

# WHITEPAPER

Möglichkeiten und Wege einer Kooperation von  
Großanwendern und IT-Sicherheitsindustrie für ein höheres  
Maß an IT-Sicherheit und Vertrauenswürdigkeit

Dieses Dokument ist im Rahmen einer Masterarbeit an der Westfälischen Hochschule in Kooperation mit dem Bundesverband IT-Sicherheit e.V. (TeleTrusT), dem VOICE e.V. und dem ASW Verband e.V. im Studiengang Master Internet-Sicherheit entstanden.

## **Die Arbeit wurde betreut durch:**

### **Prof. Dr. Norbert Pohlmann,**

Professor für verteilte Systeme und Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen im Fachbereich Informatik und Kommunikation und weiteren Engagements bei:

- Bundesverband IT-Sicherheit e.V. - TeleTrusT (Vorstandsvorsitzender)
- Verband der Internetwirtschaft - eco (Vorstandsmitglied)
- EuroCloud Deutschland\_eco e.V. (Vorstandsmitglied)
- GDD (Mitglied des Wissenschaftlichen Beirats)
- Lenkungskreis Initiative "IT-Sicherheit in der Wirtschaft" des BMWi (Mitglied)

sowie

### **Dr. Rainer Baumgart,**

Vorstandsvorsitzender (CEO) der secunet Security Networks AG und weiteren Engagements bei:

- Stakeholder Group der ENISA – der European Network and Information Security Agency
- Langjähriges Vorstandsmitglied im Bundesverband IT-Sicherheit e.V. (TeleTrusT)
- Berufenes Mitglied des Programmbeirats des Deutschen IT-Sicherheitskongresses

Essen, den 01.02.2019

Autor: Sebastian Barchnicki

[https://www.xing.com/profile/Sebastian\\_Barchnicki/](https://www.xing.com/profile/Sebastian_Barchnicki/)

<https://www.linkedin.com/in/sebastianbarchnicki/>

## Zusammenfassung

Die immer vielfältiger werdenden IT-Systeme bilden heute einen essenziellen Teil unserer Gesellschaft. Diese komplexen Systeme bieten eine breite Angriffsfläche und können durch gezielte Attacken manipuliert werden oder gänzlich ausfallen. Dieser Umstand vergrößert mit zunehmender Digitalisierung die Angriffsfläche für den Wirtschaftsraum und unsere Gesellschaft in einem bisher nie dagewesenen Ausmaß. Umso wichtiger ist die heutige, als auch zukünftige Rolle der IT-Sicherheit.

Ein hohes Sicherheitsniveau ist unter diesen Aspekten wichtig und kann nur durch den breiten und angemessenen Einsatz von IT-Sicherheitsprodukten erreicht werden. Aber wie lässt sich so etwas in der Breite umsetzen und was sind die notwendigen Voraussetzungen? Dieser Frage wurde mit Hilfe der vorliegenden Ausarbeitung und einer hierfür ausführlichen Befragung der DAX Unternehmen im Detail nachgegangen, welche einen beträchtlichen Anteil der Wirtschaftskraft in Deutschland darstellen. Dankenswerter Weise haben die Konzerne und wichtige Verbände diese Initiative begrüßt und mitgetragen. Dies führte zu einem großen Zuspruch bei den CISOs und CIOs der Großunternehmen, die sich als Verantwortungsträger den zahlreichen Fragen bereitwillig und umfassend gestellt haben.

Die Ergebnisse könnten interessanter nicht sein und bilden einen einzigartigen tiefen Einblick in die Denkweise, Bedürfnisse und Erwartungen der Großanwender. Dabei wurden Themen adressiert, wie die Beschaffung von IT-Sicherheitsprodukten und die damit zusammenhängenden Kriterien. Zudem wurde zum Einsatz von IT-Sicherheit auch die Position zu den Mitbewerbern erfragt und die Idee eines gemeinsamen DAX 30 Cyberlagezentrums diskutiert. Eines der wichtigsten Themen waren anschließend die Fragen nach den Erwartungen und besonderen Kompetenzen der IT-Sicherheitsindustrie in Deutschland, der Beurteilung der Qualität und der Bedeutung von Start-Ups. Weiterhin wurde die Bereitschaft abgefragt, größere Technologiesprünge zu machen auf Kosten übermäßig großer Investitionen. Auch das Thema Open Source wurde diskutiert und die Bereitschaft der Mitgründung bzw. Finanzierung eines Open Source Fonds zur Förderung wichtiger Kernprojekte abgefragt.

Des Weiteren war die Wahrnehmung des Marktes aus der Anwenderperspektive interessant. Demzufolge wurden die detaillierten Meinungen zu den Defiziten bei IT-Sicherheitsprodukten und dem Vertrauen in deutsche Produkte „made in Germany“ abgefragt. Ergänzend dazu wurde auch möglichen Aufgaben des Staates, Fragen zum breiteren Einsatz von Verschlüsselung und der Kontroverse rund um absichtliche Backdoors für eine regulierte Entschlüsselung Raum gegeben.

Die befragten Entscheidungsträger verfügen in ihrer Position über einen bedeutenden Erfahrungsschatz und setzen sich nicht nur mit heutigen Herausforderungen, sondern auch mit zukünftigen IT-Sicherheitsfragen auseinander, daher wurden diese ebenfalls thematisiert. So wurden in diesem Kontext die zu erwartenden Sicherheitsanforderungen in 3 bis 5 Jahren abgefragt. Darüber hinaus wurde darum gebeten einen deutlich tieferen Blick in die Zukunft zu wagen, bezüglich einer Einschätzung der Anforderungen in 10+ Jahren.

Die Notwendigkeit einer Zusammenarbeit zwischen den Großanwendern und der IT-Sicherheitsindustrie wurde nicht nur deutlich, sondern wird auch von allen in der Breite begrüßt. Hierfür ist eine klare Bereitschaft aller Beteiligten signalisiert worden, denn heute findet die Begegnung zwischen den Großanwendern und der IT-Sicherheitsindustrie nicht auf Augenhöhe statt. Erwartungsgemäß gibt es aus den verschiedensten Gründen auch einzelne dokumentierte Vorbehalte, allerdings hilft die Kenntnis darüber, diesen zu begegnen. Auf diese Weise kann eine Kooperation einfacher motiviert und durchgeführt werden.

Basierend auf den Aussagen und ausgewerteten Informationen, wurden in den einzelnen Abschnitten Implikationen formuliert, um eine erste Hilfestellung bei der Interpretation zu geben. Diese sollen dabei helfen, die richtigen Schlüsse ziehen zu können.

Dabei ist eines deutlich geworden: Letztendlich müssen sich die IT-Sicherheitshersteller zukünftig verändern, indem sie eine höhere Qualität, Skalierbarkeit und internationale Verfügbarkeit anbieten.

*» Menschen, die verrückt genug sind zu denken, sie könnten die Welt verändern, sind diejenigen, die es auch tun. «*

*Steve Jobs*

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b> .....	<b>1</b>
1.1	IT: Grundpfeiler unserer Gesellschaft.....	1
1.2	Motivation.....	1
1.3	Ziele dieser Arbeit.....	4
1.4	Methodik.....	4
<b>2</b>	<b>Art und Rollenverteilung einer Zusammenarbeit</b> .....	<b>8</b>
2.1	Aufgaben und Mehrwert für Hersteller .....	8
2.2	Bedürfnisse und Mehrwert von Anwendern.....	8
2.3	Aufgaben für Hochschulen und Forschung .....	8
2.4	Aufgaben für Verbände .....	9
2.5	Verantwortung für Politik, Gesellschaft und der resultierende Mehrwert.....	9
<b>3</b>	<b>Mögliche Hindernisse und Herausforderungen</b> .....	<b>11</b>
<b>4</b>	<b>Ergebnisse der Datenerhebung bei den Großanwendern der DAX30</b> .....	<b>14</b>
4.1	Allgemeine Informationen .....	14
4.1.1	Computer Emergency Response Team (CERT).....	16
4.1.2	Schwerpunkte bei der IT-Sicherheit .....	17
4.2	Beschaffung .....	19
4.2.1	Informationen zu Budgets.....	19
4.2.2	Lizenzierungsmodelle von IT-Sicherheit .....	19
4.2.3	Kriterien und Aspekte zur Beschaffung von IT-Sicherheitsprodukten.....	20
4.2.4	Durchschnittliche Lebenszyklen von IT-Systemen.....	21
4.2.5	Angemessene Relationen: Anschaffungspreis IT und Kosten für IT-Sicherheit.....	22
4.2.6	Beurteilung der Idee des TeleTrust-Wirkungsklassenmodells.....	23
4.2.7	Relevante Faktoren für Anschaffung von IT-Sicherheitsprodukten .....	24
4.2.8	Die wichtigsten Kennzahlen im Überblick.....	26
4.3	Einsatz von IT-Sicherheit.....	27
4.3.1	Einsatz und Dauer von beschafften IT-Sicherheitsprodukten .....	27
4.3.2	Blick auf die Mitbewerber in Bezug auf Großanwender untereinander .....	27
4.3.3	Einsatz und Erfahrungen mit Kommunikationslagebildern.....	28
4.3.4	Fiktive Idee eines „CYBERLAGEZENTRUM aller DAX30“ .....	29
4.4	Allgemeines rund um das IT-Sicherheitsangebot .....	32
4.4.1	Besondere Kompetenzen der deutschen IT-Sicherheitsindustrie.....	32
4.4.2	Beurteilung von Qualität bei IT-Sicherheit.....	34
4.4.3	Beurteilung relevanter Kriterien von IT-Sicherheitsherstellern .....	35
4.4.4	Relevanz bei der Größe von Marktanbietern.....	37
4.4.5	Bedeutung von Start-Ups .....	37
4.4.6	Einsatz von Start-Up Produkten.....	40
4.4.7	Wichtige Aspekte als Definition der Qualität von IT-Sicherheitsprodukten .....	41
4.4.8	Vergleich zwischen deutschen Anbietern und Weltmarktführern .....	42
4.4.9	Bewertung und Priorisierung von internationalem Support.....	42
4.4.10	Individuallösungen oder Standardlösungen .....	43
4.4.11	Einsatz und Förderung von Open Source .....	43
4.4.12	Defizite und Erwartungen von/an IT-Sicherheitsprodukten und Anbietern.....	46
4.4.13	Fragmentierung des IT-Sicherheitsmarktes .....	49
4.4.14	Bewusste Akzeptanz von IT-Sicherheitsgefahren .....	49
4.4.15	Hochsicherheitslösungen .....	52
4.5	Marktsituation und Defizite.....	54
4.5.1	Wunsch nach Konsolidierung des Angebotes: Zusammenfassung von Produkten .....	54

4.5.2	Wunsch und Suche nach gänzlich fehlenden IT-Sicherheitsprodukten .....	55
4.5.3	Sicherheitsanforderungen der Zukunft in 5 und 10+ Jahren .....	55
4.5.4	Beurteilung der Leistung von Behörden (BSI, BKA, LKA, Polizei) .....	57
4.5.5	Verantwortung des Staates und seine Aufgaben .....	59
4.5.6	Verschlüsselung vs. Backdoors .....	60
4.5.7	Beurteilung der aktuellen IT-Sicherheitslage .....	62
4.6	Bereitschaft zur Zusammenarbeit und Kooperation von Großanwendern .....	63
4.6.1	Zusammenarbeit mit IT-Sicherheitsherstellern und Umsetzungsideen .....	63
4.6.2	Bereitschaft bei der Mitwirkung der Einführung von neuen Lösungen, Services und Kompetenzzentren.....	64
4.6.3	Akzeptanz höherer Kosten für große Technologiesprünge .....	67
4.6.4	Akzeptanz von Einschränkungen im Tausch für höhere Sicherheit .....	68
4.6.5	Beurteilung der Einkaufsmacht von Großanwendern .....	68
4.6.6	Gemeinsame Sicherheitsstrategie von Großanwendern und deren Messbarkeit .....	69
4.6.7	Zusammenarbeit mit ausgewählten relevanten Stakeholdern .....	70
4.6.8	Identifikation von Gründen gegen eine Zusammenarbeit.....	71
4.7	Abschließende Message an die IT-Sicherheitsbranche .....	73
5	<b>Thesepapier der Großanwender in Zusammenarbeit mit dem VOICE e.V.....</b>	<b>75</b>
6	<b>Fazit.....</b>	<b>76</b>
7	<b>Ausblick .....</b>	<b>78</b>
8	<b>Literatur.....</b>	<b>80</b>
9	<b>Abbildungsverzeichnis .....</b>	<b>81</b>
10	<b>Tabellenverzeichnis .....</b>	<b>83</b>
11	<b>Appendix 1: Wirkungsklassenmodell .....</b>	<b>84</b>

## 1 Einleitung

Das vorliegende Dokument beschäftigt sich mit den Möglichkeiten und Chancen einer engeren Kooperation zwischen Großanwendern, also großen Unternehmen mit komplexen skalierbaren IT-Strukturen und den Anbietern bzw. Herstellern von IT-Sicherheitsprodukten.

### 1.1 IT: Grundpfeiler unserer Gesellschaft

Die Unternehmenswelt besteht heute maßgeblich aus IT-Produkten, welche das Rückgrat im Büro, Bereichen der Kommunikation und in der Produktion auf allen Ebenen bilden. IT-Systeme schaffen nicht nur Vorteile bei der Produktivität und sorgen für eine hohe Effizienz respektive Flexibilität, sondern vergrößern auch gleichzeitig die mögliche Angriffsfläche eines Unternehmens.

Theoretisch kann beinahe jedes IT-System mit Hilfe eines gezielten Angriffs dafür ausgenutzt werden, sich Zugang zur gesamten IT-Infrastruktur zu verschaffen – vorausgesetzt es wurden keine entsprechenden Sicherheitsmaßnahmen getroffen. Diese können jedoch nur die zu überwindende Hürde für den Angreifer anheben mit dem Ziel, ihm sein Vorhaben maximal zu erschweren.

#### Schutz unserer Wissensgesellschaft

Wir können uns als Wissensgesellschaft Angriffe, bei denen wertvolles Wissen abfließt und unsere wirtschaftliche Kraft in nationaler Hinsicht gefährdet, auf Dauer nicht leisten. Neben den existenziellen Gefahren für bedrohte Unternehmen, ist ebenso das Bewahren der eigenen Reputation sehr wichtig. Aus diesen Gründen müssen Maßnahmen getroffen werden, die gezielte und flächendeckende Angriffe wirksam an ihrer erfolgreichen Durchführung hindern. Welche das genau sind, hängt von wesentlichen Faktoren wie dem eigenen Reifegrad und Schutzbedarf ab. Die jeweiligen Maßnahmen wurden unter anderem in früheren TeleTrusT-Veröffentlichungen<sup>1</sup> oder weiteren entsprechenden Veröffentlichungen in der Fachliteratur adressiert.

Mit Hilfe von Produkten, Lösungen und Services aus dem IT-Sicherheitsbereich lässt sich zwar den meisten Bedrohungen entgegenwirken, aber eine vollständige Sicherheit gibt es nicht. Ohnehin sollte es auch nicht das primäre Ziel sein, diese zu erreichen. Viel wichtiger ist es, Maßnahmen zu treffen und Prozesse anzupassen, um damit die Hürde für einen Angreifer so hoch wie nur möglich zu legen. Hierbei darf der Faktor Mensch keinesfalls vernachlässigt werden.

Wie liegen die Verhältnisse zwischen der deutschen IT-Sicherheitsindustrie und den internationalen Anbietern? Bei einer Betrachtung des weltweiten IT-Sicherheitsmarktes wird offensichtlich, dass eine Dominanz der ausländischen Hersteller herrscht. Insbesondere kommen in vielen Technologiebereichen die Produkte der Marktführer aus den USA aber auch aus Israel zum Einsatz. Die aus Deutschland stammenden Produkte und Technologien befinden sich zwar auf Augenhöhe zu den ausländischen Marktführern, allerdings werden sie weniger häufig eingesetzt. Hier stellt sich die Frage nach den Gründen, Problemen und möglichen Lösungen, die in der vorliegenden Arbeit diskutiert werden.

Im Hinblick auf diese Aspekte und Fragestellungen sollen die Potentiale, Gründe für Vorbehalte gegenüber deutschen IT-Sicherheitsprodukten, Wünsche und Hürden beider Seiten aufgezeigt und diskutiert werden.

### 1.2 Motivation

Heutige aus dem Ausland stammende Technologien sind auch immer an die jeweiligen gesetzlichen Vorgaben und kulturellen Denkweisen gekoppelt. Diese können sich nicht nur untereinander stark unterscheiden, sondern auch im direkten Vergleich zu deutschen und europäischen Werten ä-

---

<sup>1</sup> Bundesverband IT-Sicherheit e.V. (TeleTrusT): Publikationen,

URL: <https://www.teletrust.de/publikationen/broschueren/>

Stand: 16.07.2017, Zuletzt abgerufen: 16.07.2017

ßerst divergent sein. Das prominenteste Beispiel ist die weltweit unterschiedliche Sicht auf die Stärke der einzusetzenden Verschlüsselung und den andernorts verlangten Hintertüren oder dem Verbot höherwertigerer und sicherer Kryptografie. Die Komplexität dieser Problematik und die möglichen Konsequenzen sind oft tiefergehender und vielfältiger als die gesamte Diskussion erahnen lassen könnte. Die Begründung dafür ist oft gleich: Sicherheit der Gesellschaft und der Schutz vor Terror, oft jedoch auch als politisches Machtinstrument zum Ausspähen, für Industriespionage und Überwachung. Diese immer wiederkehrenden „Argumente“ sind in einer Wissensgesellschaft ein zweischneidiges Schwert, da dies auch gleichzeitig Risiken birgt, dass die für den Schutz unseres geistigen Eigentums eingesetzten Technologien mit der „Möglichkeit der Öffnung durch Behörden“ auch immer missbraucht werden könnten. Vielleicht nicht von der jetzigen oder kommenden Regierung, aber kann dies auch für die darauffolgenden ausgeschlossen werden, sollte diese Tür einmal einen Spalt geöffnet worden sein?

Die weltweit führenden Technologiehersteller kommen heute zumeist aus den USA und bieten nicht unbedingt die qualitativ höherwertige Technologie, sind aber international sehr vertriebsstark aufgestellt und personell von hoher Quantität. Dies bedeutet gleichzeitig, dass sie auf dem deutschen und europäischen Markt in starker Konkurrenz zu den hiesigen Anbietern stehen und bei größeren Auftragsvolumina meist bevorzugt beauftragt werden. Die Gründe hierfür sind vielfältig und werden im Laufe dieser Arbeit genauer beleuchtet.

Auf dem heimischen Markt ist die IT-Sicherheitsindustrie aus Deutschland und Europa in vielen Punkten konkurrenzfähig. Um ein Ergebnis der hier durchgeführten Untersuchung vorweg zu nehmen, ist die internationale Vertriebsstärke womöglich noch ausbaufähig aber grundsätzlich sind das Potential und die Vielfalt der verfügbaren Technologien sehr breit und von hoher Güte.

### **Vertrauenswürdigkeit und Wirkung**

Die beiden Aspekte der Vertrauenswürdigkeit und Wirkung sind wichtige Faktoren, bei denen insbesondere die nationalen Anbieter punkten können. Wird das Thema der Backdoor-Freiheit oder Kryptografie ohne Vorbehalte betrachtet, führt kaum ein Weg an deutschen Produkten vorbei. Für den Einkauf ist dies vielleicht nicht immer der ausschlaggebende Grund, sich für ein Produkt zu entscheiden, aber es gibt für die Beschaffung im öffentlichen Sektor bereits erste ernstzunehmende Ansätze, wie beispielsweise die Überarbeitung des Vergaberechtes<sup>2</sup>. Eine neue Fassung fordert in Zukunft die schriftliche Zusicherung, dass durch den Hersteller keine absichtlichen Backdoors eingebaut wurden. Dies ist zwar nicht die finale Lösung für dieses Problem, da es vielschichtiger und komplexer ist, allerdings ist damit ein erster wichtiger Schritt getan.

---

<sup>2</sup> RA Thomas Feil: EVB-IT: Verbindliche Backdoor-Freiheits-Klausel in Hardwareverträgen,

URL: <https://www.recht-freundlich.de/evb-it/evb-it-verbindliche-backdoor-freiheits-klausel-in-hardwarevertraegen>.

