Unberücksichtigt bleiben an dieser Stelle Vergleiche dazu, inwieweit die Zahlungsbereitschaft für Cyberrisiko-Versicherungen mit der für andere Versicherungsprodukte vergleichbar ist. Grund hierfür ist, dass keine allgemeingültigen Aussagen darüber getroffen werden können, wie hoch Jahresprämien letztlich in der Praxis ausfallen. Jedes Unternehmen befindet sich in einer individuellen Risikosituation und bedarf daher auch einer subjektiven Betrachtung im Hinblick auf mögliche Prämiensätze. Dies gilt sowohl für Cyberrisiko-Versicherungen als auch für potenzielle Vergleichsprodukte.

5. FAZIT UND AUSBLICK

Das hohe Maß an medialer Aufmerksamkeit für Themen wie Cybercrime und Cyberrisiken in den letzten Monaten hat Wirkung gezeigt: Deutsche Unternehmen wagen sich in das Risikoneuland. Sie nehmen Cyberrisiken zwar wahr, es fehlt oft aber an entsprechenden Managementstrukturen, um Prozesse und Lösungen ganzheitlich für das Unternehmen aufbauen zu können.

Interne Cyberrisiken halten deutsche Unternehmen in Relation zu externen Cyberrisiken für besonders bedrohlich.

Cyber- bzw. Hackerangriffe an sich sind eine stetige Gefahr und finden nach Ansicht der Unternehmen auch regelmäßig statt, verbleiben aber meist im Stadium einer versuchten Schädigung.

Treten doch Schädigungen durch Cyberrisiken/-angriffe ein, sind der Verlust oder die Verletzung der Integrität von Daten Dritter und die hieraus resultierenden Haftungssituationen besonders bedeutsam. Eigenschäden werden als etwas weniger bedeutend bewertet.

In puncto Risikosteuerung setzen Unternehmen in Deutschland auf die Sensibilisierung ihrer Mitarbeiter für Cyberrisiken und halten Risikoprävention für sinnvoller und effektiver als reaktive Steuerungsmedien wie Cyber-Versicherungsprodukte.

Der Risikotransfer mittels Versicherung scheint noch schwer greifbar zu sein oder schlichtweg aufgrund einer gewissen Risikoaffinität im Bereich Cyberspace nicht benötigt zu werden. Offensichtlich hat die aktive Bewerbung von Cyberdeckungen durch die Versicherungswirtschaft bisher noch keine weitreichenden Effekte erzielt. Bezüglich der Zahlungsbereitschaft zeichnet sich dies dadurch ab, dass der Großteil der Unternehmen diese überhaupt nicht einschätzen kann oder nicht willens ist, hierfür hohe Prämien zu zahlen.

Fraglich bleibt, ob die Ergebnisse der vorliegenden Untersuchung auch längerfristig Geltung beweisen können. Schon eine zeitweilig verstärkte mediale Berichterstattung über große Schadenfälle im Kontext Cyberrisiken könnte die Wahrnehmung der Unternehmen gravierend verändern. Auch der konstante Fortschritt im Bereich der Informationstechnik und die hiermit verbundene Veränderung von Cyberrisiken könnten die Risikowahrnehmung deutscher Unternehmen nachhaltig beeinflussen.

Letztlich bestimmen die Vorteile der anonymen Online-Befragung auch die Grenzen dieser Untersuchung: Schnelligkeit, Zwanglosigkeit und Dynamik unterstützen eine prägnante Bestandsaufnahme, können aber auch eine lediglich temporäre Gültigkeit der Ergebnisse bedingen.

Vermutlich erhöht sich die Bedeutung von Cyberrisiken für deutsche Unternehmen in den kommenden Monaten. Produkte wie die Cyberrisiko-Versicherung dürften dann ähnlich wie im US-amerikanischen Markt vermehrt genutzt werden, ähnlich wie bei der Entwicklung und Akzeptanz der D & O-Versicherung.

Inhaltlich hinterlässt die vorliegende Untersuchung jedenfalls folgendes Bild: Eine akute, auffallend hohe Bedrohung durch Gefahren, die die weltweite Vernetzung über den

Cyberspace begleiten, sehen Unternehmen in Deutschland (noch) nicht.