Stand: 13.04.2016, Zuletzt abgerufen: 16.07.2017

### Nutzerakzeptanz und Usability

Auch sind die Erhöhung der Nutzerakzeptanz durch bessere Usability und Transparenz der eingesetzten Sicherheitstechnologien wichtige Schritte auf dem Weg zum Ziel<sup>3</sup>. Weitere mögliche Aspekte, wie z.B. Austauschbarkeit (*IT-Security-Replaceability*), wurden in der Vergangenheit ebenfalls bereits im Strategiepapier des Bundesverbands IT-Sicherheit e.V. (TeleTrust) „*IT-Sicherheitsstrategie für Deutschland - Wirkungsklassen von IT-Sicherheitsmaßnahmen für unterschiedliche Schutzbedarfe*“<sup>4</sup> diskutiert.

### Märkte und Potentiale: Größenverhältnisse DAX vs. Mittelstand für den IT-Sicherheitsmarkt

Interessant im Kontext dieser Arbeit ist auch die Frage nach dem durch die IT-Sicherheitshersteller adressierbaren IT-Sicherheitsmarkt in Deutschland. Für eine Bewertung der möglichen Kaufkraft aller DAX Unternehmen im Hinblick auf den IT-Sicherheitsmarkt ist auch ein Vergleich zu allen anderen kleineren Unternehmen im Mittelstand relevant.

Der deutsche Mittelstand hat im Jahr 2015 einen Gesamtumsatz von 2,217 Billionen EUR erzielt<sup>5</sup>. Im Vergleich dazu wurden 2016 durch die Großunternehmen des DAX30 1,325 Billionen EUR umgesetzt. Unter dem Aspekt, dass die betrachteten DAX Unternehmen im Durchschnitt ca. 0,1% ihres Gesamtumsatzes in IT-Sicherheit investieren, ergibt dies einen potenziellen Markt im Bereich der Großanwender DAX30 von etwa 1,32 Mrd. EUR. Unter der Annahme, dass der Mittelstand einen ähnlichen Anteil in die IT-Sicherheit investiert, ergibt dies einen Etat von 2,22 Mrd. EUR.



Abbildung 1: Gesamtmarkt DE für IT-Sicherheit nach Gesamtumsatz Mittelstand und DAX

Das bedeutet, dass der Markt für die IT-Sicherheitsindustrie im Bereich der mittelständischen Unternehmen, wie in der *Abbildung 1* dargestellt zwar größer ist, jedoch mehr Vertriebsaufwand zu leisten ist im Vergleich zu den insgesamt 30 Konzernen im DAX. Aus diesem Grund kann die vertriebliche Fokussierung auf diese Großanwender deutlich attraktiver, und mit weniger Ressourcen möglich sein.

<sup>3</sup> Prof. Dr. Thorsten Holz, Prof. Dr. Eric Bodden, Prof Dr. Matthew Smith, Prof Dr. Norbert Pohlmann: Human-Centered Systems Security: IT-Sicherheit von Menschen für Menschen,

URL: <https://www.it-sicherheit-nrw.de/forschungsaenda.html>,

Stand: 15.09.2017, Zuletzt abgerufen: 15.07.2017

<sup>4</sup> Sebastian Barchnicki: IT-Sicherheitsstrategie für Deutschland: Wirkungsklassen von IT-Sicherheitsmaßnahmen für unterschiedliche Schutzbedarfe

URL: <https://www.teletrust.de/publikationen/broschueren/wirkungsklassen/>,

Stand: 09.03.2015, Zuletzt abgerufen: 16.07.2017

<sup>5</sup> Statistisches Bundesamt; Bundesagentur für Arbeit; Institut für Freie Berufe Nürnberg; Berechnungen des IfM Bonn: Mittelstand im Überblick,

URL: <http://www.ifm-bonn.org/statistiken/mittelstand-im-ueberblick/#accordion=0&tab=1>,

Stand: 07/2017, Zuletzt abgerufen: 20.07.2017

Sollte die Gunst der DAX Unternehmen gewonnen werden, bedeutet dies auch im Umkehrschluss, alle im *Kapitel 4: Ergebnisse der Datenerhebung bei den Großanwendern der DAX30 ab Seite 14* beschriebenen Vorbehalte bei Seite geräumt und genau die gewünschten Bedürfnisse adressiert zu haben. Im Ergebnis kann diese aufgebaute Kompetenz einen deutlich reduzierten Aufwand für die mögliche Expansion in Richtung der internationalen Großanwender aller anderen Länder bedeuten, was wiederum den Zugang zu einem exorbitanten Markt auf globaler Ebene mit verhältnismäßig niedrigem Aufwand erlaubt.

Auch die Betrachtung anderer Quellen bestätigt diese Abschätzung. So spricht das BMWi in seiner Studie „Der IT-Sicherheitsmarkt in Deutschland“<sup>6</sup> 2014 von einem Markt (im „worst case“ Fall) mit einem Volumen von 3 bis 4 Mrd. EUR im Jahre 2020. Der „best case“ liegt aus Sicht des BMWi bei ca. 25 Mrd. EUR. Diese waren in einer zuvor erarbeiteten Studie deutlich niedriger angesetzt und in dieser Überarbeitung deutlich nach oben korrigiert worden. Dies ist ein Hinweis auf das aktuell rasante Wachstum der Branche und den schnell steigenden Bedarf. Des Weiteren wird die hier getroffene Annahme ebenfalls durch eine Analyse des Bitkom aus dem Jahr 2015 bestätigt, welcher den IT-Sicherheitsmarkt auf 3,723 Mrd. EUR beziffert<sup>7</sup> hat.

Der internationale Markt insgesamt ist hinsichtlich seiner Größe sehr attraktiv. Schätzungen des Cybersecurity Ventures<sup>8</sup> in Kalifornien in den USA zufolge, werden die weltweiten Ausgaben für Cyber Security von 2017 bis 2021 weltweit insgesamt den Betrag von etwa 1 Billion Dollar übersteigen. [1]

### 1.3 Ziele dieser Arbeit

Das übergeordnete Ziel dieser Arbeit besteht darin, einen Dialog zwischen den Großanwendern und der IT-Sicherheitsindustrie herzustellen, um am Ende eine erfolgreiche Kooperation zu motivieren.

Dabei ist eine der Intentionen die Begegnung beider Seiten auf Augenhöhe. Dies bedeutet, die realen Bedürfnisse und Wünsche der Großanwender in Einklang zu bringen mit den heutigen und zukünftigen Produkten und Services der IT-Sicherheitshersteller und IT-Sicherheitsanbieter.

Dieser Austausch soll mittel- bis langfristig für ein höheres Maß an Sicherheit und entsprechend mehr Vertrauenswürdigkeit sorgen und damit den heute überaus erfolgreichen Wirtschaftsstandort Deutschland langfristig sichern.

### 1.4 Methodik

Um das gesetzte Ziel der erfolgreichen Kooperation zwischen IT-Sicherheitsherstellern/IT-Sicherheitsanbietern und den Großanwendern in Deutschland zu erreichen, wurden zunächst die Großanwender definiert. Als Zielgruppe für die durchgeführte Untersuchung wurde hierfür die DAX30 Liste herangezogen.

#### DAX30 Großanwender

Die Abkürzung DAX steht für „Deutscher Aktienindex“ und repräsentiert den bedeutendsten deutschen Aktienindex. Er besteht aus den in der nachfolgenden *Tabelle 1* dargestellten 30 größten und umsatzstärksten Unternehmen, welche im Prime Standard an der Frankfurter Wertpapierbörse (Börse Frankfurt) gelistet sind.

Zum heutigen Zeitpunkt (Juni 2017) sind die folgenden Unternehmen im DAX30 gelistet:

<sup>6</sup> Herausgeber Bundesministerium für Wirtschaft und Energie (BMWi): Der IT-Sicherheitsmarkt in Deutschland, URL: [https://www.de.digital/DIGITAL/Redaktion/DE/Publikation/it-sicherheitsmarkt-in-deutschland-studie-2014.pdf?\\_\\_blob=publicationFile&v=4](https://www.de.digital/DIGITAL/Redaktion/DE/Publikation/it-sicherheitsmarkt-in-deutschland-studie-2014.pdf?__blob=publicationFile&v=4), Stand: November 2014, Zuletzt abgerufen: 01.11.2017

<sup>7</sup> Bitkom: Nachfrage nach IT-Sicherheit wächst kräftig, URL: <https://www.bitkom.org/Presse/Presseinformation/Nachfrage-nach-IT-Sicherheit-waechst-kraeftig.html>, Stand: 30.07.2015, Zuletzt abgerufen: 02.11.2017

<sup>8</sup> Cybersecurity Ventures: <http://cybersecurityventures.com/our-company/>

Adidas	Allianz	BASF
Bayer	Beiersdorf	BMW
Commerzbank	Continental	Daimler
Deutsche Bank	Deutsche Börse	Deutsche Post
Deutsche Telekom	E.ON	Fresenius
Fresenius Medical Care	HeidelbergCement	Henkel vz
Infineon	Linde	Lufthansa
Merck	Muenchener Rueck	ProSiebenSat1 Media
RWE	SAP	Siemens
thyssenkrupp	Volkswagen vz	Vonovia

Tabelle 1: Gesamtliste der deutschen DAX30, Quelle: finanzen.net<sup>9</sup>

Die wirtschaftliche Kraft ist immens: Der Gesamtumsatz aller DAX30 Konzerne lag im Jahr 2016 bei etwa 1,325 Billionen Euro<sup>10</sup> und der operative Gewinn betrug zusammengenommen rund 114,2 Mrd. Euro<sup>11</sup>. Die gesamte DAX-Marktkapitalisierung beträgt zum heutigen Zeitpunkt etwa 1.174.518 Mio. Euro<sup>12</sup>.

Ausschlaggebend für die Auswahl der zu befragenden Konzerne war in erster Linie die Bereitschaft einer Teilnahme. Für eine stichhaltige Datenbasis und die realistische Abbildung der Meinung zu den erfragten Themenkomplexen, wurde der Umfang der Befragung auf 12 der 30 möglichen Unternehmen festgelegt, also rund 40%. Der Hauptgrund hierfür war die Verfügbarkeit der relevanten Personen: Ein höherer Wert war wünschenswert, aber aufgrund der Erreichbarkeit der Ansprechpartner und des Zeitplans dieser Arbeit schwierig umsetzbar.

### Zielgruppe und ihre Rollen im Unternehmen

Aus personeller Sicht fokussierte die Befragung den *Chief Information Officer* (CIO) und/oder den *Chief Information Security Officer* (CISO) der jeweiligen DAX30 Unternehmen. Hatte das Unternehmen keinen Ansprechpartner mit dieser expliziten Funktion oder mangelte es an der Verfügbarkeit, so war der gewünschte Gesprächspartner immer eine für die Konzernsicherheit verantwortliche Person.

#### CIO - Chief Information Officer

Die Rolle des CIOs besteht in der Regel darin, die gesamte IT innerhalb eines Unternehmens zu verantworten. Dabei übernimmt er neben der strategischen auch die operative Führungsrolle und hat damit weitreichende Gestaltungsmöglichkeiten und Befugnisse. Der CIO berichtet i.d.R. unmittelbar an den CEO. Die CIOs der großen und mittelständischen Unternehmen sind heute bestens untereinander vernetzt und verfügen über verschiedene Plattformen für den Austausch untereinander und nach außen.

#### CISO - Chief Information Security Officer

Der CISO eines Unternehmens ist im Prinzip der Beauftragte für die Informationssicherheit eines Unternehmens bzw. eines bestimmten Bereiches – dies bedeutet, es kann auch mehrere Personen in dieser Rolle geben. Oft hat dieser einen IT-sicherheitsbezogenen Hintergrund. Zudem verfügt er

<sup>9</sup> finanzen.net: Auflistung aller DAX 30 Werte mit aktuellen Kursen, URL: <http://www.finanzen.net/index/DAX/30-Werte>, Stand: 03.01.2017, Zuletzt abgerufen: 03.01.2017

<sup>10</sup> Angabe ohne Banken: Banken sind in Kernbereichen ihres Geschäftes von der Umsatzsteuer befreit. Grund ist, dass Banken im Kredit- und Einlagengeschäft keinen Umsatz haben, sondern eine Marge erwirtschaften, die dem Unterschied zwischen Soll- und Haben-Zinsen entspricht. Diese Bruttomarge ist aber weder Umsatz noch Gewinn. Sie dient der Deckung der Risikokosten (z.B. Kreditausfall) sowie der Verwaltungskosten (Personal- und Sachkosten) der Bank und ist Quelle ihres Gewinns. (Quelle: Statista)

<sup>11</sup> Wirtschafts Woche: Dax-Konzerne erreichen neue Rekordwerte, URL: <http://www.wiwo.de/politik/konjunktur/umsatz-und-gewinn-dax-konzerne-erreichen-neue-rekordwerte/19526948.html>, Stand: 16.03.2017, Zuletzt abgerufen: 20.07.2017

<sup>12</sup> Boerse.de: Marktkapitalisierung Dax-Aktien, URL: <http://www.boerse.de/gewichtung/DAX-Aktien/DE0008469008>, Stand 26.05.2017, Zuletzt abgerufen: 26.05.2017

über tiefgehende Kenntnisse im Bereich der Sicherheit und den dazugehörigen Normen, wie beispielsweise ISO/IEC 27000 und dem BSI Grundschutz. Die Aufgaben sind hier vielfältig und häufig handelt es sich dabei um eine Stabsstelle. Die Besetzung einer CISO Position findet bei immer mehr Unternehmen Anklang, da sich die IT-Sicherheitslage für die deutschen Unternehmen im Augenblick weiter verschärft und der Handlungsbedarf ansteigt.

Die tatsächlichen Aufgaben und Befugnisse eines CISOs variieren von Unternehmen zu Unternehmen sehr stark. Die IT-Sicherheit spielt dabei zwar eine Schlüsselrolle, versteht sich aber stets als Teilmenge aller Themen rund um die Informationssicherheit. Der CISO berichtet meist ebenfalls direkt dem CEO und ist *in der Regel* nicht dem CIO unterstellt. Die Vernetzung der CISO-Community nimmt im Augenblick ebenfalls zu, was sich in der Entstehung von entsprechenden Webseiten und den dazugehörigen News-Ressorts widerspiegelt.

Trotz prinzipieller Bereitschaft zur Teilnahme an der Befragung, musste oft mangels verfügbarer Zeit seitens der Entscheider die gestellte Anfrage für ein angefragtes Fragegespräch leider abgelehnt werden.

Die Durchführung der Befragung wurde vorzugsweise in einem persönlichen Gespräch mit dem Verantwortlichen vor Ort durchgeführt. Dies war bis auf eine Ausnahme (Telekom) immer der Fall. Als Alternative zu einem persönlichen Treffen wurde ein Telefonat oder WebEx-Meeting angeboten.

### Teilnehmer der Befragung

Die Großanwender, die einer Teilnahme zugestimmt haben und befragt werden konnten, sind nachfolgend in *Tabelle 2* dargestellt:

Allianz
Bayer
E.ON
Infineon
Lufthansa
Pro7Sat1
RWE
Siemens
thyssenkrupp
T-Systems/Telekom
Volkswagen
Vonovia

Tabelle 2: An der Befragung beteiligte Unternehmen in alphabetischer Reihenfolge

An dieser Stelle gilt der Dank den jeweiligen Verantwortlichen der beteiligten Unternehmen, die sich trotz eines sehr eng getakteten Terminkalenders, die Zeit zur Beantwortung aller Fragen und für eine sehr interessante und konstruktive Diskussion genommen haben.

Weiterhin wurde diese Arbeit inhaltlich auch durch zahlreiche weitere Personen begleitet und unterstützt, welche die Idee einer Zusammenarbeit für wichtig erachtet haben. Auch ihnen gilt der Dank für ihre investierte Zeit. Insgesamt war die Unterstützung durch alle Beteiligten für die Anfertigung dieser Masterarbeit enorm.

### Unterstützer

Unter anderem wurde diese Arbeit aktiv durch den Bundesverband IT-Sicherheit e.V. (TeleTrust)<sup>13</sup> mit seinen 300 aktiven Mitgliedern (Stand: 25.06.2017) und dem Bundesverband der IT-Anwender

<sup>13</sup> Bundesverband IT-Sicherheit e.V. (TeleTrust): Zentrale TeleTrust-Positionen, URL: <https://www.teletrust.de/teletrust-positionen>, Stand: 01.01.2017, Zuletzt abgerufen: 01.01.2017

e.V. – VOICE<sup>14</sup> unterstützt. VOICE repräsentiert den Kreis der Anwender, die über ein jährliches Einkaufsvolumen für IT-Produkte von rund. 30 Mrd. Euro verfügen.

Des Weiteren hat auch der ASW Bundesverband, der eine Allianz für Sicherheit in der Wirtschaft<sup>15</sup> darstellt, diese Arbeit unterstützt. Hier haben mehrere themenspezifische Workshops stattgefunden. Neben den Verbänden waren auch weitere Unternehmen, Institutionen und Personen in verschiedenen Rollen unterstützend tätig.

Diese Arbeit erhielt darüber hinaus die Unterstützung der IT-Sicherheitsindustrie. Hierzu wurde beispielsweise bei einer Veranstaltung des Bundesverbands IT-Sicherheit e.V. (TeleTrusT), welches im Juni 2016 in München stattgefunden hat, ein sehr lebhafter und gut besuchter interner Workshop<sup>16</sup> „*Warum setzen große Anwendungsunternehmen nicht mehr deutsche IT-Sicherheitsprodukte ein?*“ mit den anwesenden IT-Sicherheitsanbietern durchgeführt. Dort wurden viele wichtige Aspekte und Ideen aus der Perspektive der IT-Sicherheitsbranche diskutiert, welche für die Gegenperspektive der Großanwender von wichtiger Bedeutung sind.

Für den Vorschlag einer sinnvollen Basis der Zusammenarbeit und Kooperation war es notwendig, beide Perspektiven kennenzulernen. Für die Generierung von verwertbaren Ergebnissen und Indikationen wurden also sowohl die IT-Sicherheitsindustrie, als auch die Anwenderseite direkt auf Entscheider- und Vorstandsebene befragt.

---

<sup>14</sup> VOICE - Bundesverband der IT-Anwender e.V.: Vorstellung der Präsidiumsmitglieder, <http://www.voice-ev.org/praesidium>, Stand: 01.01.2017, Zuletzt abgerufen: 01.01.2017

<sup>15</sup> ASW Bundesverband - Allianz für Sicherheit in der Wirtschaft e.V., URL: <http://asw-bundesverband.de/ueber-uns/>, Stand: 30.09.2016, Zuletzt abgerufen: 30.09.2016

<sup>16</sup> TeleTrusT-interner Workshop 2016, 15./16.06.2016 in München, URL: <https://www.teletrust.de/veranstaltungen/tutorials-workshops/teletrust-iws-2016>, Stand: 16.06.2016, Zuletzt abgerufen: 03.01.2017

## 2 Art und Rollenverteilung einer Zusammenarbeit

Im Hinblick auf eine gemeinsame Zusammenarbeit ist es notwendig, dass die jeweiligen Stakeholder sich in ihrer relevanten Rolle an der Kooperation beteiligen. Diese ist abhängig vom jeweiligen Verantwortungsbereich und Umfeld. Auch die Fragen nach den notwendigen Voraussetzungen und den damit verbundenen Aufgabenstellungen sind für eine erfolgreiche Zusammenarbeit wichtig. Diese Aspekte sollen nachfolgend diskutiert werden.

### 2.1 Aufgaben und Mehrwert für Hersteller

Möchte ein Unternehmen am Markt erfolgreich sein, sind dafür die richtigen Produkte bzw. ein abgestimmtes Portfolio von zentraler Bedeutung. Im Idealfall gibt es ein breites Angebot, das verschiedene Produkte und Dienstleistungen aus einer Hand kombiniert. Es ermöglicht dabei gleichzeitig auch eine sinnvolle Bündelung von Lösungen in Verbindung mit der Möglichkeit der Interoperabilität.

Des Weiteren ist es auch wichtig, dass die Produkte sich in die umgebende Landschaft einfügen können. Der Nutzer ist nicht gewillt seine Umgebung an die IT-Sicherheitsprodukte anpassen zu müssen. Diese Verantwortung liegt, bis auf wenige Ausnahmefälle, stets beim Hersteller.

Die Abgabe eines Qualitätsversprechens sollte nicht nur unter Marketingaspekten geschehen, sondern sich auch in der Wahrnehmung der Anwender widerspiegeln. Dies ist heute in vielen Fällen nicht der Fall und muss zukünftig mit aller konstruktiven Ehrlichkeit berücksichtigt werden.

Das bedeutet letztendlich auch, dass es auf den Anwender und den Markt zugeschnittene Produkte geben muss, bei der die Erwartungshaltung der Nutzer erfüllt wird.

Dies stellt eine solide Basis für den gemeinsamen Dialog dar. Sollte dies gelingen, so ist anzunehmen, dass die stärkere Internationalisierung der deutschen IT-Sicherheitsbranche deutlich einfacher gelingen kann. Dies führt gleichzeitig nicht nur zu mehr Umsatzvolumina und womöglich zu günstigeren Preisen, sondern erhöht auch mit dem steigenden Marktanteil die Marktmacht.

### 2.2 Bedürfnisse und Mehrwert von Anwendern

Der Anwender hat im Hinblick auf seine IT-Sicherheitslandschaft verschiedene Bedürfnisse. In erster Linie sind ihm Qualität, internationale Verfügbarkeit und faire Preise wichtig. Auch das Thema der Backdoors ist ein wichtiges. Die Erwartungshaltung an die IT-Sicherheitsindustrie ist dabei, dass die Hersteller ein tieferes Verständnis für ihr Business entwickeln.

Die Anwender sind sich durchaus bewusst, dass es keine ultimativen und alles könnenden IT-Sicherheitslösungen gibt aber trotzdem ist das aktuelle Angebot noch viel zu weit von diesem Punkt entfernt. Der Markt ist sehr kleinteilig, was die Frage nach einer Konsolidierung aufwirft. Diese könnte für den zukünftig avisierten internationalen Erfolg der IT-Sicherheitsbranche zwingend notwendig sein. Ein Austausch zwischen den Anwendern und den Herstellern wäre notwendig und ist ausdrücklich gewünscht.

Sollte eine Zusammenarbeit gelingen, führt dies durch Adaption besserer und mehr maßgeschneiderter IT-Sicherheitstechnologien zwangsläufig zu einem insgesamt erhöhten IT-Sicherheitsniveau.

Die Anwender verfügen über beachtliche finanzielle Mittel. Das lässt die Frage aufkommen, ob die Großanwender nicht in naher Zukunft das „Warten“ auf die richtigen Produkte aus der IT-Sicherheitsbranche aufgeben und es einfach selbst umsetzen. Ein Anwender allein besitzt bereits zahlreiche Möglichkeiten; was, wenn sich alle 30 DAX Konzerne vereinen? Solch ein erster Versuch ist die Gründung der DCSO.

### 2.3 Aufgaben für Hochschulen und Forschung

Die Hochschullandschaft in Deutschland ist sehr stark und der Bereich der IT-Sicherheitsforschung ebenfalls. Forschungsprojekte erzeugen Innovationen, ermöglichen neue Produkte und generieren

dabei gleichzeitig personelle Kompetenz. Diese fließen in verschiedenen Formen verbessernd wieder zurück in die Lehre aber auch in die Wirtschaft. Dieser Transfer findet auch mit der Begleitung und Unterstützung durch die Industrie statt. Dies ist auch ein wichtiger Schritt bei der Positionierung gegen die sehr starke Forschung und Entwicklung in den USA oder Israel.

Die Forschung kann hier durch Begleitung und Mitarbeit des Prozesses helfen, diesen optimal auszugestalten. Auch entstehende Innovationslücken ließen sich so mit Hilfe der Forschung und Wissenschaft, begleitend zum stattfindenden Dialog und darüber hinaus aufgreifen und beseitigen.

## 2.4 Aufgaben für Verbände

Für eine effektive Kommunikation im Hinblick auf eine Zusammenarbeit bieten sich die Verbände als Medium, Mediator respektive Kommunikationskanal an. Würden die Beteiligten aller Seiten, also Hersteller, Anwender und Hochschulen auf direktem Wege miteinander kommunizieren, wäre das im Hinblick auf Effektivität und Geschwindigkeit problematisch. Verbände ermöglichen es hier vermittelnd eine direkte 1:1 Kommunikation zielgerecht zu kanalisieren und können dabei helfen, die einzelnen Gruppen über definierte Schnittstellen am Gesamtprozess zu beteiligen.

Außerdem kennen die Verbände jeweilige Interessen und Befindlichkeiten der eigenen Mitglieder sehr gut. Dies kann organisatorisch in Form von Arbeitskreisen geschehen. Für die Gründung eines solchen Arbeitskreises haben sich beispielsweise zahlreiche TeleTrust-Mitglieder beim internen Workshop Ende Juni in Essen ausgesprochen. Dieser befindet sich in der Vorbereitungsphase und wird aller Voraussicht nach im Spätsommer bzw. Frühherbst die Arbeit aufnehmen. Weiterhin sollten die gemeinsamen Aktivitäten zusammen mit dem VOICE e.V. und ASW e.V. fortgesetzt werden.

Beim Aufbau von Kompetenzen und dem Erarbeiten innovativer Lösungen ist eine effiziente Arbeitsweise ausschlaggebend.

## 2.5 Verantwortung für Politik, Gesellschaft und der resultierende Mehrwert

Damit die Bedrohungslage nicht die Oberhand gewinnt und unsere Gesellschaft einholt, stehen hier verschiedene Gruppen mit verschiedenen Kompetenzen in der Verantwortung, die diese als solche auch wahrnehmen müssen. Die Politik hat hier z.B. regulatorische und andere unterstützende Maßnahmen als Werkzeuge, welche zur Verbesserung der heutigen Situation genutzt werden sollten.

Die Gesellschaft muss geschlossen begreifen, dass erfolgreich durchgeführte Cyberangriffe am Ende uns allen nachhaltig Schaden zufügen. Eine ausweichende und gleichgültige Einstellung demgegenüber ist der gesamten Gesellschaft gegenüber fahrlässig und darf nicht hingenommen werden. Ein wesentlicher Schritt in diese Richtung ist das IT-Sicherheitsgesetz. Nichts desto trotz besteht nach wie vor großer Handlungsbedarf.

Die heutigen Gesetze berücksichtigen lediglich in Teilen die Entwicklungen der letzten 2 bis 5 Jahre und adressieren erst recht nicht die kommenden 5 bis 10 Jahre, in denen sich völlig neue Technologien, Geschäftsmodelle und gleichzeitig auch Risiken entwickeln und etablieren werden. Die Politik und die Gesellschaft müssen einen Weg finden voran zu gehen, um mindestens am Puls der Zeit zu bleiben, statt wie bisher von der technischen Entwicklung und den Bedrohungen „überholt“ zu werden.

Ein Kernthema dabei ist auch die digitale Souveränität, die jeder einzelne als Person oder Unternehmen für sich beanspruchen muss. Dabei geht auf der einen Seite es zwar primär darum, einen Weg aus der digitalen Abhängigkeit von den jetzigen Marktführern zu finden. Auf der anderen Seite ist die Souveränität über die eigenen Daten, also der Informationen im Kontext der digitalen Selbstbestimmung, einer der wichtigsten Aspekte in unserer Zeit. Diese gilt es als solche wahrzunehmen und auszubauen.

Um diese Probleme zu lösen, ließe sich beispielsweise eine Arbeitsgruppe auf hoher politischer Ebene einrichten, bestehend aus jungen Experten und erfahrenen Unternehmern, denen die aktuellen Technologien und die zukünftigen Entwicklungen mehr als nur ein Begriff sind. Hierbei muss das Thema Sicherheit stark gewichtet werden, damit dieser Herausforderung auf Augenhöhe begegnet werden kann.

Die ersten Schritte zu diesem Thema in Form des Diskussionspapiers „Digitale Souveränität: Debatte über einen besonnenen Umgang mit internationalen Herausforderungen und die Stärkung des Industriestandorts Deutschland“ [2] und „KOMPETENZEN FÜR EINE DIGITALE SOUVERÄNITÄT“ [3], auf denen aufgebaut werden könnte, sind bereits unternommen worden.

### 3 Mögliche Hindernisse und Herausforderungen

Stellt sich die Frage nach einer Kooperation oder Zusammenarbeit, gibt es natürlich auch häufig einzelne Aspekte, die dagegensprechen könnten. Dies könnten etwa diametrale Ansichten oder rechtliche Hindernisse sein. Es gilt also den Umstand nach den möglichen Problemen bei einer Kooperation zu klären.

Da der Sachverhalt aus juristischer Perspektive zu wenig bestimmt ist, um eine konkrete Würdigung einschließen zu können, bedarf es einer generischen Betrachtung. Im Allgemeinen bedeutet dies die Frage nach allgemeinen Hindernissen aus der Anbieter- und der Anwenderperspektive.

Im Hinblick auf den Anwender auf der Erwerbseite, ist die Betrachtung auf den ersten Blick weniger kritisch. Bei den Anbietern könnte es zu Problemen kommen, denn hier spielen das Wettbewerbsrecht bzw. Kartellrecht eine relevante Rolle. Auch eine Monopolbildung gilt es aus Gesetzgebersicht grundsätzlich zu vermeiden. Auch wenn sich große Marktanbieter zusammenschließen, muss dieser frei bleibend sein. Hierbei spielen das Gesetz gegen den unlauteren Wettbewerb (UWG) und andere weitere rechtliche Beschränkungen eine wichtige Rolle.

Eine marktbeherrschende Stellung ist also problematisch, nicht aber eine Kooperation wie dies beispielsweise bei deutschen und französischen Automobilherstellern der Fall ist. Hier bedienen sich mehrere große Hersteller eines gemeinsamen Baukastenprinzips, um aus der Basis gleicher Module verschiedene Autos herzustellen, die den gleichen Markt adressieren. Solch eine Zusammenarbeit kann in Form von Konsortien oder Kooperationen stattfinden, um die Stärken zu addieren. Dies kann unter zeitlicher Begrenzung stattfinden oder nur beschränkt auf einzelne Produkte.

So sind beispielsweise die Roaming Verordnungen auf EU-Ebene kartellrechtlich relevant. Hier existieren horizontale und vertikale Vertriebsverträge. Dies betrifft also ein aufeinander abgestimmtes Verhalten zwischen mehreren Unternehmen und die kartellrechtlichen Vorgaben, Beschränkungen und möglichen Konsequenzen. Vertriebsgebiete dürfen bestimmt werden, wie zum Beispiel die Aufteilung des Marktes unter Anbietern, dabei aber nicht länger als 5 Jahre Gültigkeit behalten.

Die Frage nach einer Kooperation von Anwendern untereinander führt zu dem Schluss, dass Kooperationen und Zusammenarbeit in der Privatwirtschaft grundsätzlich kein Problem darstellen. Im Hinblick auf einen gemeinsamen Einkauf von Produkten und Lösungen könnte dies genutzt werden, um gemeinsam eine stärkere Verhandlungsposition gegenüber den Herstellern einnehmen zu können. Größere Abnahmemengen und Einkaufsvolumina spielen in dem Kontext eine große Rolle.

Im Bereich der öffentlichen Beschaffung ist dies dagegen eher schwierig, da es hier klare Regeln für den Einkauf gibt. Diese müssen zumeist mit Ausschreibungen verbunden sein, was die Mitverhandlungsmöglichkeiten deutlich reduziert. Eine Kooperation zwischen den Anbietern und seinen Kunden ist in diesem Fall jedoch kein Problem. So kann sich beispielsweise die Stadt Berlin grundsätzlich auch privatwirtschaftlich engagieren, wie auch die deutsche Bahn oder Post.

Der Staat unterliegt dabei jedoch anderen Compliance-Vorgaben als rein privatwirtschaftliche Unternehmen. Die Verwaltung hat dem Legalitätsprinzip zu folgen und muss sich in jeder denkbaren Hinsicht rechtskonform verhalten. In der Wirtschaft ist dies ein wenig anders gelagert, denn hier spielt die Zweckdienlichkeit eine Rolle und der Inhalt möglicher geschlossener Vereinbarungen im Kontext der in Deutschland herrschenden Vertragsfreiheit. Auch Universitäten könnten sich in solch einem Vertragsverhältnis bewegen. Wichtig hierbei ist das gesetzte Ziel, der monetäre Aufwand, die notwendigen Ressourcen und das Know-how. Auch der Umgang mit dem entstandenen Wissen muss entsprechend vertraglich geregelt werden.

### Juristische Hindernisse

Im Falle einer breiten Kooperation der IT-Sicherheitsanbieter ist das Kartellrecht ein wichtiges Thema. Im Gegensatz zu den Anwendern, für die so etwas problemlos umsetzbar wäre, ist dies für die Hersteller deutlich schwieriger und der Asymmetrie des Marktes geschuldet. Die Anwender würden hier dem Prinzip der „Sammelbestellung“ folgen. Zwar wäre dies organisatorisch gesehen ein Einkaufskonsortium, jedoch kann ein Vertragsverhältnis die formalen Beziehungen regeln, wie Lizenzrecht bei Weitergabe an die Konsortialteilnehmer und Gewährleistungsabwicklungen.

Grundsätzlich würden Entitäten in Verhandlung treten, mit der Absicht den Markt dominieren zu wollen und anderen damit implizit schaden zu wollen. Zwar kommt es hier auf das Maß und den Umfang an aber prinzipiell wäre dies unzulässig. Dies kann im Einzelfall dazu führen, dass das Konsortium über andere rechtliche Bedingungen verfügt, als wenn jede Entität einzeln einkauft.

### Einkaufsmacht

Die Bündelung der Einkaufsmacht kann in der Anforderung diffus sein. In der betriebswirtschaftlichen Betrachtung bestimmt der Käufer die Nachfrage. Die Ausübung der Einkaufsmacht würde dieses Prinzip verschieben. Die konkrete Steuerung von Aspekten ist so vermutlich eine Herausforderung, denn es stellt sich die Frage nach der praktischen Umsetzung. Es würde nach einer neuen Strategie, ähnlich einer Ausschreibungsplattform oder einem anderen neuen Werkzeug, verlangen. Dies wäre vergleichbar mit der Handwerkerplattform „MyHammer“<sup>17</sup>, bei der Aufträge genau formuliert werden können, auf welche sich dann qualifizierte Anbieter bewerben können. Der Suchende erhält daraufhin kostenlose und unverbindliche Angebote verschiedener Firmen und wählt das Angebot mit dem besten Preis-Leistungs-Verhältnis.

Relevant in diesem Kontext ist auch, dass beispielsweise die Einkaufsmacht der Bundesverwaltung den größten Bedarfsträger darstellt und sich für die Entwicklung nationaler Anbieter mitverantwortlich zeichnet.

Dies hätte zur Folge, dass Anbieter gezwungen wären, ihr Angebot insgesamt anders darzustellen. Auch, was die Supportzeiträume oder bestimmte Qualitätskriterien anbelangt. Um der Ausübung der Einkaufsmacht zu begegnen, könnten die Anbieter dazu übergehen stets Fremdprodukte mit anzubieten. Dieses Verfahren könnte zwar zum gewünschten Ziel führen, allerdings kann dies fachlich und zeitlich gesehen ungünstig sein. Der gesamte Prozess und die Findung aller exakten Anforderungen könnten sehr langwierig sein. Letztendlich wird sich das Unternehmen dann womöglich für die allgemeine Lösung entscheiden, da sie in der Breite eingesetzt wird und entsprechende Risiken minimiert. Dies führt jedoch unweigerlich zum Ausschluss aller Spezialanbieter und wird zum Vermarktungsproblem der hiesigen Anbieter.

### Direkter gemeinsamer Einkauf beim Hersteller: Nein, danke?

Es wäre vermutlich naiv zu glauben, dass sich alle Kunden einfach zusammenschließen, um das Anbieterverhalten zu beeinflussen. Dafür sind die Interessen und Geschäftsmodelle zu unterschiedlich. Weiterhin ist die Informationsgewinnung aus dem Bedarf bestimmter Kunden für spezielle Produkte ein Thema. Die herrschende Nachfrage bedeutet die Aufdeckung des jeweiligen Bedarfs für den Hersteller, was zum Herleiten von Schwachstellen und Problemen führen kann. Selbst mit einem NDA ließe sich nicht sicher vermeiden, dass diese Informationen nach außen gelangen und der Reputation schaden könnten. Bei einem Konsortium relevanter Größe wäre die Geheimhaltung schwierig.

### Nebeneffekte

Die geschilderten Vorhaben hätten vermutlich weitere Nebeneffekte zur Folge. Die ausländischen Firmen würden im Falle einer starken Zusammenarbeit unter Umständen versuchen sich dagegen zu positionieren. Die Mittel könnten harte Mergers & Acquisitions Aktivitäten, das „Reindrücken“ der

<sup>17</sup> „MyHammer - Deutschlands Handwerkerportal Nr.1“: <https://www.my-hammer.de>

eigenen Produkte zu deutlich reduzierten Preisen (Dumping) und Kooperationen verschiedener Art sein.

Diese Probleme gab es in der Vergangenheit bereits in anderen Bereichen. Dies ist kein IT-sicherheitspezifisches Problem. In diesem Kontext sollten die gefundenen Problemlösungen genauer analysiert werden, um eine mögliche Adaption zu überprüfen oder zumindest aus ihnen zu lernen.

### **Think Big**

Letztendlich wäre es sinnvoll nicht in deutschen, sondern in europäischen Dimensionen zu denken. Der Grund dafür ist zum einen die wirtschaftlich deutlich größere Dimension und zum anderen der gleiche Rechtsrahmen, bei dem durch Teil- oder voll Harmonisierung innerhalb der EU die entsprechenden rechtlichen Bedingungen herrschen.

## 4 Ergebnisse der Datenerhebung bei den Großanwendern der DAX30

Es gibt zahlreiche interessante und wichtige Themen rund um das Thema IT-Sicherheit und Kooperation. Aus diesen leiten sich bedeutende Fragen ab, auf die viele IT-Sicherheitsanbieter glauben eine Antwort zu haben, jedoch meist, ohne auch tatsächlich danach gefragt zu haben. Genau dies hatte die Datenerhebung zum Ziel: Die betreffenden Gruppen einmal genauer nach ihren Bedürfnissen und Wünschen im Detail zu befragen.

Für die Datenbasis wurden zuerst thematisch unterschiedlich gegliederte Fragebögen erarbeitet, welche als Grundlage für die persönliche Befragung bzw. ein Fragegespräch genutzt wurden. Die übergeordneten Themenkomplexe waren allgemeine Informationen zum Unternehmen, Fragen zur Beschaffung und Fragen zum Einsatz der beschafften Produkte. Weiterhin Themen rund um Allgemeines in Bezug auf Qualität, Start-Ups, internationale Fähigkeiten von Anbietern, Individuallösungen und Fragen rund um das Thema Open Source. Hier wurden auch Aspekte zur Akzeptanz von IT-Sicherheit, Hochsicherheitslösungen und dem bewussten in Kauf nehmen von Restrisiken beleuchtet. Im letzten Drittel wurden Themen der Marktsituation und Defizite, der Zusammenarbeit und der Einkaufsmacht adressiert. Am Ende wurden Fragen zur Sympathie gegenüber einer Auswahl der am Markt aktiven Anbietern gestellt und um ein finales Statement gebeten. Alles stets im Kontext der IT-Sicherheit und der IT-Sicherheitsbranche.

Die so erfassten Antworten auf die einzelnen Fragen der oben genannten Themenkomplexe wurden schließlich für eine Auswertung genutzt, deren Ergebnisse in den nachfolgenden Unterkapiteln dargestellt und diskutiert werden.

Am Ende einiger Unterkapitel werden an den entsprechenden Stellen Implikationen in Form einer zusammengefassten Empfehlung oder Schlussbetrachtung der jeweiligen Teilergebnisse hergeleitet.

### 4.1 Allgemeine Informationen

Für einen ersten Einstieg ins Gespräch wurden erst einmal grundsätzliche Themen angesprochen. Aus diesem Grund beschäftigen sich dieser Abschnitt und der Beginn des Interviews mit Fragen allgemeiner Natur zum Unternehmen, der IT-Sicherheitsinfrastruktur und den Schwerpunkten im Hinblick auf die IT-Sicherheit. Die reine Anzahl der Mitarbeiter in den verschiedenen Bereichen lässt jedoch nicht auf die Effektivität schließen. Diese Zahlen sollen lediglich einem einfachen Vergleich der jeweils zur Verfügung stehenden Ressourcen dienen.

#### Umsatz p.A. in Mrd. Euro

Der Umsatz ist in der nachfolgenden *Tabelle 3* dargestellt. Im vergangenen Geschäftsjahr aller an der Umfrage beteiligten Konzerne lag dieser im Mittel bei etwa 59,15 Mrd. EUR, der kleinste war dabei Pro7Sat1 mit 3,8 Mrd. Euro und mit Abstand der größte Volkswagen mit 217,3 Mrd. EUR Umsatz im vergangenen Jahr.