Cyberrisiken sind für sie vielmehr Teil einer ubiquitären, aber nur mittelmäßigen Bedrohungssituation. Diese gilt es zu analysieren und weder zu unter- noch zu überschätzen. Eintretende Schadenszenarien werden durchaus als möglich betrachtet, nicht aber als zwingend wahrscheinlich.

6. CYBERRISIKO-ANALYSE ALS PRÄVENTIVE MASSNAHME ZUR SCHADENABWEHR

Die Studienergebnisse zeigen, dass die Risiken im Cyber-Bereich nicht klar von Unternehmen benannt werden können und auch mögliche Schadenpotenziale oftmals noch eine Black-Box für Unternehmen darstellen.

In der Praxis kann immer wieder festgestellt werden, dass Cyberrisiken fast ausschließlich im Verantwortungsbereich der IT gesehen werden. Vielfach gibt es keine klar geregelten Verantwortlichkeiten für die Schnittstelle zwischen digitaler und analoger Wertschöpfung. Diese Unternehmensstrukturen führen häufig zu schwerwiegenden Schadenverläufen und die fehlende Verantwortlichkeit kostet wertvolle Zeit im Schadenfall. Wenn z. B. trotz aller Softwareupdates und neuester Hardware ein Schaden oder ein Hackerangriff droht, muss sich ein Unternehmen über die Auswirkungen bewusst sein. Was bedeutet dieser Angriff auch für die Wertschöpfungskette und welche Wechselwirkungen gibt es insgesamt?

Der Leiter einer IT-Abteilung wird in der Regel diese Fragen nicht beantworten und somit auch keine Rückschlüsse darauf ziehen können, was dieser Schaden für die Existenz des Unternehmens bedeutet. Nur wenige für die Geschäfts-IT zuständige Manager haben ein ausreichendes Verständnis dafür, was an Fertigungsstraßen und Roboterlandschaften IT-mäßig so alles vor sich geht. Verschärft wird die Situation noch durch die zunehmende Anzahl von Drahtlosnetzen sowie mobilen Geräten und den Trend zur Fernwartung – die oft genug mit unprofessionell gesicherten Zugängen ausgestattet sind. Echte Profis haben kaum Probleme, ungesicherte Einfallstore in der Produktionslandschaft zu identifizieren.

Dabei sollte die Security, gerade in produzierenden Branchen, einen Spitzenplatz bei den infrastrukturbezogenen Themen einnehmen – und zwar entlang der gesamten Wertschöpfungskette, von Zulieferern über Hersteller bis zur Händlerschaft. Das ist nur konsequent: Wirtschaftsspionage ist mittlerweile einer der größten Teilbereiche der IT-bezogenen Kriminalität.

Wird die IT-Landschaft sorgfältig gemanagt, stellt sie nicht notwendigerweise ein Risiko dar. Das Gefährdungspotenzial bleibt aber, denn nichts ist 100 % sicher, darin sind sich alle Experten einig. Die Quintessenz: Es kommt darauf an, dem Angreifer die entscheidende Nasenlänge voraus zu sein.

6.1 Analyseansatz von Funk RMCE – Risikopotenziale erkennen, Maßnahmen ergreifen

Um mehr Transparenz im Unternehmen zu erzeugen und das Risikoverständnis für die Cyberrisiken in Unternehmen zu verbessern, hat Funk RMCE einen speziellen Analyseansatz entwickelt.

Dieser besteht aus fünf Schritten und verknüpft die Eigenschaften des klassischen Risikomanagements mit den neuen Themen aus dem Cyber-Bereich.

Abbildung 13: Ablauf einer Cyber-Risk-Analyse

In dem ersten Schritt – der **Spezifikation** – werden die Projektziele und das dazugehörige Projektteam verbindlich festgelegt. Gute Erfahrungen konnten in der Praxis damit gemacht werden, neben dem Leiter IT auch den Leiter Einkauf, den Vertrieb, das Versicherungswesen, den Produktionsleiter und einen Mitarbeiter aus dem Risikomanagement einzubinden. Jeder dieser Teilnehmer kann einen wichtigen Beitrag leisten, wenn es später um die Risikoanalyse geht.