Konzern	Umsatz in Mrd. EUR	Konzern	Umsatz in Mrd. EUR
Allianz	122,4	RWE	45,8
Bayer	46,8	Siemens	79,6
E.ON	38,2	thyssenkrupp	39,2
Infineon	6,5	T-Systems/Telekom	73,1
Lufthansa	31,6	Volkswagen	217,3
Pro7Sat1	3,8	Vonovia	5,5

Tabelle 3: An der Umfrage beteiligte Unternehmen in alphabetischer Reihenfolge und der jeweilige Umsatz in Mrd. EUR; Quelle: Statista

Die Zahlen verdeutlichen die Dimensionen, in denen sich die Konzerne in ihrer Denk- und Handlungsweise bewegen. Aber auch die Höhe von möglichen zu kalkulierenden Risiken und Schäden haben eine ganz andere Größenordnung, als es beispielsweise bei kleinen und mittleren Betrieben der Fall ist. Wenn ein DAX Konzern im Falle einer Schadenshöhe von 1 Mio. EUR Maßnahmen und Risiken abwägen muss, ist die Auswirkung eine ganz andere im Verhältnis zu einem Umsatz von z.B. 70 Mrd. EUR, als bei einem KMU mit 20 Mio. EUR.

### Anzahl MitarbeiterInnen im Konzern

Insgesamt beschäftigen die befragten Konzerne etwa 1.892.593 MitarbeiterInnen. Die Aufteilung auf die einzelnen Unternehmen wurde in der nachfolgenden *Tabelle 4* gegenübergestellt. Im Durchschnitt sind das 157.716 Arbeitnehmer pro Konzern, wobei der kleinste Arbeitgeber unter den Befragten Pro7Sat1 mit ca. 5.500 Mitarbeitern ist und Volkswagen mit 619.346 Arbeitnehmern mit Abstand der größte.

Konzern	Mitarbeiter gesamt	Konzern	Mitarbeiter gesamt
Allianz	142.500	RWE	66.000
Bayer	117.000	Siemens	365.000
E.ON	35.000	thyssenkrupp	154.906
Infineon	40.000	T-Systems/Telekom	218.341
Lufthansa	121.000	Volkswagen	619.346
Pro7Sat1	5.500	Vonovia	8.000

Tabelle 4: Anzahl der Mitarbeiter im jeweiligen an der Umfrage beteiligten DAX Konzern in alphabetischer Reihenfolge; Quelle: Fincancial Reports/Befragte

### Anzahl MitarbeiterInnen im Bereich der IT und der IT-Sicherheit

Der Durchschnitt aller in der IT tätigen MitarbeiterInnen liegt bei 3.538 über alle Teilnehmer hinweg. Die kleinste Anzahl der IT-MitarbeiterInnen in einem DAX lag bei 120. Die höchste Anzahl an IT-Spezialisten belief sich auf 11.000.

Wird die Ebene unter der IT betrachtet und die Frage nach den Experten im Bereich der IT-Sicherheit gestellt, so reduziert sich diese Zahl erwartungsgemäß, da sie immer integrativ enthalten ist. Im Durchschnitt verfügt jedes DAX Unternehmen über etwa 131 MitarbeiterInnen, die sich dediziert mit IT-Sicherheit beschäftigen. Die Spitzenreiter beschäftigen etwa 350 MitarbeiterInnen im Bereich der IT-Security. Die kleinste Mann-Stärke wurde mit 3 Beschäftigten angegeben. Das Mittel-feld bewegt sich hier im Bereich 60 bis 150 Beschäftigten.

Bei der durchschnittlichen Gegenüberstellung von MitarbeiterInnen in den Konzernen bei der Betrachtung von Gesamtanzahl, IT und IT-Security zeigt sich das unterproportionale Verhältnis, wie die nachfolgende *Abbildung 2: Durchschnittliche Gegenüberstellung MitarbeiterInnen im Konzern: Gesamt vs. IT vs. IT-Security* zeigt.

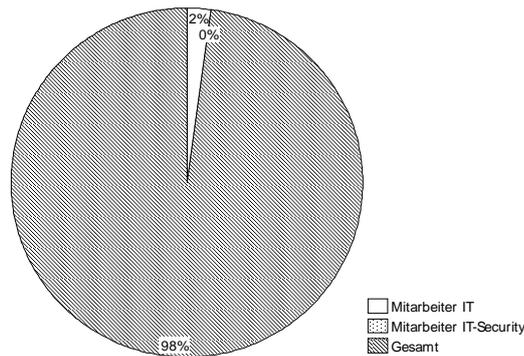


Abbildung 2: Durchschnittliche Gegenüberstellung MitarbeiterInnen im Konzern: Gesamt vs. IT vs. IT-Security

Insgesamt beläuft sich der Anteil der Beschäftigten in der IT bei 2%. Der Anteil der MitarbeiterInnen im Bereich IT-Sicherheit liegt bei 0,1%.

Wird der Durchschnitt aller im IT-Sicherheitsbereich tätigen MitarbeiterInnen auf sämtliche 30 DAX Konzerne hochgerechnet, ergibt dies eine Gesamtzahl von insgesamt ca. 3.930 IT-Sicherheitsexperten.

Unter der Annahme, dass sich in Nordrhein-Westfalen etwa 1.000 Experten in Unternehmen und Wissenschaft mit der IT-Sicherheitsforschung<sup>18</sup> befassen und NRW grob geschätzt mit 17,84 Mio. Menschen ein Viertel der Bevölkerung in Deutschland besitzt, würde dies hochgerechnet schätzungsweise 4.000 IT-Sicherheitsforscher ergeben. Dies ist eine beachtliche Zahl von IT-Sicherheitskompetenz, die den 3.930 Sicherheitsexperten in den 30 DAX Unternehmen gegenüberstehen.

#### 4.1.1 Computer Emergency Response Team (CERT)

Große Konzerne bieten aufgrund ihrer umfangreichen Systemlandschaft entsprechend fulminante Angriffsflächen. Aufgrund hoher Werte und komplexer Infrastruktur ist der Schutzbedarf entsprechend hoch. Neben dem regulären Betrieb einer IT-Security-Abteilung werden ferner sog. CERTs eingesetzt, die *Computer Emergency Response Teams*, also ein „Computersicherheits-, Ereignis- und Reaktionsteam“.

Auch wenn für den Aufbau eines CERT hochqualifizierte personelle Ressourcen notwendig sind, so besitzen tatsächlich alle 12 der befragten DAX Unternehmen ein eigenes CERT. Bei 66% (8) handelt es sich um ein Rund-um-die-Uhr-Betriebsmodell, welches an allen Wochentagen zur Verfügung steht. In allen anderen Fällen stehen die Mitarbeiter zu den normalen Bürozeiten zur Verfügung, mit einzelnen Bereitschaftsarrangements.

#### Betriebsmodelle

Ein Teil der CERTs folgt jedoch auch anderen Betriebsmodellen. So gibt es einen mit 8/5 Betrieb, also 8 Stunden pro Tag an 5 Tagen in der Woche, was den üblichen geregelten Bürozeiten entspricht. Ein anderer wiederum arbeitet in diesem Bereich inhaltlich stark mit Dienstleistern zusammen. So wurde hier unter anderem ein beträchtlicher Teil an IBM ausgelagert.

Weitere DAX setzt ebenfalls auf das gleiche Betriebsmodell, ergänzt dieses jedoch mit einer 24/7 Rufbereitschaft einzelner Personen. Auch haben einige einen globalen Ansatz gewählt und erzeugen die 24/7 Verfügbarkeit durch die Einbindung einiger Experten aus der Zeitzone in Indien. Die

<sup>18</sup> Forschungstag IT-Sicherheit NRW: Die Zukunft in NRW sicher entwickeln,

URL: <http://www.forschungstag-it-sicherheit.de/ForschungITSicherheit2016.pdf>

Stand: 05/2016, Zuletzt abgerufen: 20.07.2017

Verteilung über verschiedene Zeitzonen nach dem „follow the Sun“ Prinzip scheint dafür gut geeignet und immer breitere Anwendung zu finden.

Einige CERTs werden zudem als Global Shared Service betrieben, das allen Standorten unabhängig von Zeitzone und geografischer Lage entsprechende Möglichkeiten bietet.

Die CERTs unterscheiden sich stark in der personellen Stärke. Der kleinste verfügt über 4 Mitarbeiter und der größte verfügt über 70 Personen. Die breite Masse bewegt sich personell im Bereich von 10 bis 22.

Erwähnenswert ist neben den personellen Strukturen auch, dass einige DAX Unternehmen regelmäßig eine Art Katastrophenfall als mehrtätige Übung durchführen, bei dem auch die oberste Führungsebene eingebunden wird. Hierfür gibt es spezielle umfangreich ausgestattete Räumlichkeiten. Simulationen dieser Art binden zwar über die Dauer der Übung wertvolle Ressourcen, sollen aber im Ernstfall die Entscheidungswege und Effizienz auf die Probe stellen, hinterfragen und Verbesserungsmöglichkeiten aufzeigen.

Eine Besonderheit war beispielsweise, dass die CERT-Spezialisten nicht nur nach IT-Sicherheitsvorfällen Ausschau halten und Infrastrukturen beobachten, sondern auch die sich im Ausland befindenden Mitarbeiter begleiten in Form von Monitoring, um in Krisen- oder Gefahrenfällen möglichst schnell reagieren und eingreifen zu können. Dies trägt der sich in den letzten Jahren weltweit stark negativ veränderten öffentlichen Sicherheit Rechnung.

#### 4.1.2 Schwerpunkte bei der IT-Sicherheit

Da das gesamte Feld der IT-Sicherheit unter Umständen sehr breit sein kann und jeder Unternehmensbereich für sich genommen umfangreiche sicherheitsrelevante Aktivitäten erlaubt, wurde dementsprechend die Frage nach den Schwerpunkten gestellt. Damit war beabsichtigt, mehr über die Fokussierung der wertvollen und sehr begrenzten IT-Sicherheits-Ressourcen zu erfahren.

##### Einzelne Schwerpunkte:

<b>Authentication und Encryption</b>	<b>Pentesting &amp; Forensik</b>	<b>CERT</b>	<b>Awareness und Mitarbeitertraining</b>
<b>Schutz von „Golden Nuggets“</b>	<b>Prevention, Monitoring, SIEM</b>	<b>Shopfloor</b>	<b>SCADA-Security</b>
<b>Incident Response/APT Handling</b>	<b>Blue Team/Red Team</b>	<b>Audits/ISO27000</b>	<b>IAM</b>

Tabelle 5: Schwerpunkte der befragten Unternehmen bei der IT-Sicherheit im Einzelnen

##### Übergeordnete Schwerpunkte:

<b>Infrastruktur</b>	<b>Governance</b>	<b>Compliance</b>	<b>Incident Prevention &amp; Management</b>	<b>Awareness</b>
----------------------	-------------------	-------------------	---	------------------

Tabelle 6: Schwerpunkte der befragten Unternehmen bei der IT-Sicherheit als Schwerpunkte

Wie die Darstellungen der vorangehenden Tabellen zeigen, ist die Ausrichtung der Schwerpunkte recht unterschiedlich. Übergeordnet lassen sich jedoch bei näherer Betrachtung oft Gemeinsamkeiten identifizieren.

Die häufigsten Bereiche sind Infrastrukturen, Awareness und Governance bzw. Compliance. Ergänzend ist anzumerken, dass auch die DCSO einer der wichtigen übergeordneten Schwerpunkte ist<sup>19</sup>.

Insbesondere das Thema Awareness bewegte die meisten der befragten Unternehmen sehr stark. Im Verlauf der Gespräche ist entsprechend klar zum Ausdruck gebracht worden, dass in diesem Zusammenhang die vollständige Verantwortung fälschlicherweise oft beim Nutzer allein gesehen wird. Dabei werden ganz stark die Hersteller entsprechender Produkte in der Pflicht bzw. Verant-

<sup>19</sup> Die jeweilige Zuordnung wurde zur Wahrung der Identität des DAX-Unternehmens verallgemeinert.

wortung gesehen, sowohl von allgemeinen Produkten (Stichwort: Security by Design) als auch bei reinen IT-Sicherheitslösungen.

## 4.2 Beschaffung

Um die grundsätzlichen Parameter, die bei der Beschaffung von Technologien relevant sind, gegenüber stellen zu können, wurde auch das Thema der Beschaffung nachfolgend adressiert. Dementsprechend wurden Fragen zu Budgets gestellt. Auch Lizenzierungsmodelle und Kriterien, die eine Rolle spielen, wurden thematisiert.

### 4.2.1 Informationen zu Budgets

Dieser Abschnitt enthält Informationen zu Etats im Bereich der allgemeinen IT und der IT-Sicherheit. Hierbei sollten die zueinanderstehenden Verhältnisse ermittelt und dargestellt werden. Weiterhin wurden die Pro-Kopf-Ausgaben im Bereich der IT und IT-Sicherheit dargestellt.

Die IT-Budgets fallen sehr unterschiedlich aus. Das mit Abstand höchste liegt bei 3,5 Mrd. EUR, gefolgt von 2 Mrd. EUR und 1,4 Mrd. EUR. Die am unteren Ende angesiedelten Budgets belaufen sich auf lediglich 3 Mio. EUR und damit den kleinsten Etat. Das Mittelfeld bewegt sich dabei im Bereich von 40 bis 80 Mio. EUR.

Auch das Budget für die IT-Sicherheit im Unternehmen war ein Thema. Die IT-Sicherheitsbudgets entstammen immer jeweils dem IT-Budget, da sie dort in allen Fällen immer integrativ enthalten sind.

Die höchsten IT-Sicherheitsbudgets betragen 175 Mio. EUR und 145 Mio. EUR. Das niedrigste Budget wurde mit 0,6 Mio. EUR angegeben. Auch hier liegt das Mittelfeld im Bereich von 40 bis 75 Mio. EUR.

Um ein Gefühl für die Höhe zu erhalten, wurde der jeweilige Wert als durchschnittliche pro Kopf Ausgabe berechnet.

Die höchste jährlichen IT pro Kopf Ausgaben liegt bei ca. 24.500 EUR, die niedrigste bei 375 EUR. Das Mittelfeld bewegt sich im Bereich von 1.500 EUR bis 5.000 EUR. Auf den ersten Blick erscheinen einige Ausgaben überproportional, allerdings haben die teilweise hohen Budgets Gründe. Dabei handelt es sich um höhere Investitionen in Unternehmensstrukturen, Digitalisierung und Instandhaltung respektive Investitionsvorbereitungen.

Eine genauere Interpretation dieser ermittelten Zahlen ist nicht trivial, da es sich um unterschiedliche Infrastrukturarchitekturen handelt und die organisatorischen Eigenschaften innerhalb eines Unternehmens hier eine wesentliche Rolle spielen. Auch die Geschäftsmodelle der betrachteten Unternehmen sind zum Teil absolut konträr. Ob eine sehr niedrige pro Kopf Ausgabe auf hohe Effizienz schließen lässt oder einfach zu niedrig ist, lässt sich ohne einen tieferen Blick in die jeweilige Organisation nicht sagen.

Insgesamt wird deutlich, dass Sicherheit am Ende verhältnismäßig einen geringen Teil des IT Budgets ausmacht. Im Mittel sind das insgesamt 6,8%, also etwa 55,2 Mio. EUR. Werden die Mittelwerte der Pro Kopf Ausgaben betrachtet, so liegt dieser Wert im Mittel für IT bei 9.112 EUR und für IT-Sicherheit bei 510 EUR.

### 4.2.2 Lizenzierungsmodelle von IT-Sicherheit

Produkte lassen sich auf verschiedene Weise lizenzieren. Hier gibt es unterschiedliche Modelle und Trends ändern sich mit der Zeit. Nachfolgend wurden daher verschiedene Möglichkeiten der Lizenzierung von Produkten abgefragt. Dabei wurden der *einmalige Kauf von Major Releases*, *As-a-Service-Leistungen* oder *Pay-per-Use* als Wahlmöglichkeiten angeboten. Differenziert wurde dabei zwischen der heutigen Bezugsweise und den zukünftig wünschenswerten Bezahlmodellen.

Wie in der nachfolgenden *Tabelle 7* dargestellt, wurde im ersten Schritt die Frage nach den heute genutzten Lizenzierungsmodellen gestellt, bei der die überwiegende Tendenz insgesamt mit 46% in Richtung einmaligem Kauf beantwortet wurde.

Welches Lizenzierungsmodell <b>nutzen Sie heute?</b>		
Einmaliger Kauf von Major-Releases	●	46%
As-a-Service / laufzeitabhängig bzw. kontinuierlich	◐	31%
"Pay-per-Use"	◑	23%
<i>Summe:</i>		100%

Tabelle 7: Antworten zu der Frage nach den heute genutzten Lizenzierungsmodellen

Interessant war natürlich im zweiten Schritt die Abfrage nach den Wünschen und Präferenzen für die Zukunft. Wie die nachfolgende Darstellung in der *Tabelle 8* zeigt, findet eine deutliche Verschiebung von ehemals 31% zu 42% zugunsten As-a-Service statt. Auch die Option Pay-per-Use wurde hier vereinzelt häufiger genannt und gewinnt dabei 6%. Beides zu Lasten des einmaligen Kaufs von Produkten (-17%).

Welches Lizenzierungsmodell würden Sie gerne <b>in Zukunft nutzen?</b>		
Einmaliger Kauf von Major-Releases	◑	29%
As-a-Service / laufzeitabhängig bzw. kontinuierlich	●	42%
"Pay-per-Use"	◐	29%
<i>Summe:</i>		100%

Tabelle 8: Antworten zu der Frage nach den zukünftig präferierten Lizenzierungsmodellen

Bei der Frage nach dem Lizenzierungsmodell gibt es insgesamt zwar keinen absolut klaren Favoriten, aber eine Tendenz. Ein Teil der Befragten setzt alle genannten Modelle ein und wird dies auch in Zukunft tun, dies jedoch immer jeweils in Abhängigkeit zum Szenario und Situation. Trotzdem geht die breit gewünschte Tendenz in Richtung „as a Service“ bzw. „Pay per Use“ – auch im Hinblick auf die immer stärkere Cloudifizierung der Infrastrukturen und eingesetzten Dienste.

#### 4.2.3 Kriterien und Aspekte zur Beschaffung von IT-Sicherheitsprodukten

Hier wurden Kriterien zur Beschaffung von IT-Sicherheitsprodukten zur Abfrage dargestellt, die nach *wichtig*, *weniger wichtig* und *unwichtig* bewertet werden sollten. Die angebotenen Kriterien in Bezug auf IT-Sicherheit waren *Qualität*, *Preis*, *Nutzerfreundlichkeit*, *Made in Germany*, *Made in Europe*, *Made in „egal“*, *Supportzeitraum*, *Größe des Anbieters*, *Internationaler Support* und *Marktführerschaft*.

Differenziert wurden die Kategorien in drei Stufen: 1. *wichtigste Aspekte*, 2. *weniger wichtige Aspekte*, 3. *Aspekte, die keine Rolle spielen* und wurden in der nachfolgenden *Tabelle 9* gegenübergestellt.

	wichtigster		weniger wichtig		keine Rolle	
Qualität	● 23%		○ 2%		○ 0%	
Preis	◐ 13%		◐ 12%		○ 0%	
Nutzerfreundlichkeit	◐ 9%		◐ 12%		◐ 10%	
Made in Germany	○ 2%		◐ 16%		◐ 14%	
Made in Europe	◐ 4%		◐ 12%		◐ 14%	
Made in "egal"	◐ 6%		◐ 7%		◐ 24%	
Supportzeitraum	◐ 13%		◐ 9%		○ 0%	
Größe des Anbieters	◐ 9%		◐ 7%		◐ 19%	
Internationaler Support	◐ 17%		◐ 7%		○ 5%	
Marktführerschaft	◐ 4%		◐ 16%		◐ 14%	
<i>Summe</i>	<i>100%</i>		<i>100%</i>		<i>100%</i>	

Tabelle 9: Kriterien zur Beschaffung von IT-Sicherheitsprodukten

Keine große Rolle spielen demnach die Herkunft, welche mit 24% für „made in egal“, und jeweils 14% für „made in Europe“ und „Made in Germany“ bewertet wurden. Diese genannten Kriterien wurden auch in der Kategorie „weniger wichtig“ recht stark bewertet. Daraus lässt sich eindeutig ableiten, dass die Herkunft der Produkte eine untergeordnete spielt, was für die deutsche IT-Sicherheitsindustrie als ein wichtiger Hinweis gewertet werden sollte.

Hierzu gesellt sich auch die Kategorie „Marktführerschaft“. Es spielt offenbar nur eine geringe Rolle, ob ein Anbieter mit seinem Produkt der Marktführer ist oder nicht, die anderen Kriterien sind tendenziell deutlich bedeutender. Dies wurde auch in den Gesprächen immer wieder deutlich.