Bei den Projektzielen können Unternehmen sich zum einen um die Transferierbarkeit der Risiken im Rahmen einer Versicherungslösung kümmern oder alternativ eine betriebswirtschaftliche Herangehensweise wählen, um z. B. auch Wechselwirkungen bzgl. etwaiger Betriebsunterbrechungen transparent machen zu können.

Die **Risikoidentifikation** und die **Bewertung** können in einem interdisziplinären Workshop zusammen durchgeführt werden. Bei diesem Schritt sollte darauf geachtet werden, dass das unternehmensinterne Risikomanagement mit einbezogen wird. Im Risikomanagement spielen Fragestellungen bzgl. der Wechselwirkungen und Bewertungen eine wichtige Rolle. Darüber hinaus ist die Frage zu stellen: Ab wann stellt ein Risikoszenario für das Unternehmen ein bedeutendes Risiko dar und ab welcher Größenklasse an Schadenpotenzial werden weitere Maßnahmen eingeleitet und geplant?

Um möglichst alle relevanten Risiken im Unternehmen identifizieren zu können, sollten Unternehmen sich zumindest einen Tag Zeit nehmen. Denkbar sind Szenarien wie z. B. der Ausfall von Unternehmensservern oder Energiezufuhr, aber auch Sabotage oder Fehlbedienung durch Mitarbeiter. Der Einsatz von Risikofeldermatrizen und Checklisten ist in der Praxis üblich – sie erleichtern die Identifikation erheblich und stellen auch sicher, dass nicht zu viele Ressourcen während des Projektes gebunden werden.

Bei der Bewertung sollten vorerst qualitative Einschätzungen vorgenommen werden, z. B. anhand einer Risiko-Relevanzskala. Bei allen wesentlichen Risiken ab einer gewissen Relevanzstufe sollten Risiken auch quantitativ bewertet werden. Hierbei werden dann Einschätzungen über die Eintrittswahrscheinlichkeiten und Schadenausmaße vorgenommen.

Das Ergebnis der Risikoanalyse ist ein priorisiertes **Risikoinventar**, das Aufschluss darüber gibt, welche Risiken wirklich die schwerwiegenden im Cyber-Bereich sind und welche Wechselwirkungspotenziale zu anderen Unternehmensbereichen bestehen. Wer seine Risiken auf diesem Weg identifiziert, analysiert und bewertet, wird eine deutlich erhöhte Transparenz im Unternehmen schaffen können. Der Mehrwert macht sich insbesondere in der Risikobewältigung bemerkbar.

Nur wenn Unternehmen ihr Risiko kennen, können sie auch einschätzen, welche **Bewältigungsmaßnahme** die passende ist und ob diese auch monetär betrachtet die beste Alternative darstellt. Gerade für die Erstellung einer **Transferlösung** ist der Aufbau eines priorisierten Risikoinventares sinnvoll.

Zusammengefasst hilft die Cyber-Risk-Analyse, bestehende Risikopotenziale im Unternehmen transparent zu machen, etwaige Absicherungsmaßnahmen zu überprüfen und die Notwendigkeit möglicher zusätzlicher Maßnahmen zu diskutieren.

Im Fokus des Projektes stehen insbesondere mögliche Schäden aus:

- Betriebsunterbrechung
- Dritthaftung
- Imageschädigung
- Know-how-Verluste

Ursachen wie z. B. Datenverluste oder -manipulationen (z. B. Hackerangriffe), Nichtverfügbarkeit der Systeme, Computerviren, Fehlbedienungen sowie Ausfall der Stromversorgung werden in einem Workshop mit Mitarbeitern aus allen Unternehmensbereichen diskutiert und analysiert.

7. STAND DER VERSICHERBARKEIT VON CYBERRISIKEN (SEPTEMBER 2014)

Cyberrisiken sind grundsätzlich über die „klassischen" Versicherungsprodukte, wie z. B. die Betriebs-Haftpflicht-, Technische- oder Vertrauensschaden-Versicherung versicherbar. Ganz überwiegend beinhalten diese aber lediglich Teilbereiche. Wichtige Deckungsbestandteile, insbesondere im Kosten- und Eigenschadenbereich, auf die noch ausführlicher eingegangen wird, fehlen oder sind stark sublimitiert. Auch ist die Eintrittspflicht für den Versicherungsschutz an Voraussetzungen geknüpft, die nicht dem speziellen Risiko angepasst und somit oftmals nicht gegeben sind. Zu nennen ist hier beispielsweise, dass eine Bereicherungsabsicht oder ein Verschulden vorliegen muss, um Deckungsschutz zu erhalten. Ein Großteil der Schadenfälle resultiert aber aus der Unachtsamkeit von Mitarbeitern, so dass die Szenarien folglich nicht versichert wären. Darüber hinaus sehen die „klassischen" Versicherungsprodukte mitunter umfangreiche Cyberrisiko-Ausschlüsse vor.

In den USA sind spezielle Cyberrisiko-Policen seit Mitte der 1990er-Jahre bekannt. Eine Belebung des Marktes fand allerdings erst 2003 statt. Ausgelöst wurde dies durch eine kalifornische Gesetzgebung, die Unternehmen, die von einem Verlust personenbezogener Daten betroffen sind, verpflichtet, die Betroffenen zu unterrichten. Fast alle US-Bundesstaaten haben regulatorisch nachgezogen.

Seit einiger Zeit gibt es auf dem Versicherungsmarkt auch in Europa und Deutschland spezielle Cyberrisiko-Policen. Hier bieten die Versicherer ein weitergehendes und bezüglich der klassischen Versicherungssparten bereichsübergreifendes Paket an definierten Cyberrisiken an. Zum einen sehen die Deckungskonzepte Versicherungsschutz für Datenrechts- und/oder Vertraulichkeitsverletzungen und insbesondere deren Folgen vor. Zum anderen Schäden aufgrund der Nutzung des Internets. Hier sind speziell Schäden durch Schadprogramme, Hackerangriffe, aber auch durch digitale rechtswidrige Kommunikation zu nennen.

Die Policen sind häufig im Bausteinsystem aufgebaut, unterscheiden sich zwischen Dritt- und Eigenschäden und beinhalten spezielle Serviceleistungen. Eine umfangreiche Risikoanalyse mit anschließender präventiver Krisenberatung durch einen externen Dienstleister stellen einige Versicherer bereits vor Vertragsabschluss zur Verfügung. Die Kosten werden über den Abschluss subventioniert und nur fällig, wenn man sich gegen die Absicherung entscheidet.

Im Bereich „Drittschäden" werden Ansprüche versichert, die aus Datenschutz-, Vertraulichkeits- oder Netzwerksicherheitsverletzungen sowie rechtswidriger digitaler Kommunikation entstehen. Darüber hinaus bieten einige Versicherer ebenfalls Versicherungsschutz für die Verletzung von Benachrichtigungspflichten und damit zusammenhängende Bußgelder, für Verfahrenskosten oder für Entschädigungen mit Strafcharakter (z. B. punitive oder exemplary damages). Bei Bedarf können optional Vertragsstrafen, wie sie etwa in den Payment Card Industry Data Security-Standards üblicherweise vereinbart sind, versichert werden.

Den größten Mehrwert gegenüber den „klassischen" Versicherungsprodukten weisen die speziellen Cyberrisiko-Policen im Bereich „Eigenschäden" auf. Hier gibt es derzeit u. a. folgende Absicherungsmöglichkeiten:

- **Kosten für Computer-Forensik**
  Der Versicherer entschädigt die notwendigen Kosten für externe Computer-Forensik-Analysen zur Ermittlung der Ursache sowie für die Identifizierung der betroffenen Dateninhaber bei einer möglichen Datenrechtsverletzung.

- **Kosten für Rechtsberatung**
  Hier besteht Versicherungsschutz für Honorare und Auslagen, die für die rechtliche Prüfung des dem Versicherungsfall zugrunde liegenden Sachverhalts einschließlich einer Empfehlung zur weiteren rechtlichen Vorgehensweise notwendig sind.

- **Benachrichtigungskosten**
  Sofern eine Verpflichtung zur Benachrichtigung von betroffenen Dateninhabern besteht, leistet der Versicherer für Aufwendungen zur Benachrichtigung der Betroffenen und der verantwortlichen Datenschutzbehörde.