Aus der Kategorie der wichtigsten Aspekte sind mit 23% die Qualität, mit 13% der Preis, mit 13% der Supportzeitraum und mit 17% der internationale Support die wesentlichsten. Insbesondere der internationale Support wurde in den Gesprächen an verschiedenen Stellen immer wieder thematisiert und gehört übergreifend als Querschnittsthema zu den wichtigsten Faktoren.

### Implikationen

- ▶ Wichtigste Kriterien: Qualität, Preis, Supportzeitraum und Internationaler Support
- ▶ Made in Germany spielt keine wesentliche Rolle, Herkunft ist insgesamt vernachlässigbar

#### 4.2.4 Durchschnittliche Lebenszyklen von IT-Systemen

Lebenszyklen von IT-Produkten können aus verschiedenen Perspektiven betrachtet werden. Einerseits lässt sich die Frage stellen, wie lange der Hersteller seine Produkte pflegt und mit Sicherheitsupdates versorgt. Andererseits wie lange der Anwender diese Produkte beabsichtigt operativ zu nutzen. Diese beiden Sichtweisen können durchaus unterschiedlich sein.

In diesem Abschnitt wurden daher die durchschnittlichen Lebenszyklen von IT-Systemen in Jahren abgefragt. Ziel war es zu ermitteln, wie stark Lebenszyklen der genannten Gruppen unter den Großanwendern im direkten Vergleich konvergieren. Berücksichtigt wurden SMDs (Smart Mobile Devices inkl. Tablets), Notebooks, Workstations, Infrastrukturkomponenten im Allgemeinen, Maschinen, Perimeter und VPN-Gateways. Diese werden zwischen 2 und 5 Jahren eingesetzt, ehe sie durch modernere Geräte ersetzt werden.

Insgesamt ähneln sich die Angaben zur Dauer der jeweils eingesetzten Komponenten. Im Hinblick auf Industrie 4.0 sind auch die sehr langen Lebenszyklen der eingesetzten Maschinen von 20 Jahren und mehr, sowie der dazugehörigen Leittechnik interessant. Diese werden im Wandel eine große Rolle spielen auf dem Weg zur gelebten Industrie 4.0 und eine große Herausforderung werden.

Möglicherweise werden hier adaptive Lösungen, welche die alten Maschinen mit neuen kombinieren können, für einen sanften Übergang notwendig sein.

Wird der Bereich der Nutzerendgeräte betrachtet, liegen hier die durchschnittlichen Lebenszyklen bei etwa 3-4 Jahren mit vereinzelt Ausschlägen auf 5 Jahre.

In vielen Fällen wurde klar dargelegt, dass die tatsächliche Nutzungsdauer auch sehr stark von der Updateversorgung durch den Hersteller abhängig ist. Die großen Unternehmen können und wollen sich keinen Einsatz von Produkten innerhalb ihrer Infrastruktur leisten, bei denen der Hersteller keine Unterstützung mehr anbietet.

#### **4.2.5 Angemessene Relationen: Anschaffungspreis IT und Kosten für IT-Sicherheit**

Hier wurde eine mögliche angemessene Relation zwischen dem Anschaffungspreis von IT-Systemen und den Kosten für die dafür benötigte IT-Sicherheit thematisiert. Dabei wurde ein Mapping auf das bereits erwähnte Strategiepapier „IT-Sicherheitsstrategie für Deutschland“<sup>20</sup> des Bundesverbands IT-Sicherheit e.V. durchgeführt, bzw. jenes dort vorgestellte Wirkungsklassenmodell. Dieses Konzept findet sich in einer vollständigen Version des Modells im *Appendix 1: Wirkungsklassenmodell* auf Seite 84 dieser vorliegenden Arbeit.

Die Frage nach einem akzeptablen Aufpreis in Relation zum Anschaffungspreis des betroffenen IT-Systems für höherwertige IT-Sicherheit konnte mit 0% (*Sicherheit ist vollständig enthalten*), 5%, 10%, 20%, 50% und 400% beantwortet werden.

Eine Mehrfachauswahl war bei der Fragestellung möglich und durch die Befragten auch ausdrücklich gewünscht, da es Systeme mit sehr unterschiedlichen Schutzbedarfen gibt. Sicherheit ist für die Großanwender ein durchaus leidvolles Thema.

Viele tendierten zwar dazu, über die dokumentierten 20% hinaus, dass Sicherheit eigentlich integrativ dazugehört, es jedoch besonders sensible Bereiche gibt, wo die Abdeckung durch diese vollkommen unrealistisch erscheint. Hochsicherheit ist für alle ein wichtiges Thema, aber hierzu wurden separate Fragen gestellt, die im Kapitel 4.4 *Allgemeines rund um das IT-Sicherheitsangebot* genauer dargestellt werden. Insgesamt lässt sich jedoch vorwegnehmen, dass entsprechend sensible Bereiche mit Hilfe von Hochsicherheitsprodukten als schützenswert erachtet werden. Den Preis die Freiheitsgrade des Nutzers dadurch einzuschränken, nehmen die Entscheider in diesem Fall in Kauf.

---

<sup>20</sup> Bundesverband IT-Sicherheit e.V. (TeleTrust): Strategiepapier „IT-Sicherheitsstrategie für Deutschland“, URL: [https://www.teletrust.de/fileadmin/docs/IT-Sicherheitsstrategien/2015-Barchnicki-IT-Sicherheits-Wirkungsklassen\\_09-03-2015.pdf](https://www.teletrust.de/fileadmin/docs/IT-Sicherheitsstrategien/2015-Barchnicki-IT-Sicherheits-Wirkungsklassen_09-03-2015.pdf), Stand: 09.03.2015, Zuletzt abgerufen: 13.07.2017

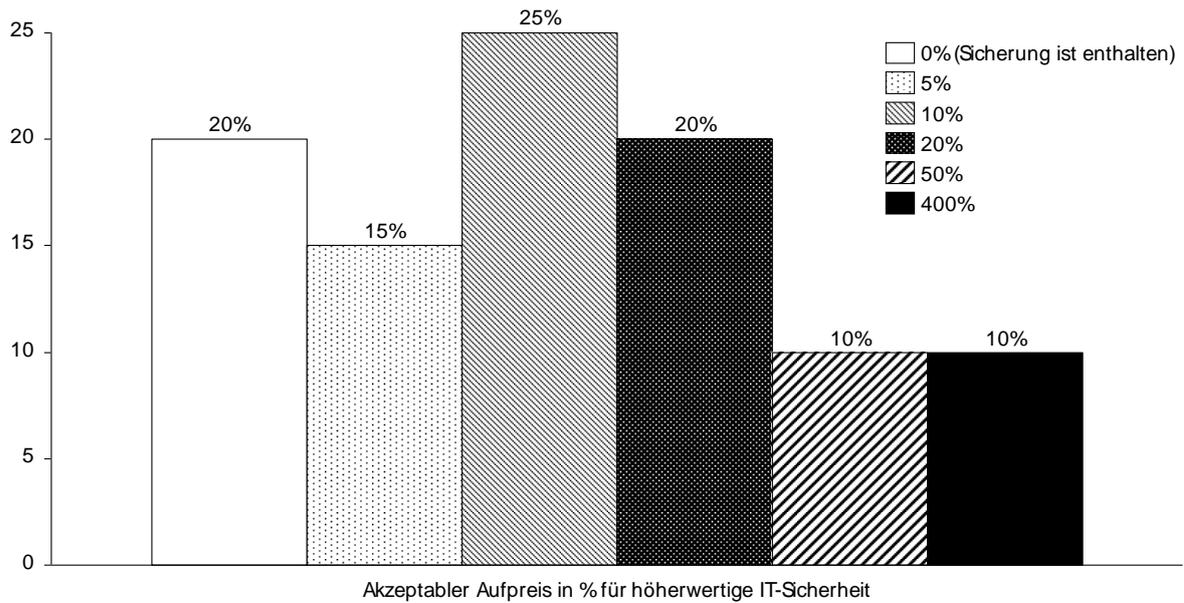


Abbildung 3: Akzeptabler Aufpreis in % für höherwertige IT-Sicherheit

Wie die vorangegangene *Abbildung 3: Akzeptabler Aufpreis in % für höherwertige IT-Sicherheit* darstellt, ergibt sich ein interessantes Bild hinsichtlich der Bereitschaft in höherwertige IT-Sicherheit zu investieren. Werden die Bereiche +10% bis +20% Aufpreis zusammen betrachtet, liegt der Anteil bei insgesamt 45%. Würden die +5% Aufpreis mit in die Betrachtung genommen, so liegt die Bereitschaft sogar bei 60% einen 5- bis 20-prozentigen Aufpreis zu akzeptieren.

#### Unterschiedliche Sichtweisen im Detail

Einige Befragte sehen Security by Design als obligatorisch an. Auch deshalb, weil es im Hinblick auf die eigenen Produkte in der Strategie verankert ist.

Dieser strategische Bezug zur Sicherheit der eigenen Produkte wurde ebenfalls nachgefragt, um herauszufinden, an welchem Punkt diese an Wichtigkeit gewonnen hat. Die Antwort war dabei interessant und ehrlich zugleich: Die Sicherheit ist im Konzern hineingewachsen und war nicht von Beginn an ein entscheidend und bestimmend. Auch wird eine starke Abhängigkeit vom Level des Schutzbedarfs gesehen. Dabei steht die Frage nach der Kritikalität eines Systems im Vordergrund und ist auch stets abhängig vom Business Case – mit dem Fokus auf das Kerngeschäft, oft ohne genaue Vorgaben für die konkrete Umsetzung.

Zudem gehen einige Teilnehmer strikt risikobasiert vor und der Schutz muss den „Juwelen“ entsprechen, ist also vom möglichen Schaden abhängig. Für diesen Zweck wird in manchen Fällen eine abstufende Klassifikation herangezogen, welche zwischen verschiedenen Vertraulichkeitsgraden oder Klassen unterscheidet.

Eine klare einfache Antwort ist in der Realität jedoch schwierig, denn die Erwartung ist klar: Sicherheit ist heute (notwendigerweise) „State of the Art“.

#### Implikationen

- ▶ Ein Teil der Unternehmen erwartet, dass die Sicherheit integriert ist
- ▶ Es ist durchaus der Wille vorhanden, deutlich mehr Geld für Sicherheit auszugeben

#### 4.2.6 Beurteilung der Idee des TeleTrust-Wirkungsklassenmodells

Basierend auf der vorangegangenen Frage zur angemessenen Relation und dem Wirkungsklassenmodell, wurde nach Bewertung der generellen Idee dieses Modells gefragt. Im Detail ging es darum, wie realistisch das Modell beurteilt wird und wie sinnvoll der breite Einsatz dieses Modells in Zu-

kunft wäre. Die möglichen Antworten dabei waren, dass es *eine gute Idee* ist, lediglich *ein Zukunftsmodell*, es *bereits so in der Form umgesetzt* wird oder es *kurzfristig nicht relevant* ist.

Insgesamt bewerteten alle Befragten die Idee eines solchen Modells als gut, aus diesem Grund ist in der nachfolgenden *Abbildung 4* jene Kategorie entsprechend mit 12 Stimmen dokumentiert. Von diesen 12 haben zudem 3 Beteiligte angegeben, dass dies bereits sogar so oder in ähnlicher Form umgesetzt wird.

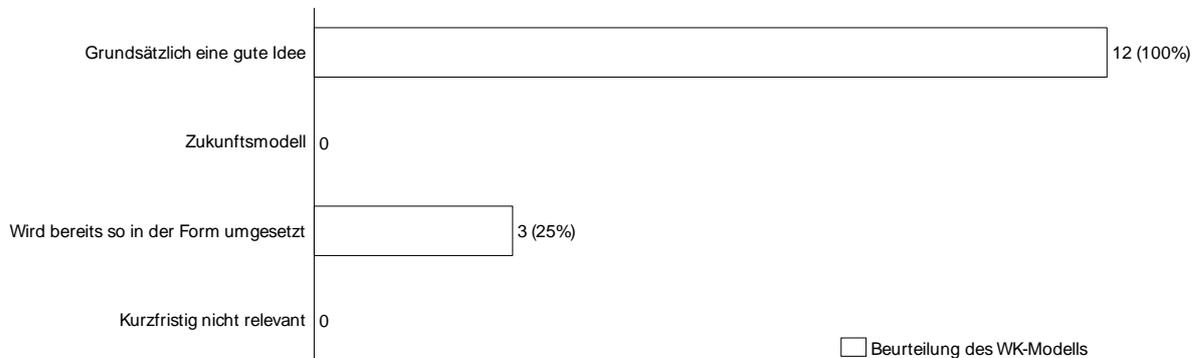


Abbildung 4: Beurteilung des TeleTrust-Wirkungsklassenmodells durch die befragten Entscheider

So wurde angegeben, ein ähnliches Modell bereits intern einzusetzen, welches sich jedoch mit seinen drei Stufen in der Aufteilung ein wenig vom Wirkungsklassenmodell unterscheidet.

Trotzdem fanden die Teilnehmer das vorgestellte Modell grundsätzlich gut. Jedoch ist auch klar artikuliert worden, dass so ein Modell in der Breite nur als globaler Standard erfolgreich werden kann. In diesem Fall müsste jedoch die Objektivität entsprechend gewahrt bleiben. Eine Erweiterungsidee um die Möglichkeit der Zertifizierung wurde als weiterführende Option ergänzt.

#### 4.2.7 Relevante Faktoren für Anschaffung von IT-Sicherheitsprodukten

Hier wurden die Faktoren abgefragt, die eine Anschaffung von IT-Sicherheitsprodukten beeinflussen können. Auf der einen Seite wurde nach der präventiven Beschaffung gefragt. Auf der anderen Seite war von Interesse, ob erst auftretende Vorfälle für einen direkten Erwerb von IT-Sicherheit sorgen.

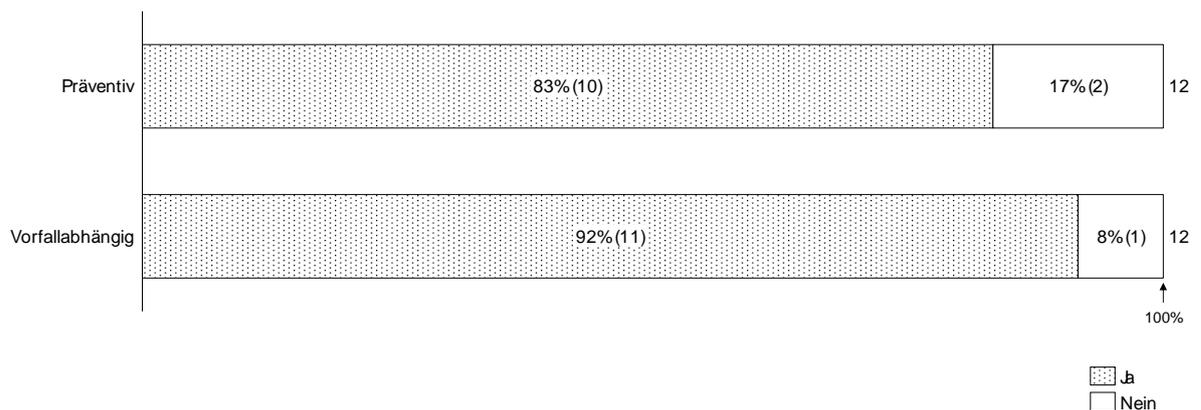


Abbildung 5: Einflüsse auf die Beschaffung von IT-Sicherheitsprodukten

Die Auswertung in *Abbildung 5* zeigt auf, dass 83% (10) der befragten Unternehmen präventiv handeln und 17% (2) hier keinen Anlass sehen, Investitionen im Vorfeld zu tätigen. Im Falle auftretender Vorfälle erwerben dann 92% (11) IT-Sicherheitsprodukte und nur einer (8%) tut dies dann trotzdem nicht. Hier hat in beiden Fragestellungen ein einziges Unternehmen jeweils mit nein geantwortet, mit der Begründung eines internen Risikomodells, welches die Beschaffung maßgeblich beeinflusst.

Insgesamt lässt das Ergebnis den Schluss zu, dass die präventive Beschaffung noch ausbaufähig ist. Des Weiteren ist hier die Risikobereitschaft offenbar durchaus vorhanden, dies hängt in einigen Fällen jedoch mit dem Preis-Leistungsverhältnis zusammen. Zwar spielt für einige Konzerne der Preis wie bereits zuvor dargestellt nur eine untergeordnete Rolle, allerdings übersteigt in der Gesamtbetrachtung irgendwann der gänzliche Aufwand den tatsächlichen Nutzen. Diese Tatsache hat für die IT-Sicherheitsanbieter eine gewichtige Bedeutung, denn das stellt die Frage nach einer möglichen Anpassung der Vertriebsstrategie. Sind die Produkte für den Erwerb und die Absicherung in diesem Kontext zu teuer, müssten die IT-Sicherheitsanbieter prüfen, in wie weit ein preislich reduziertes Angebot möglich wäre.

### Implikationen

- ▶ Die Vertriebsstrategie der IT-Sicherheitsanbieter sollte an die Beschaffungsstrategie angepasst werden
- ▶ Es ist eine Preisanpassung im Kontext der „letzten Meile“ zu prüfen: Kauf von Produkten aufgrund zu hoher Kosten ab einem Punkt nicht mehr attraktiv; Prüfung einer Neuausrichtung des Portfolios unter diesem Aspekt empfehlenswert

#### 4.2.8 Die wichtigsten Kennzahlen im Überblick

Nachfolgend finden sich in der *Anteil des IT-Sicherheitsbudget vom Gesamt-Budget* **0,93 %**

Tabelle 10 die wichtigsten Kennzahlen aus diesem Kapitel zusammengefasst in einer Gesamtübersicht. Die Werte beziehen sich dabei immer auf die jeweils befragten 12 DAX Konzerne.

Kennzahl	Wert
Ø Umsatz p.A.	59,15 Mrd. EUR
Niedrigster Umsatz p.A.	3,8 Mrd. EUR
Höchster Umsatz p.A.	217,3 Mrd. EUR
Ø IT-Budget	991 Mio. EUR
Anteil des IT-Sicherheitsbudget vom IT-Budget	6,8%
Ø IT-Sicherheitsbudget	55,2 Mio. EUR
Ø Mitarbeiter allgemein	157.716
Niedrigste Anzahl Mitarbeiter	5.500
Höchste Anzahl Mitarbeiter	619.346
Ø Mitarbeiter IT	4.079
Ø Mitarbeiter IT-Sicherheit	131
Summe aller Mitarbeiter IT-Sicherheit DAX30 (extrapoliert)	3.930
Niedrigste Anzahl Mitarbeiter IT-Sicherheit	3
Höchste Anzahl Mitarbeiter IT-Sicherheit	350
Ø Mitarbeiter CERT	23
Anteil des IT-Sicherheitsbudget vom Gesamt-Budget	0,93 %

Tabelle 10: Die wichtigsten Kennzahlen im Überblick

### 4.3 Einsatz von IT-Sicherheit

In diesem Kapitel wird der Einsatz von IT-Sicherheit thematisiert. In diesem Kontext wurden unter anderem Fragen zur Einschätzung der Mitbewerber aus der Sicht der jeweils befragten Großanwender gestellt. Auch wurden der Einsatz von Kommunikationslagebildern und die Idee eines „Cyberlagezentrums DAX30“ thematisiert.

#### 4.3.1 Einsatz und Dauer von beschafften IT-Sicherheitsprodukten

Die Lebenszyklen von IT können sehr verschieden ausfallen. Die Pflege solcher Produkte durch die Hersteller in Form von Firmware- und Softwareupdates variiert sehr stark. Es gibt Produkte, die über viele Jahre mit Updates versorgt werden, andere wiederum bleiben im schlimmsten Fall dauerhaft auf dem Stand der Auslieferung.

Nachfolgend wurde also die generelle Einsatzdauer von IT-Sicherheitsprodukten erfragt. Hier wurde ebenfalls thematisiert, ob angeschaffte Produkte rückblickend auch tatsächlich immer zum Einsatz gebracht werden.

Auf die gestellte Frage, ob die angeschafften Produkte am Ende auch immer tatsächlich ihren Weg in den operativen Einsatz finden, wurde in allen 12 Fällen mit Ja geantwortet. Dies zeigt, dass die Entscheider sich ihrer Bedürfnisse bewusst sind und genau wissen, was sie erwerben wollen und was nicht. Auch werden vor der Beauftragung Teststellungen in der eigenen Infrastruktur aufgebaut und getestet. Dies ist heute insbesondere bei komplexeren Produkten üblich und minimiert das Risiko eines Fehlkaufs. Die Frage, wie viele Produkte als Teststellung vor Anschaffung im Test evaluiert und anschließend nicht erworben wurden, ließ sich in diesem Kontext nicht beantworten.