- **Monitoringkosten**
  Sofern es Anhaltspunkte für den Missbrauch mit personenbezogenen Daten Betroffener im Zusammenhang mit Kreditkartendaten gibt, besteht Versicherungsschutz für Monitoring-Aufwendungen zur Prüfung und Benachrichtigung.

- **Kosten zur Schadenminderung**
  Versicherungsschutz besteht für Aufwendungen, Vergütungen und Auslagen, die zur Minderung der negativen Folgen einer Informationssicherheitsverletzung oder zur Verkürzung des Zeitraums einer Betriebsunterbrechung nötig sind.

- **Betriebsunterbrechungsschäden**
  Versicherungsschutz besteht für Ertragsausfallschäden, die aufgrund einer Nichtverfügbarkeit des Computersystems entstanden sind.

- **Kosten zur Wiederherstellung von Daten sowie der Funktionsfähigkeit der IT**
  Der Versicherer erstattet Aufwendungen, die für die Wiederherstellung oder die Reparatur der Website, des Intranets, des Netzwerks, des Computersystems, der Programme oder der elektronisch aufbewahrten Daten entstanden sind. Darüber hinaus bieten einige Versicherer auch eine Sicherheitsanalyse einschließlich der Kostenübernahme von Sicherheitsverbesserungen an.

- **Kosten für Public-Relations-Maßnahmen**
  Kosten für Public-Relations-Maßnahmen als Reaktion auf nachteilige oder ungünstige Publizität oder Aufmerksamkeit der Medien werden vom Versicherer getragen.

- **Aufwendungen für Erpressungsgelder und Krisenberater**
  Der Versicherungsschutz umfasst Erpressungsgelder sowie Gebühren und Auslagen eines Krisenberaters.

- **Cyber-Diebstahl-Schäden**
  Der Versicherungsschutz umfasst den Verlust von Geldern oder Übertragung von Wertpapieren oder den Verlust von Waren aufgrund einer unbefugten Lieferung dieser Waren, der aus einer externen Datenübertragung durch oder in das Netzwerk des Versicherten resultiert.

Die Cyber-Policen verfügen somit über einen deutlich umfangreicheren und abgestimmteren Versicherungsschutz als die „klassischen" Versicherungsprodukte. Eine All-Risk-Lösung gegen die sehr komplexe Gefahr „Cyber" sind die angebotenen Standardprodukte aber nicht. Auch wenn die Versicherer in ihren Policen regelmäßig alle wichtigen Haftpflicht- und Kostenpositionen anbieten, ist der Umfang, der sich hinter den Bausteinen verbirgt, stark abweichend. Die versicherten Gefahren und Schäden sowie die einzelnen Definitionen zur Beschreibung dieser unterscheiden sich je nach Baustein und führen dadurch zu erheblichen Deckungsunterschieden. Umso wichtiger ist es, den Versicherungsschutz individuell auf den Bedarf des Kunden abzustimmen. Dies erfordert vorab eine umfangreiche Risikoanalyse, wobei der Fokus auf ein ganzheitliches Risikomanagement gelegt werden sollte. Im Anschluss ist der Deckungsumfang individuell auf die besonderen Bedürfnisse und die Risikosituation des Kunden mit dem Versicherer zu verhandeln.

Durch den zunehmenden Wettbewerb auf dem Markt werden in den nächsten Jahren eine deutliche Harmonisierung und Optimierung der Bedingungswerke sowie sinkende Preise erwartet. Auch wird unter anderem durch Schäden bzw. Schadenszenarien, die jetzt noch nicht vorhersehbar sind, die Absicherung derartig komplexer Risiken auch im Zusammenhang mit steigenden Compliance-Anforderungen mehr in den Fokus des Risikomanagements von Unternehmen rücken. Es kann davon ausgegangen werden, dass in fünf bis zehn Jahren „Cyber"-Policen als grundlegende Existenzsicherung eine breite Marktabdeckung erfahren werden.