Weiterhin stellte sich die Frage nach der Dauer des Einsatzes dieser beschafften IT-Sicherheitsprodukte. Diese gestalten sich an einigen Stellen sehr unterschiedlich.

So werden in einigen Fällen sehr geringe Zyklen von nur einem Jahr angegeben. Dies funktioniert mit Hilfe eines Baukastensystems, bei dem Komponenten problemlos durch andere ersetzt werden können. In einigen Fällen gab es zudem keine Angabe eines Zeitraums, sondern die herrschende Bedrohungslage ist maßgeblich, also Gefahrenabhängig. Auch die Abhängigkeit im Lifecycle wurde genannt, also solange „State of the Art“.

Darüber hinaus gibt es durchaus auch Intervalle von 7 bis 10 Jahren (sogar bis hin zu 25 Jahren).

Alle sind sich jedoch einig, dass die Produktzyklen aktuell drastisch sinken – bei stetig fallender Lebensdauer.

#### 4.3.2 Blick auf die Mitbewerber in Bezug auf Großanwender untereinander

Hier wurden die Großanwender danach befragt, ob die Aktivitäten der eigenen Mitbewerber eine Rolle spielen und wie diese bewertet wird. Hier wurde diskutiert, ob es relevant ist, welche IT-Sicherheitsprodukte die Mitbewerber einsetzen und wie die eigene Situation zum Vergleich zu den direkten bzw. engsten Mitbewerbern ist. Auch wurde gefragt, wie die eigene Situation im Vergleich zur gesamten Branche eingeschätzt wird. Hier konnte jeweils *weniger gut* und *besser* als diese geantwortet werden.

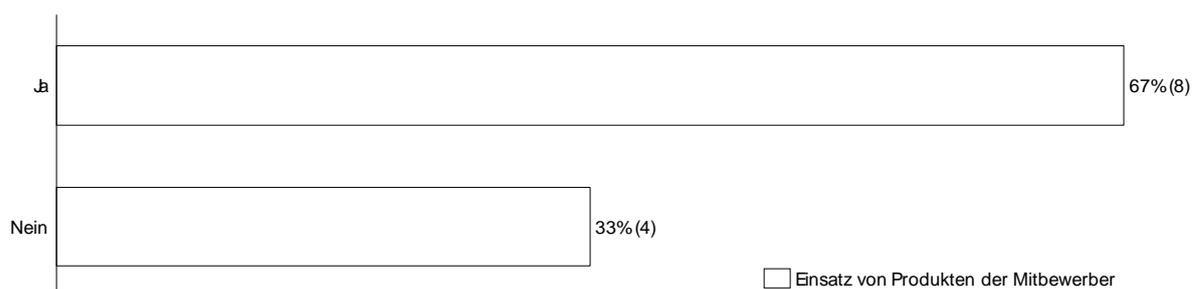
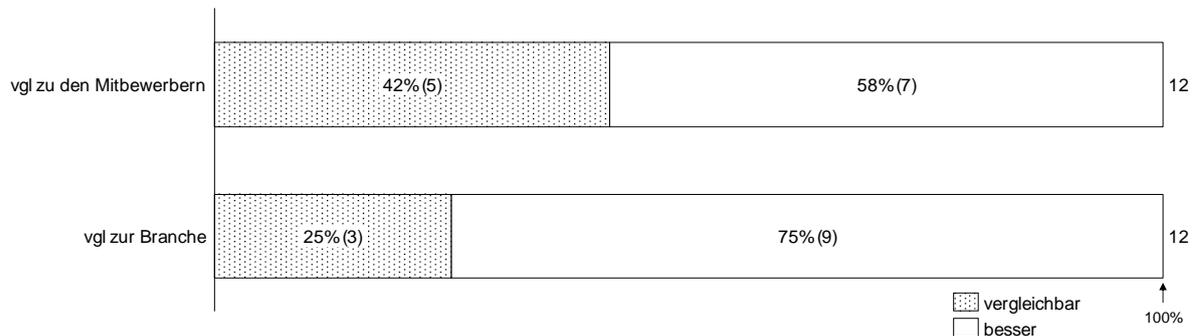


Abbildung 6: Relevanz beim Einsatz von IT-Sicherheitsprodukten durch die Mitbewerber

Wie in *Abbildung 6* dargestellt, spielt der Einsatz von Produkten bei den Mitbewerbern für 67% der Befragten durchaus eine gewichtige Rolle. Etwa ein Drittel der Befragten gibt hier an, dass der Einsatz durch die Mitbewerber keine einflussnehmende Relevanz hat.

Dies spiegelt möglicherweise einen Vertriebsansatz wieder. Da ein größerer Teil der Befragten durchaus die Mitbewerber im Blick hat, kann hier ein erfolgreicher Einstieg in den Großanwendermarkt über eben diese Unternehmen stattfinden.

Des Weiteren wurde bei der Frage nach der Einschätzung der eigenen Situation im direkten Vergleich zu den Mitbewerbern und zur gesamten Branche gefragt, die nachfolgend in *Abbildung 7* dargestellt ist.



**Abbildung 7:** Einschätzung der eigenen Situation direkt zu den Mitbewerbern und zur gesamten Branche

Bei der Betrachtung der Ergebnisse wird deutlich, dass die Selbsteinschätzung durchweg sehr unpräzise ausfällt. Niemand hat hier eine klare Führung gegenüber anderen Mitbewerbern signalisiert, sondern Bescheidenheit an den Tag gelegt, wohlwissend über die Komplexität der Produkte und Situation im Kontext der Digitalisierung.

Insgesamt schätzen sich 58% besser als ihre Mitbewerber ein und 42% vergleichbar. Wird der Vergleich zur gesamten Branche gezogen, so steigt hier die eigene Einschätzung deutlich auf 75% und die Vergleichbarkeit sinkt entsprechend auf 25%.

Dies könnte mit den Größenverhältnissen der jeweiligen Unternehmen plausibilisiert werden. Ein globaler Konzern hat hier eine andere Ausgangsposition als ein Unternehmen, welches ähnliche Märkte adressiert, jedoch deutlich kleiner und unter Umständen nur regional tätig ist.

### Implikationen

- ▶ Erfolg des Vertriebs von Sicherheitsprodukten lässt sich unter Umständen mit Hilfe der Angabe von Referenzen anderer Großanwendern steigern
- ▶ Darstellung, dass die woanders eingesetzten Sicherheitsprodukte die Branche und Mitbewerber besser schützen, ist eine mögliche Strategie

#### 4.3.3 Einsatz und Erfahrungen mit Kommunikationslagebildern

In diesem Abschnitt wurde nach dem Einsatz von Kommunikationslagebildern<sup>21</sup> gefragt. Alternativ sind hier auch die moderneren Begriffe, wie „Advanced Security Analytics Plattform“ respektive „Sicherheitsanalyseplattform“ als Synonyme zu verwenden und finden immer häufiger Verwendung.

Zum einen war von Interesse, ob diese neue Art der Sicherheitstechnologien sich bereits im Einsatz befindet und zu bewerten, ob *gute* oder *weniger gute* Erfahrungen mit dem bisher eingesetzten Produkt gemacht worden sind.

<sup>21</sup> Institut für Internet-Sicherheit – if(is), Prof. Dr. Norbert Pohlmann: Ein Kommunikationslagebild für mehr IT-Sicherheit,

URL: <https://norbert-pohlmann.com/app/uploads/2015/08/292-Ein-Kommunikationslagebild-für-mehr-IT-Sicherheit-Prof-Norbert-Pohlmann.pdf>

Stand: 23.11.2015, Zuletzt abgerufen: 13.07.2017

So setzen wie in *Abbildung 8* dargestellt 83% der Befragten bereits Kommunikationslagebilder ein und 17% bisher noch nicht.

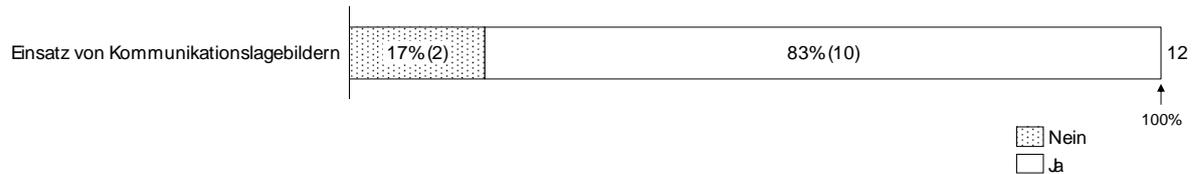


Abbildung 8: Übersicht über den Einsatz von Kommunikationslagebildern

Die Frage nach den damit gemachten Erfahrungen wurde durch die Einsetzenden zum größten Teil mit gut bewertet. Lediglich 18% sind mit der Technologie in ihrer eingesetzten Form unzufrieden.



Abbildung 9: Übersicht über gemachte Erfahrungen mit Kommunikationslagebildern; (11 Teilnehmer, einer unkommentiert)

Hier ist der Markt aktuell jedoch in starker Bewegung und bei den befragten Unternehmen kommen nicht immer die Produkte der nächsten Generation zum Einsatz. Aufgrund der grundsätzlichen Zufriedenheit bleibt dies auch in Zukunft ein interessanter, wenn auch zunehmend immer stärker umkämpfter Markt.

#### 4.3.4 Fiktive Idee eines „CYBERLAGEZENTRUM aller DAX30“

Hier wurde angenommen, es gäbe die Möglichkeit sich an ein gemeinsames „Cyberlagezentrum aller DAX30“ Unternehmen anzuschließen, um gegenseitig von Informationen zu profitieren aber dafür auch entsprechend Kommunikationslagebildinformationen liefern zu müssen. Dies könnte basierend auf einer modernen *Advanced Security Analytics Platform* geschehen. Weiterhin wurde nach der Begründung bzw. der eigenen Motivation für die gegebene Antwort gefragt.

Wie in der nachfolgenden *Abbildung 10* dargestellt, ist die Bereitschaft einer Beteiligung an einem gemeinsamen Lagezentrum groß. Grundsätzlich befürworten das 10 der 12 befragten Unternehmen, was 83% ausmacht. Lediglich zwei Konzerne haben hier so starke Vorbehalte, dass sie eine Beteiligung zum jetzigen Zeitpunkt ablehnen.

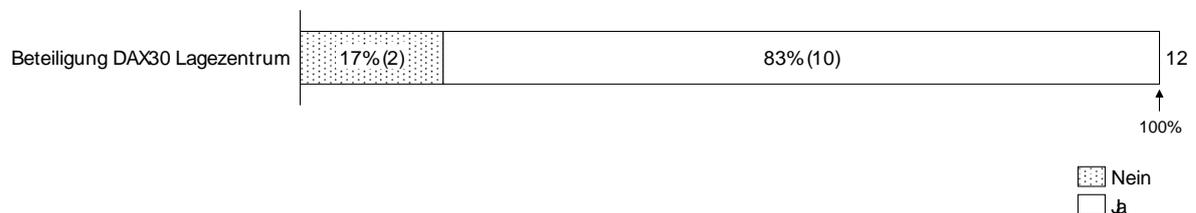


Abbildung 10: Bereitschaft einer Beteiligung an einem gemeinsamen Lagezentrum

Auf beiden Seiten gibt es für die jeweiligen Positionen gute Gründe. Bei den Vorteilen wurden verschiedene Aspekte genannt, die nachfolgend einmal genauer dargestellt werden.

Die Hauptargumente für eine Teilnahme waren die Möglichkeit des gegenseitigen Lernens und des Entstehens von Schwarmwissen, welches zu höherem Know-how aller Beteiligten führt und die Erkennungsrate deutlich verbessert. Je Unternehmen gerechnet, wäre diese Einrichtung signifikant

billiger durch das Teilen der gleichen Ressourcen und es entstünden gleichzeitig Top-Know-how-Pools.

Es wurde auch deutlich die Ansicht vertreten, dass alle CERTs gemeinsam deutlich mehr erkennen können, als einer alleine und da sich die Angreifer ebenfalls vernetzen, wäre dies eigentlich ein notwendiger und essentieller Schritt. Unterm Strich führt dies also zur Bündelung von Kräften, Technologien und Ressourcen. Genau dies waren die Grundgedanken bei der Gründung der DCSO im September 2015, der Deutschen Cyber-Sicherheitsorganisation (*Abbildung 11*) mit Sitz in Berlin, zu deren Initialgründern Allianz, BASF, Bayer und Volkswagen gehören.



Abbildung 11: DCSO Logo; Quelle: DCSO

Weiterhin gibt es die Cyber Security Sharing & Analytics (CSSA, *Abbildung 12*), einen von sieben deutschen Großunternehmen im November 2014 gegründeten Verein.



Abbildung 12: Mitglieder der CSSA; Quelle: CSSA

Die Hauptmotivation dabei ist eine enge Zusammenarbeit im Bereich der Cybersicherheit. Inhaltlich werden Vorfälle ausgetauscht und gemeinsam analysiert. Die Bündelung gemeinsamer Kräfte für schnellere Erkennung und bessere Abwehr werden als Hauptgründe angeführt.

Es existieren aber auch Beweggründe, die unter Umständen gegen einen Zusammenschluss sprechen. Es gibt Großanwender, die schlicht der Meinung sind, dass die Teilnahme „nichts bringt“. Die Argumente dafür sind zum einen die fehlende technische Tiefe solch eines gemeinsamen Vorhabens und zum anderen auch die Erfahrung, dass Angreifer sehr branchenspezifisch vorgehen. Begründet wurde die ablehnende Haltung im Detail durch eine am Markt vollkommen diametrale bzw. entgegengesetzter Positionierungen zueinander, wodurch es an Vergleichbarkeit fehlt.

Auch die Kosten und die notwendigen Ressourcen wären insbesondere Anfangs zu hoch, was die eigene Position in dieser Zeit schwächen könnte. Nicht jedes Unternehmen verfügt über die nötigen Ressourcen oder wäre bereit diese aufzubauen respektive freizugeben.

Da die Angriffsvektoren immer öfter auch über externe Dienstleister führen, ist dies ebenfalls ein Problem. Hier ist die Erkennung kontaminierter Lieferantenketten ein wichtiges Thema, ist in der Realität jedoch eine Herausforderung für alle relevanten Branchen.

Eine der größten Hürden bei einem Zusammenschluss jeglicher Art stellen die Themen der Compliance und die Wahrung eigener Geschäftsinteressen dar, die eine starke ablehnende Haltung erzeugen können. Am Ende muss neben der Wahrung der eigenen geschäftlichen Interessen, der Mehrwert für alle Beteiligten klar erkennbar sein und genau an dieser Stelle zeigte sich breite Skepsis.

#### 4.4 Allgemeines rund um das IT-Sicherheitsangebot

Dieses Kapitel widmet sich vornehmlich den besonderen Kompetenzen der deutschen IT-Sicherheitsindustrie, der Qualitätsbeurteilung, Vertrauen, wichtigen Kriterien von Herstellern, Bedeutung von Start-Ups und dem Einsatz von Start-Up Produkten.

Weiterhin auch Aspekten, die Qualität von Produkten definieren und dem Blick auf wichtige Punkte rund um das Thema der Internationalität. Auch Open Source als wichtiger Faktor in der IT-Landschaft und essenzieller Baustein heutiger Produkte ist ein Thema. Hier wurden verschiedene Fragen zur Nutzung und der Unterstützungsbereitschaft gestellt.

Auch die (nicht erfüllten) Erwartungen und Defizite wurden thematisiert, sowie auch die bewusste Akzeptanz von IT-Sicherheitsgefahren. Am Ende wurde die Bereitschaft abgefragt, einen Schritt weiter zu gehen, den Einsatz von Hochsicherheitslösungen zu bewerten und inhaltlich zu beurteilen.

##### 4.4.1 Besondere Kompetenzen der deutschen IT-Sicherheitsindustrie

Die sehr offene Kryptopolitik in Deutschland gepaart mit der weltweit anerkannten deutschen Ingenieurskunst lässt die Frage aufkommen, ob und in wie fern die IT-Sicherheitsindustrie von diesen Aspekten profitiert.

Hier wurde also die Frage nach den besonderen Kompetenzen der deutschen IT-Sicherheitsindustrie gestellt. Im Kern ging es um die freie Beurteilung als Wahrnehmungsfrage aus der Großanwenderperspektive. Die Antworten konvergieren in Teilen und sind in der nachfolgenden *Tabelle 11* inhaltlich unverändert gegenübergestellt.

Besondere Kompetenzen	Kritikpunkte
<ul style="list-style-type: none"> <li>▪ Eine andere Vertraulichkeit (Informationssicherheit, keine Weitergabe)</li> <li>▪ Verbindlichkeit</li> <li>▪ Kryptografie</li> <li>▪ Digitale Signaturen</li> <li>▪ Kompetenzen im Bereich der Kryptografie (BSI, Fraunhofer)</li> <li>▪ Duktus der klassischen ordentlichen Ingenieurskunst, gleichzeitig ist dies der Nachteil</li> <li>▪ hohe Sicherheit (bei schlechter Usability)</li> <li>▪ Rechtsrahmen, Produkt ist befreit von politischen Dingen (im Kontext von Snowden)</li> <li>▪ sehr harte gesetzliche Lage, nach der sich die Industrie jeweils richten muss</li> <li>▪ Standards, ISO 27000 Zertifizierung</li> <li>▪ Deutscher Datenschutz</li> <li>▪ Vertrauensvorschuss</li> <li>▪ Hardwarelastigkeit</li> <li>▪ Mittelständisch geprägt und einige machen sehr guten Job aufgrund der Spezialisierung</li> <li>▪ Lokale Gesetzgebung und Kultur</li> <li>▪ Deutsche Gründlichkeit/Ehrlichkeit</li> <li>▪ Usability</li> <li>▪ Reporting</li> <li>▪ sehr gute Leute (Assets) aber davon sehr wenige, "schwierig"</li> </ul>	<ul style="list-style-type: none"> <li>▪ Vorbehalte bei der Qualität</li> <li>▪ Industrie zu kleinteilig aufgrund der hohen Fragmentierung und fehlender Integration</li> <li>▪ IT-Anbieter liefern uns benötigte Produkte, Herkunft unbedeutend</li> <li>▪ Keine besonderen, im wesentlichen Kompetenzen, die man braucht; USA &amp; Israel können alles genauso gut</li> <li>▪ Duktus der klassischen ordentlichen Ingenieurskunst, gleichzeitig ist dies der Nachteil</li> </ul>

- Deutsche Tools im Bereich der Forensik
- Historie in der Kryptografie
- sehr gute Leute
- Security Architektur (integrierte Lösungen)
- Hochsicherheitsbereich ist stark

Tabelle 11: Besondere Kompetenzen der deutschen IT-Sicherheitsindustrie

Neben den genannten besonderen Kompetenzen, die zugleich auch die Stärken repräsentieren, gab es jedoch auch erwähnenswerte Vorbehalte. Die gravierendsten wurden ebenfalls für eine Gegenüberstellung in der Tabelle als Defizite aufgenommen. So gibt es durchaus die Auffassung, dass die deutsche IT-Sicherheitsindustrie gegenüber den ausländischen Anbietern eigentlich keine hervorzuhebenden Vorteile bietet. Insbesondere wird den USA und Israel unterstellt, dass sie ein ähnlich gutes Angebot besitzen und über die nötigen Kompetenzen verfügen.

Einige Anwender sondieren die Produkte nach ihrem Bedarf mit Hilfe von Webinaren und Beratern. Dabei legen sie in erster Linie den Fokus auf ihre technischen Bedürfnisse, bei denen die Herkunft keine Rolle spielt. In manchen Fällen kann dies laut den Anwendern auch gar nicht nachvollziehbar unterschieden werden.

Zwar gibt es viele erwähnte Stärken, allerdings sind die in diesem Kontext genannten negativen Punkte als solche umso interessanter. Als Konklusion lässt hier für den Markt durchaus Konsolidierungspotential herleiten. Aber auch die Verbesserung der Usability und das Herausstellen der Vorteile von Produkten aus Deutschland wären mögliche Ansatzpunkte.

### Implikationen

- ▶ Besondere Kompetenzen, auf denen aufgebaut werden sollte: Kryptografie, Signaturen, Hochsicherheit, hervorragende Experten, Vertraulichkeit, Verbindlichkeit
- ▶ Stärkere Kommunikation der deutschen Stärken an die Großanwender
- ▶ Stärkere Kommunikation der durch die Großanwendern konstituierten besonderen Kompetenzen an den Mittelstand
- ▶ Die Kleinteiligkeit der IT-Sicherheitsindustrie ist ein Nachteil und sollte angegangen werden
- ▶ Die Qualitätssicherung der IT-Sicherheitsprodukte muss breit verbessert und nach außen kommuniziert werden (Qualitätskampagne)

#### 4.4.2 Beurteilung von Qualität bei IT-Sicherheit

Dieser Abschnitt wirft die Frage auf, ob der Großanwender der deutschen IT-Sicherheitsindustrie mehr vertraut, als ausländischen IT-Sicherheitsherstellern. Im zweiten Schritt wurde nach einer Begründung für die gegebene Antwort gefragt. Anschließend wurde erörtert, ob das Tragen eines „IT Security made in Germany“-Siegels<sup>22</sup> (ITSMIG) für den Großanwender einen entscheidenden Aspekt für die Bewertung der Vertrauenswürdigkeit darstellt.

Wie die in *Abbildung 13* dargestellten Ergebnisse belegen, ist das generelle Vertrauen in deutsche IT-Sicherheitsprodukte unter den Befragten gespalten. Im Ergebnis vertraut die Hälfte den deutschen Anbietern nicht mehr als ausländischen.

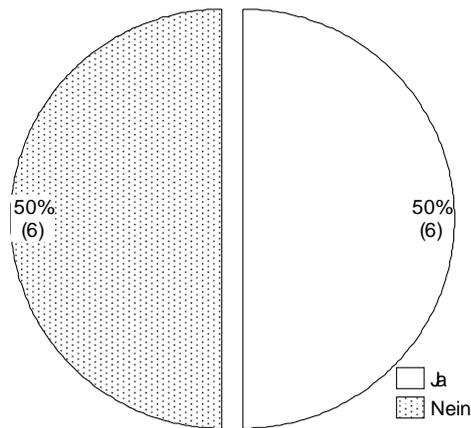


Abbildung 13: Gegenüberstellung des Vertrauens in deutsche IT-Sicherheitsprodukte

Die Gründe für diese sehr ausgeglichene Verteilung der Entscheidungen sind ebenfalls genannt worden und sind in der nachfolgenden *Tabelle 12* im Original gegenübergestellt.

Aufgrund → siehe NSA, Wikileaks, Snowden
Politischer Rahmen
Nichts wo man jemandem anderen mehr vertraut als dem anderen
Produkte mit guter Qualität zum günstigen Preis kommen zum Zuge
Deutsche Produkte kommen von Anbietern, die Nischenprodukte anbieten
Snowden hatte hier keinen Einfluss, die Manipulationen kommen meist nachträglich rein
Unterstellung: Alle Produkte könnten absichtliche Schwächen haben, auch deutsche
Deutsche Hersteller handhaben die Dinge nicht unbedingt anders als ausländische
Härtere Regelung als im Ausland (z.B. Datenhandel)
Geheimhaltungsregularien
Warum sollte man? Nationalität hat jetzt keinen Einfluss
Lücken in der Produktentwicklung
Lokale Gesetzgebung
Hoher Security-Standard gepaart mit hohen Anforderungen
Funktionalität
Qualität
Datensicherheitsgesetzesrahmen ist enger
Gesellschaftliches Verständnis für den Umgang mit Daten

<sup>22</sup> TeleTrust Bundesverband IT-Sicherheit e.V.: IT Security made in Germany Siegel

URL: <https://www.teletrust.de/itsmig/>

Stand: 13.07.2017, Zuletzt abgerufen: 13.07.2017

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Deutsche Gesetzgebung & Geheimdienste stehen sich nicht nahe (wie z.B. in einigen anderen Ländern der Fall)
Aufgrund von Snowden: Gilt nach wie vor und flächendeckend
Patriot Act bzw. Verhalten der USA erzeugt hohe Skepsis
Nicht auf internationaler Infrastruktur anzuwenden
Alles nicht für die Masse geeignet
Gefahr: Das wird im Ernstfall eher versagen
Zertifizierungen und Überprüfungen; wird breit kommen, Welt wird poröser und baut große Dinge auf → Zertifizierung zukünftig als Fundament wichtig
Veröffentlichungen zu Einflussnahme (z.B. auf Huawei und Google)
Angriffe durch russische/chinesische Geheimdienste
Machen keinen Unterschied

Tabelle 12: Darstellung Gründe der Entscheidung für oder gegen die deutsche IT-Sicherheit

Bei der Beurteilung der Vertrauenswürdigkeit auf Basis des IT Security made in Germany Siegels von TeleTrusT verändert sich die Beurteilung leicht zugunsten der deutschen IT-Sicherheitsprodukte. Den wenigsten der befragten Unternehmen war dieses Siegel geläufig und wurde bei dem Gespräch näher dargestellt.

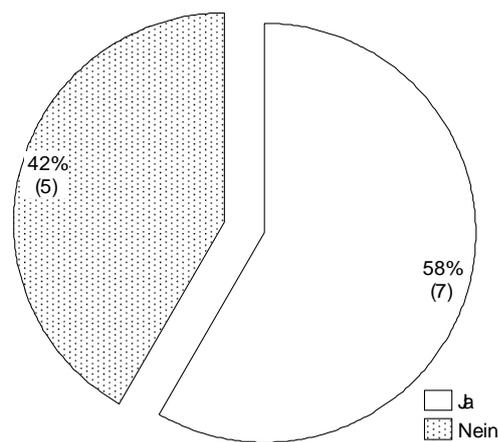


Abbildung 14: Beurteilung der Vertrauenswürdigkeit in Form des IT Security made in Germany Siegels als entscheidender Aspekt

Diese leichte Verschiebung in *Abbildung 14* zugunsten der deutschen Produkte kann als Möglichkeit interpretiert werden, mit Hilfe von Kommunikation und der Hervorhebung solch eines Siegels die Akzeptanz weiter zu erhöhen. Hier scheint durchaus eine Empfänglichkeit vorzuliegen.

#### Implikationen

- ▶ Gemeinsame Werbekampagne der großen deutschen Hersteller für die Adressierung der 50%, die deutschen Produkte mehr vertrauen als ausländischen
- ▶ Kommunikationsstrategie für gute Gründe eines Einsatzes deutscher Produkte, um die anderen 50% zu adressieren
- ▶ IT Security made in Germany Siegel zeigt, dass es anerkannt wird, wenn es verstanden wurde, aus diesem Grund muss über eine breite und größere Werbekampagne nachgedacht werden

#### 4.4.3 Beurteilung relevanter Kriterien von IT-Sicherheitsherstellern

Hier wurde gefragt, welche Kriterien eines IT-Sicherheitsherstellers für wie wichtig bewertet werden. Zur Wahl standen dabei der persönliche Kontakt, Onlineangebot bzw. Onlinevertrieb, eine exzellente Webseite, der Auftritt in sozialen Medien, ein aktiver Blog über aktuellen Fragestellungen, Mehr-

sprachigkeit, Möglichkeiten der Zusammenkunft mit anderen Anwendern und Schulungsangeboten. Beurteilt werden konnte dies mit den Attributen *sehr wichtig*, *wichtig*, *weniger wichtig* und *unwichtig*.

Die dargestellten Ergebnisse in *Tabelle 13* zeigen in verschiedenen Bereichen wichtige Faktoren, die aus Sicht der IT-Sicherheitsindustrie eine wichtige Rolle spielen.

	sehr wichtig	wichtig	weniger wichtig	unwichtig
Persönlicher Kontakt	39%	5%	17%	0%
Onlinevertrieb/Angebot	0%	3%	22%	30%
Eine exzellente Webseite	0%	8%	22%	22%
Auftritt in sozialen Medien	0%	3%	11%	39%
Aktiver Blog über aktuelle Fragestellungen	6%	16%	17%	9%
Mehrsprachigkeit	22%	22%	0%	0%
Möglichkeiten der Zusammenkunft mit anderen Anwendern	17%	19%	11%	0%
Schulungsangebote	17%	24%	0%	0%
Summe	100%	100%	100%	100%

Tabelle 13: Zusammengefasste Beurteilung und Gewichtung relevanter Kriterien von IT-Sicherheitsherstellern

So ist den befragten Anwendern der persönliche Kontakt zu den entsprechenden IT-Sicherheitsanbietern am wichtigsten. Hier sind insbesondere positive Präsenz und das Wirken des Vertriebs gemeint. Im Bereich sehr wichtig sind insbesondere die Mehrsprachigkeit, die Möglichkeit der Zusammenkunft mit anderen Anwendern und Schulungsangebote hervorzuheben.

Als wichtig hingegen empfinden die Anwender einen aktiven und gut gepflegten Blog, die Mehrsprachigkeit der angebotenen IT-Sicherheitsprodukte, die Möglichkeit der Zusammenkunft mit anderen Anwendern und Schulungsangebote.

Auch eine ordentliche Referenzliste mit vergleichbaren Referenzen wurde als wichtig angeführt. In diesem Kontext wurde auch klar kommuniziert, dass der DAX insgesamt die kleineren Unternehmen deutlich stärker in die Pflicht nehmen wird. Dieses Vorhaben betrifft auch implizit die Anbieter von IT-Sicherheitslösungen.

Weniger wichtig sind insbesondere der Onlinevertrieb und eine exzellente Webseite, es gab jedoch auch Hinweise, dass diese sehr informativ gestaltet sein sollte.

Als grundlegend unwichtig ist der Onlinevertrieb, eine exzellente Webseite und der Auftritt in sozialen Medien, der heute aus Unternehmersicht oft als State of the Art empfunden wird, bewertet worden. Doch insgesamt schwankt hier die Bandbreite zwischen wichtig und unwichtig.

### Implikationen

- ▶ Der persönliche Kontakt sollte in Zukunft stärker ausgebaut werden in Verbindung mit einem markanten und professionellen Auftritt des Vertriebs
- ▶ Der Vertrieb sollte in diesem Bereich gesondert geschult werden, um den Anforderungen und Erwartungen der Großanwender gerecht zu werden
- ▶ Der Aufbau eines Blogs mit aktuellen Beiträgen, die am Puls der Zeit liegen, sollte in Betracht gezogen werden; dieser kann einen Mehrwert für die Anwender und den Anbieter gleichermaßen erzeugen
- ▶ Es muss ein Forum geboten werden, welches der Zusammenkunft von Anwendern dient
- ▶ Schulungsangebote sollten breit angeboten werden und sich dynamisch nach den aktuellen Bedürfnissen und Fragen der Anwender richten

#### 4.4.4 Relevanz bei der Größe von Marktanbietern

Diese Frage widmet sich der Empfindung einer Größe von Marktanbietern. Gefragt wurde im Detail, was die notwendige Größe eines Anbieters wäre, gemessen an der Anzahl der dort tätigen Mitarbeiter, bei dem der Verantwortliche ein gutes Gefühl hätte.

30 bis 300+

Diese Frage adressiert die notwendige „kritische Größe“, um bei Erwerbsvorhaben überhaupt generell in eine Auswahl zu kommen. Hierbei spielt die Größe des Anbieters durchaus eine zentrale Rolle, wenn dies auch nicht immer ausschlaggebend ist. Die Bandbreite, bei der die Großanwender „ein gutes Gefühl“ hätten liegt als minimale Anforderung bei ca. 30 bis 300+ Mitarbeitern. Die Größe des Anbieters spielt dann eine untergeordnete Rolle, wenn hinter diesem Start-Up bzw. sehr kleinem Unternehmen eine größere Gesellschaft steht, sei es als übergeordnete Muttergesellschaft oder in Form eines Joint-Venture bzw. Teilhaber. Hier wurden Kontinuität und Beständigkeit als Hauptgrund genannt.

Darüber hinaus gibt es aber auch andere Faktoren, die das in Frage kommen maßgeblich bestimmen. Diese sind beispielsweise in komplexen Einkaufsrichtlinien definiert, die sich untereinander stark unterscheiden.

Vereinzelt wurde jedoch auch artikuliert, dass die Größe unerheblich ist, sofern eine globale Einsatzfähigkeit gegeben ist. Insgesamt wurden mit kleineren Unternehmen jedoch immer wieder negative Erfahrungen gemacht, was auch zu der hier dargestellten Perspektive geführt hat.

#### 4.4.5 Bedeutung von Start-Ups

Oft entstehen Innovationen außerhalb der etablierten Unternehmen. Die Treiber dafür sind heute oft Hochschulen, die in der Lage sind, Ideen voranzutreiben, Innovationen zu generieren und den Transfer in die Wirtschaft zu ermöglichen. Die dort entstandenen Start-Ups sind in der Lage, sich außerhalb komplexer Regularien und Begrenzungen zu bewegen. Die fest etablierten Prozesse in großen Unternehmen sind ihnen egal, da sie in ihrer Größe mit flachen Hierarchien und losen Prozessen vollkommen dynamisch agieren können.

Weitere Treiber sind Venture Capital-Geber, die bereit sind auf der einen Seite die Umsetzung guter Ideen in Prototypen zu unterstützen und die Produktifizierung auf der anderen Seite mit Mitteln und ihren Erfahrungen zu unterstützen.

Hier wurde entsprechend gefragt, welche Bedeutung Start-Ups im Bereich der IT-Sicherheit beigemessen wird und nach der Begründung. Mögliche Einstufungen der Antworten dabei waren *sehr hoch, hoch, weniger hoch* und *gar keine* Bedeutung.

Insgesamt messen die befragten Großanwender den Start-Ups zum größten Teil sehr hohe (58%) bis hohe Bedeutung (17%) zu. Lediglich 25% schätzen diese weniger hoch ein aber kein einziger würde diese ohne Bedeutung bewerten. Die Ergebnisse zeigen, dass Start-Ups in den Augen der Anwender eine große Rolle spielen. Dies wurde auch in den Gesprächen immer wieder klar.

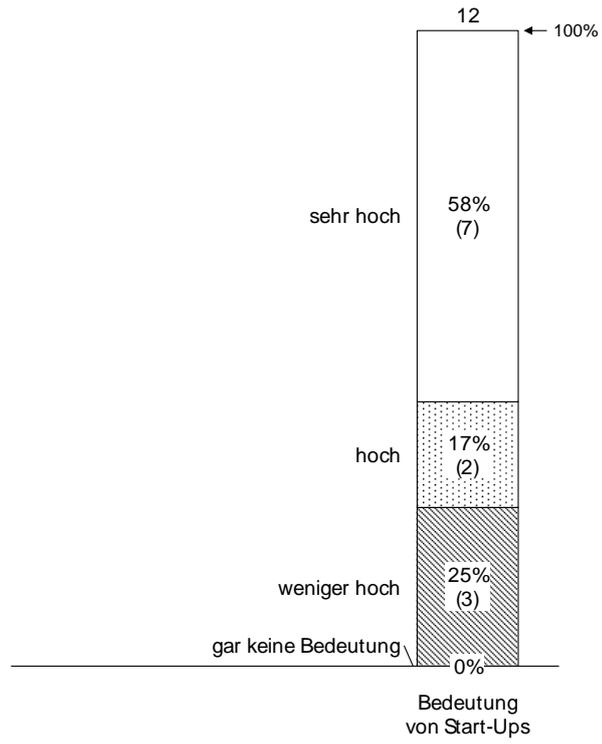


Abbildung 15: Beurteilung der Bedeutung von Start-Ups im Bereich der IT-Sicherheit

Die genaueren Gründe für die gegebenen Antworten sind vielfältig und decken das gesamte Spektrum ab. Die nachfolgende Tabelle 14 zeigt eine Gegenüberstellung der detaillierten Gründe und Gedanken zu dieser Fragestellung.

Man muss neue Dinge ausprobieren (da müsse man hinkommen)
Agilität/Flexibilität
Nicht alles Gold was glänzt
Viel „Schlangenöl“ unterwegs, 30 Start-Ups der TU-Darmstadt, 10 interessant, 5 übrig
Produktreife unbefriedigend
Maximale Verfügbarkeit ein Muss
Kreative neue Ideen am Markt
Helfen mit neuen Ideen effektiver und effizienter zu bestehen
Weil Sicherheitsmarkt sich schnell verändert
Dauerhaftigkeit der Produkte muss gesichert sein (5 Jahre Einsatz)
Innovativ / Neue Ideen
Hochflexibel
Aktuelle Bedrohungen deutlich besser zu verstehen/analysieren
Dynamisch und hohes persönliches Engagement
Thinking out of the Box
Nicht eingefahren
wg. Integrierbarkeit, Skalierbarkeit, internationalem Support
Flexibel → Agilität
Bedrohungslage ändert sich sehr schnell und die Start-Up Szene ist sehr innovativ
Der Glaube an generelle Innovationskraft von Start-Ups
Innovation
Leading Edge Technologien
Wo sind Durchbruch-Technologien, wo ist man blind auf einem Auge?
Selbst machen ist nicht immer innovationsfähig und agil
Kreativität
Embedded Software → AI und Deep Learning
Innovationskraft

**Tabelle 14: Gründe für Beurteilung der Bedeutung von Start-Ups im Bereich der IT-Sicherheit**

Es wurden sowohl positive, als auch negative Aspekte genannt. Am häufigsten wurde jedoch die hohe Innovationskraft, Flexibilität und Agilität wertgeschätzt.

Das Gesamtbild zeigt deutlich auf, dass Start-Ups eine große Rolle spielen und sich auch in Zukunft trauen sollten auf die Großanwender zuzugehen, um mit ihnen ins Gespräch zu kommen.

### Implikationen

- ▶ Start-Ups sind wichtig und sollten sich stets auch trauen auf die Großanwender zuzugehen
- ▶ Aufgrund sich sehr schnell ändernder Bedrohungen, bedarf es neuer Antworten
- ▶ Innovationskraft, neue Ideen, hohe Flexibilität und Dynamik sollten als positive Eigenschaften durch die Start-Ups gelebt werden
- ▶ Start-Ups sollten auf keinen Fall „Schlangenöl“<sup>23</sup> anbieten und eine angemessene Produktreife erreichen
- ▶ Die Dauerhaftigkeit (~5 Jahre) von Produkten zu sichern, kann von Vorteil sein

<sup>23</sup> „Schlangenöl (aus dem Englischen snake oil) ist die Bezeichnung für ein Produkt, das wenig oder keine echte Funktion hat, aber als Wundermittel zur Lösung vieler Probleme vermarktet wird.“

URL: <https://de.wikipedia.org/wiki/Schlangenöl>

Stand: 21.12.2016, Zuletzt abgerufen: 23.07.2017

#### 4.4.6 Einsatz von Start-Up Produkten

Neugegründete Unternehmen können sich nur etablieren und wachsen, wenn ihre Produkte den breiten Weg zum Kunden finden. Entsprechend wichtig ist nicht nur die „Belebung“ eines solchen Start-Ups und seiner Idee, sondern schließlich auch die Bereitschaft der Anwender diese Produkte auch einzusetzen. Daher wurde hier nach eben dieser Bereitschaft gefragt, Produkte von Start-Ups zu erwerben und der dazugehörigen Begründung.

Insgesamt sind 75% der befragten Anwender bereit, Produkte von Start-Ups zu erwerben, wenn auch teils unter Auflagen und besonderen Voraussetzungen. Entsprechend 25% sind jedoch gänzlich abgeneigt dies zu tun.

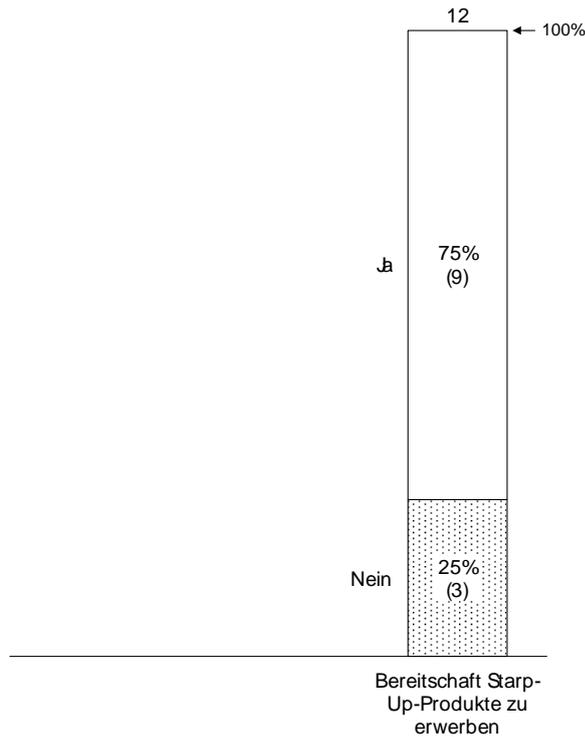


Abbildung 16: Bereitschaft der Großanwender, Produkte von Start-Ups zu erwerben

Die erwähnten Voraussetzungen aber auch genaueren Gründe für die Befürwortung oder Ablehnung sind im Original in der nachfolgenden *Tabelle 15* gegenübergestellt.