ABKÜRZUNGSVERZEICHNIS

A. d. A.	Anmerkung des Autors
BKA	Bundeskriminalamt
bzw.	beziehungsweise
D & O	Directors & Officers
ebd.	ebenda
etc.	et cetera
IT	Informationstechnik
k. A.	keine Angaben
Mio.	Millionen
US	United States (of America)
vgl.	vergleiche
z. B.	zum Beispiel

ABBILDUNGSVERZEICHNIS

QUELLENVERZEICHNIS

BKA 2012 — Bundeskriminalamt, Cybercrime. Bundeslagebild 2012, 2012, abrufbar unter: http://www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true, (Erstelldatum: k. A., Verfügbarkeitsdatum: 11.02.2014)

CEBULA/YOUNG 2010 — Cebula, James J., Young, Lisa R., A Taxonomy of Operational Cyber Security Risks, Dezember 2010, abrufbar unter: http://resources.sei.cmu.edu/asset_files/TechnicalNote/2010_004_001_15200.pdf, (Erstelldatum: k. A., Verfügbarkeitsdatum: 12.02.2014), S. 16

CNSS 2010 — Committee on National Security Systems (CNSS), CNSS Instruction No. 4009. National Information Assurance (IA) Glossary, 26.04.2010, abrufbar unter: http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf, (Erstelldatum: k. A., Verfügbarkeitsdatum 12.02.2014), S. 22

JUNG 2013 — Jung, Marcus, Virtuelle Kampfzone, in: JUVE Rechtsmarkt, 16 (2013) Nr. 11 November 2013

WEF 2013 — World Economic Forum, Global Risks 2014. Ninth Edition, Dezember 2013, abrufbar unter: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf, (Erstelldatum: k. A., Verfügbarkeitsdatum: 10.02.2014), S. 39

Anmerkung

Funk dankt Herrn Julian Meister für die Zurverfügungstellung der Ergebnisse seiner Bachelor-Arbeit.

Das hier vorliegende Dokument basiert auf der von Herrn Meister eingereichten Arbeit.

Ausführliche Literaturhinweise, Ableitungen zu Antwortverhalten der befragten Unternehmen sowie weiterführende Diagramme erhalten Sie auf Anforderung bei Funk, Frau Ulrike Meyer, Business Development Manager, u.meyer@funk-gruppe.de.

Über Funk RMCE

Seit über 15 Jahren berät Funk RMCE Unternehmen beim Aufbau sowie Optimierung ganzheitlicher Risikomanagement-Systeme. Hierbei steht für die Gesellschaft die methodische Unterstützung ihrer Kunden im Vordergrund. Darüber hinaus bietet Funk RMCE ihren Kunden effiziente Softwarelösungen im Bereich der Identifikation, Bewertung, Steuerung und Bewältigung von Risiken sowie spezielle Analyse-Tools im Kontext von Betriebsunterbrechungen an. Funk RMCE ist auch Initiator verschiedener Branchen-Arbeitskreise zum Thema Risikomanagement, z. B. für die Ernährungswirtschaft, Automobilzulieferindustrie sowie Energieversorgung.

Aktuell hat Funk RMCE mit der „Cyber-Risk-Analyse" einen Beratungsansatz entwickelt, der Unternehmen bei der Identifikation von Cyberrisiken unterstützt und etwaige Absicherungsmaßnahmen überprüft und ggf. sinnvoll ergänzt.

Funk RMCE ist ein Unternehmen von Funk, dem größten eigenständigen Versicherungsmakler und Risk Consultant in Deutschland sowie einer der Branchenführer Europas.

Ansprechpartner Funk RMCE

Hendrik F. Löffler

Funk RMCE
Valentinskamp 20 | 20354 Hamburg
fon + 49 40 359 14-642 | fax + 49 40 359 14 73-642 | Mobil +49 172 459 2281
h.loeffler@funk-gruppe.de | FUNK-GRUPPE.DE

Herausgeber

Funk RMCE
Valentinskamp 20 | 20354 Hamburg
www.rmce.de

Hendrik F. Löffler, Nadine Sopart, Ulrike Meyer, Julian Meister, Michael Winte

Meinungsbeiträge geben die Auffassung der Autoren wieder.

Impressum

Funk RMCE GmbH
(Hrsg.): Studie zum Stand der gegenwärtigen Wahrnehmung von Cyberrisiken in deutschen Unternehmen
Valentinskamp 20 | 20354 Hamburg

Printed in Germany

Funk RMCE GmbH | Valentinskamp 20 | 20354 Hamburg
fon +49 40 35914-0 | fax +49 40 35914-406 | welcome@funk-gruppe.de

FUNK-GRUPPE.COM