Innovativität, z.B. Authentisierungsmechanismen
kleines Umfeld → Proof of Concept, aber mit Filterungsprozess um zu schauen, ob die Idee wirklich gut ist und zum Kerngeschäft passt
Um in Nischen Erfahrung zu sammeln
Schwierig wegen Kriterienkatalog (dieser ist verpflichtend und ausschlaggebend)
Agilität
Um spezielle Anforderungen zu erfüllen oder auf besondere Bedrohungsschwerpunkte reagieren zu können; z.B. Anomalie Erkennung im Netzwerk
Greifen auf etablierte Hersteller zurück, Agilität brauchen wir nicht
in bestimmten unkritischen Bereichen → State of the Art
Unterstützung (im Einzelfall vielleicht) → Produkte und konkrete Features
Um etwas auszuprobieren, was die Großen nicht haben, für ein kleines definiertes Umfeld
Innovation & Können
Versorgungssicherheit ein möglicher Grund dagegen, es sei denn dahinter steht eine solide Firma → starkes Commitment der Mutter notwendig
Hauptgründe: Proof of Concept & Wirtschaftliche Unterstützung, aber nicht für Produktvertrieb

Qualität und Leistungsfähigkeit, wichtiger als „der Beste“ zu sein

Integration in Produkte

Tabelle 15: Gründe, die für oder gegen den Erwerb von Start-Up-Produkten sprechen

Bei den befürwortenden Großanwendern wurde häufig die Unterstützung der Start-Ups genannt, ohne die Absicht die erworbenen Produkte in der ganzen Breite einzusetzen. Auch das Sammeln von Erfahrungen in Nischen oder auf besondere Bedrohungsschwerpunkte reagieren zu können.

**Implikationen**

- ▶ Start-Ups sollten die eigenen Produkte möglichst schnell ins Feld der Großanwender zum Einsatz bringen, um aus den dortigen Gegebenheiten schnell zu lernen
- ▶ Sollten den Großanwendern dabei helfen, in Nischen Erfahrungen zu sammeln als Argument für den Einsatz der eigenen Produkte
- ▶ Produkte sollten in der Lage sein, an die Wünsche und speziellen Anforderungen der jeweiligen Großanwender angepasst zu werden
- ▶ Start-Ups sollten Fragen, ob das eigene Produkt und Preismodell auch wirklich skaliert

**4.4.7 Wichtige Aspekte als Definition der Qualität von IT-Sicherheitsprodukten**

In diesem Abschnitt wurde nach den wichtigen Aspekten bei Produkten gefragt. Konkret nach den Kriterien, welche die Qualität definieren und welche wiederum weniger wichtig im Kontext von Qualität sind. Zur Verfügung standen hier die *(internationale) Verfügbarkeit, Innovation, Supportdauer, Stärke der Kryptografie, Zertifizierung von Produkten, gute Dokumentation* und *sehr einfache Bedienbarkeit*.

Im Detail liegen die Beurteilungen für die Kriterien in jeder Gruppe recht nahe beieinander. Die in Tabelle 16 dargestellten Ergebnisse zeigen dabei auf, dass gewissermaßen Supportdauer und die Stärke der Kryptografie wichtiger sind, als Innovation und eine gute Dokumentation.

	wichtig für Qualität	weniger wichtig für Qualität
Verfügbarkeit	15%	15%
Innovation	13%	19%
Supportdauer	20%	4%
Stärke der Kryptografie	17%	11%
Zertifizierung von Produkten	11%	19%
Gute Dokumentation	13%	15%
Sehr einfache Bedienbarkeit	11%	19%
<i>Summe</i>	100%	100%

Tabelle 16: Wichtige Aspekte als Definition für Kriterien der Qualität

Hier lässt sich durchaus ableiten, dass sowohl die Stärke der Kryptografie, als auch die Supportdauer und die Verfügbarkeit zu den wichtigsten Kriterien gehören. Die Zertifizierung ist zwar ebenfalls ein Thema, hier überwiegt jedoch die Einstufung in der Kategorie der weniger wichtigen Aspekte.

**Implikationen**

- ▶ Internationale Verfügbarkeit, Supportdauer und die Stärke der Kryptografie sollten durch die Anbieter zukünftig am stärksten bedacht werden
- ▶ Innovation und Usability sind wichtige Elemente, auf die Wert gelegt werden sollte bei der Planung und Umsetzung neuer Produkte
- ▶ Es sollte von Anfang an klar kommuniziert werden, wie lange Produkte unterstützt werden

#### 4.4.8 Vergleich zwischen deutschen Anbietern und Weltmarktführern

In diesem Abschnitt wurde gefragt, was die Anbieter aus dem Ausland besonders gut machen. Weiterhin wurde erfragt, was die Großanwender sich hier von deutschen Anbietern wünschen. Antwortmöglichkeiten waren *Image des Produktes*, *breitere Palette im jeweiligen Portfolio bzw. aus einer Hand*, *günstigere Preise* und *guter Support*.

In der nachfolgenden Tabelle 17 wird deutlich, dass die Anbieter im Ausland aus Sicht der Großanwender besonders gut beim Image ihrer Produkte sind, aber auch beim breiten Angebot aus einer Hand. Dabei wird auch deutlich, dass hier die Preise und der Support eher unterdurchschnittlich bewertet worden sind.

	Anbieter Ausland Besonders gut	Wünsche an DE Anbieter
Image des Produktes	● 33%	◐ 19%
Breitere Palette im jew. Portfolio / aus einer Hand	● 38%	● 35%
Günstigere Preise	◐ 13%	◐ 23%
Guter Support	◐ 17%	◐ 23%
Summe	100%	100%

Tabelle 17: Gegenüberstellung der Stärken ausländischer Anbieter und der Wünsche an die deutsche Sicherheitsindustrie

Die an die deutschen Anbieter gerichteten Wünsche sind dabei ganz klar die Verbreiterung der Angebotspalette bei einzelnen Anbietern, um möglichst viel von nur einem einzigen Anbieter erwerben zu können. Die Preise und der Support wurden dabei stärker bewertet als der Aufbau von besserem Image der Produkte. Offenbar legen die Anwender auf das Image keinen so großen Wert, wenn die restlichen Aspekte miteinander im Einklang sind.

#### Implikationen

- ▶ Die kleinteilige IT-Sicherheitsbranche sollte eine Marktkonsolidierung anstreben, um eine gemeinsame breite Palette an Produkten aus einer Hand anbieten zu können
- ▶ Günstigere Preise und ein guter Support sind wichtiger als das Image

#### 4.4.9 Bewertung und Priorisierung von internationalem Support

In diesem Abschnitt wurde die Frage nach der Wichtigkeit von internationalem Support gestellt. Mögliche Antworten waren hier *ausschlaggebend*, *wichtig*, *nicht wichtig* und *uninteressant*.

Die *Abbildung 17* zeigt deutlich, dass der internationale Support mit 50% (6) als ausschlaggebend und mit 42% (5) mit wichtig bewertet worden ist. Lediglich 8% (1) hat diesen mit nicht wichtig bewertet. Dies zeigt, dass Großanwender hierauf großen Wert legen, dass jedoch bekanntermaßen auch gleichzeitig ein Defizit der deutschen IT-Sicherheitsbranche darstellt. Dies wurde in den durchgeführten Gesprächen in diesem Kontext immer wieder angeführt.

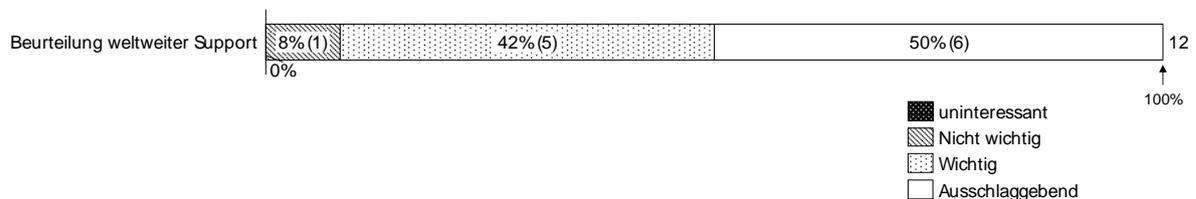


Abbildung 17: Beurteilung der Wichtigkeit von internationalem Support

In diesem Kontext war es wichtig zu verstehen, was international aus der Sicht des jeweiligen Konzerns bedeutet. Dies kann in der Realität durchaus stark vom normalen Verständnis abweichen und mit verschiedenen Blickwinkeln auf die Regionen der Welt begründet sein.

In der dargestellten *Abbildung 18* zeigt sich, dass 92% (11) der befragten international als „Weltweit ohne Einschränkungen“ sehen und 8% (1) im eigenen Kontext Europa versteht.

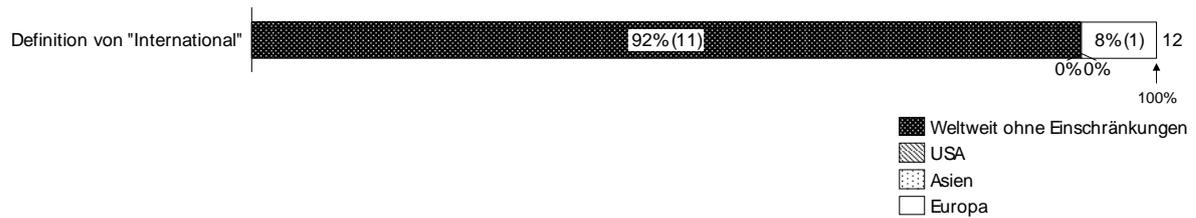


Abbildung 18: Definition des Begriffs "International" im jeweiligen Kontext des eigenen Unternehmens

An dieser Stelle wird deutlich, dass die Großanwender überwiegend international tätig sind. Dies hat auch unmittelbare Auswirkungen bei der Anschaffung von Produkten und Evaluation von Sicherheitslösungen. Anhand dieser Ergebnisse und der formulierten Anforderungen sind die Anbieter aus Deutschland hier gut beraten deutlich stärker international aufzutreten, falls sie die Großanwender zu ihren Kunden zählen wollen. Dies umfasst das Gesamtportfolio, die breiten Rolloutfähigkeiten und den Support – weltweit.

#### 4.4.10 Individuallösungen oder Standardlösungen

Hier wurde gefragt ob fertige Komponenten, also Standardlösungen, oder individuelle Lösungen bevorzugt werden. Die Darstellung der Ergebnisse in *Abbildung 19* zeigt, dass überwiegend gerne fertige Standardlösungen ausgewählt werden. Kein Großanwender würde gerne ausschließlich auf individuelle Produkte setzen wollen.

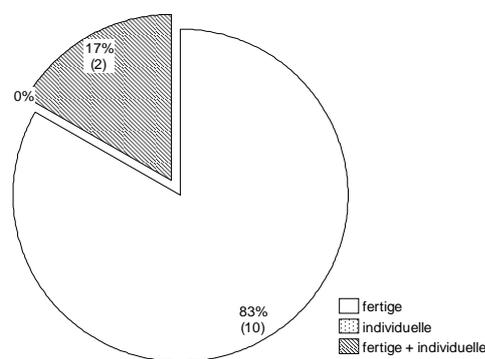


Abbildung 19: Bevorzugte Art der einzusetzenden IT-Sicherheitslösung

In den abweichenden Fällen wurde dargelegt, dass zwar beides in Frage kommt, aber fertige Lösung am Ende die Präferenz darstellen. Des Weiteren wurden auch deswegen beide Angaben gemacht, da es auch themenabhängig ist, welche der beiden Möglichkeiten relevant sein könnte.

Diese Bewertung erlaubt die Annahme, dass der Markt für standardisierte Lösungen dominierend ist, es jedoch nach wie vor auch einen nicht unerheblichen Nischenmarkt für Individuallösungen gibt.

#### 4.4.11 Einsatz und Förderung von Open Source

Open Source ist heute ein essenzieller Bestandteil aller verwendeten IT-Produkte. Daher wäre es besonnen, wenn diese Projekte über die entsprechenden personellen und finanziellen Ressourcen verfügen würden. Hierzu wurden einige wichtige Fragen adressiert.

Als erstes wurde die Frage nach der Nutzung von Open Source Produkten im Bereich der IT und IT-Sicherheit gefragt. Weiterhin wurde um die Beurteilung der Wichtigkeit von Open Source gebeten.

Von Interesse war auch, ob die Großanwender sich allgemein vorstellen könnten Open Source Projekte und deren Entwicklung hinsichtlich höherer Qualität und Sicherheit finanziell zu unterstützen.

Es wurde anschließend die Idee eines möglichen „DAX 30 Open Source Fonds“ unterbreitet, um Qualität und Sicherheit von wichtigen Open Source Projekten langfristig zu fördern und zu verbessern und ob eine jährliche finanzielle Beteiligung in Frage käme. Abschließend wurde die Größenordnung dieser Summe erfragt als Mindestbetrag, der pro Jahr zur Verfügung gestellt werden könnte.

## 100% nutzen Open Source

Insgesamt gaben alle 12 der der Befragten an, Open Source im Bereich der IT und IT-Sicherheit zu nutzen. Dies sind 100% aller befragten Großanwender. Gleichzeitig könnten sich 11 der 12 befragten Unternehmen grundsätzlich vorstellen, Open Source Projekte und deren Entwicklung finanziell zu unterstützen, mit dem Ziel der Steigerung von Qualität und Sicherheit. Ein Teilnehmer war dabei unentschlossen, hat die Idee jedoch nicht prinzipiell abgelehnt. Der Grund für diese Frage hat einen bestimmten Hintergrund.

### Open Source ist (nicht immer) sicher

Die Annahme aus der Vergangenheit, die Offenlegung von Quellcode würde eine höhere Sicherheit zur Folge haben, hat sich nicht unbedingt als wahr herausgestellt. Eher ist das Gegenteil eingetreten. Dies liegt mitunter daran, dass der Community schlicht und einfach die Ressourcen fehlen, um sich intensiver mit der Qualitätssicherung bei der Entwicklung und bei der Produktpflege auseinanderzusetzen zu können.

### DAX 30 Open Source Fonds

Bei einer finanziellen Beteiligung an entsprechenden Projekten stellt sich die Frage nach der Organisation und einer möglichen Umsetzung. Hierfür wurde ein fiktiver DAX 30 Open Source Fonds zur Sprache gebracht, um auf dieser Grundlage mögliche Arten der Zusammenarbeit und die dafür bereitgestellten finanziellen Mittel abzufragen. Dieser wird als fiktiv bezeichnet, da es diesen bisher in dieser oder ähnlicher Form nicht gibt. Die genannten Vorbehalte, Ideen und Summen unterschieden sich sehr stark voneinander. So zeigt die nachfolgende *Abbildung 20* ein differenziertes Bild. Insgesamt wären 67% (8) Großanwender bereit diesem Fonds beizutreten, 17% (2) waren zu diesem Zeitpunkt unentschlossen und die verbliebenen 17% (2) haben diese Idee abgelehnt.

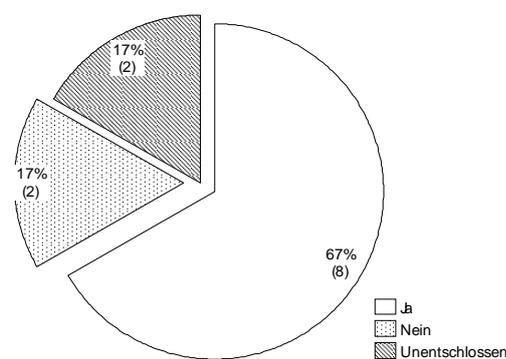


Abbildung 20: Open Source Fond DAX 30: Teilnahme und Zuwendung mit einer grundsätzlichen Beteiligung

Natürlich waren im Falle einer Beteiligung die mögliche Summe und Voraussetzung bedeutende und interessante Punkte.

## 10.000 EUR bis 5.000.000 EUR p.a.

Bei der Frage welche Größenordnung aus Sicht der jeweiligen Großanwender als jährlicher Beitrag möglich wäre, sind sehr unterschiedliche Summen genannt worden. Der niedrigste Betrag wurde mit 10.000 EUR genannt. Es gab aber durchaus die Bereitschaft auch 100.000 EUR bis 200.000 EUR zu investieren, wobei hier die Frage nach einer möglichen Rendite gestellt worden ist. Der zweithöchste Betrag lag bei 2.000.000 EUR. Den mit Abstand höchsten Beitrag pro Jahr belief sich auf 5.000.000 EUR. Alle anderen Teilnehmer konnten und wollten sich auf keine Zahl festlegen, haben aber deutlich gemacht, dass dies stark vom Konzept, Einfluss und Mehrwert abhängig wäre. Es gibt an dieser Stelle in jedem Fall Potential und über die Gründung solch eines Fonds sollte zukünftig unbedingt nachgedacht werden. Dies könnte unter dem Dach eines Vereins oder Verbandes umgesetzt werden.

### Implikationen

- ▶ Bei der Gründung eines Open Source Fonds würden auf einen Schlag beträchtliche Mittel zur Verfügung stehen, die heute ungenutzt sind
- ▶ Eine Organisation ist zu gründen, die das Geld abrufen und darüber verfügen kann – möglicherweise unter dem Dach eines Verbandes, wie VOICE oder in Kooperation mit der OSB Alliance (Open Source Business Alliance<sup>24</sup>)
- ▶ Es muss eine Strategie entwickelt werden, wie möglichst alle Großanwender zu einer Teilnahme an einem Open Source Fonds motiviert werden können

---

<sup>24</sup> Open Source Business Alliance: <http://osb-alliance.de/ueber-uns/was-ist-die-osb-alliance>

#### 4.4.12 Defizite und Erwartungen von/an IT-Sicherheitsprodukten und Anbietern

Dieser Abschnitt beschäftigt sich mit der Erwartungshaltung an IT-Sicherheitsprodukte und gliedert sich in drei Bereiche. Als erstes wurde gefragt, was die Großanwender bei dem Gedanken an IT-Sicherheitsprodukte „nervt“. Dann wurde erfragt, was das allerwichtigste ist, dass sie von einer IT-Sicherheitslösung erwarten. Anschließend wurde die Erwartungshaltung gegenüber dem IT-Sicherheitsanbieter erörtert, bei der es um darum ging, was als allerwichtigstes Merkmal bewertet wird.

Bei der Frage, was die Großanwender an IT-Sicherheitsprodukten „nervt“ wurden von den meisten zahlreichen Aspekten genannt, die in der nachfolgenden *Tabelle 18* gegenübergestellt werden. Dies zeigt, dass es hier offenbar sowohl Frustration gibt als auch gleichzeitig Raum für Verbesserungen. Dies sollte von der IT-Sicherheitsindustrie als Herausforderung gesehen werden, um zukünftig herrschende Vorbehalte reduzieren zu können.

Preis
Qualität
Komplexität
Es werden im Vergleich nur kleine Teilprobleme adressiert → immer nur Nischen
Die Produkte halten nicht, was sie versprechen
Schwarz/weiß → entweder sicher oder nicht, Grautöne fehlen
<i>(relativ wenig)</i>
Mangelnde Usability
Dass das Bewusstsein nicht da ist, dass Sicherheit Geld kostet <i>(auch aus Sicht als Anbieter von Produkten selbst)</i>
Spionageverhältnisse
Insbesondere, wenn sie betrieben werden (müssen) unter dem, was möglich ist (selten Prozesse und Trainings für die effektive Einführung → „Friss oder Stirb“)
Oft fehlende Passgenauigkeit
Alles ist kompliziert
Unterscheidungsmerkmale sind nicht einfach, Bauchentscheidungen unnötig machen
Komplexität bei der Implementierung
Systeme werden nicht schneller/besser bedienbar
Höhere Versprechen als Funktionalität
Funktionalität in Produkten oft vorrangig und Gefahr, dass sie hinten runterfällt, weil komplex & teuer
Auf sich allein gestellt als DAX
Schlechte Nachvollziehbarkeit der Wirkung
Usability
Integrationsfähigkeit mangelhaft! (nicht minimal invasiv, keine Server, simpel und transparent sollte es sein)
Dass Deutschland nicht in der Lage ist, digitale Souveränität zu erzeugen!
In Kernbereichen kein Einsatz von deutschen Produkten, nur Drumherum
Nichtintegrierbarkeit
Anbieter-Lock-In Verhalten
Keine IT-Replaceability
Suggestieren oft als die Lösung aller Probleme
Awareness ist heute aufwändig
Vieles über verschiedene Dienstleister nötig → nervt
Arbeitet unzuverlässig
Neue Projekte = Aufwand immens groß (→ zu hoch)

**Tabelle 18: Negative nervende Eigenschaften von IT-Sicherheitsprodukten**

Die Hauptmerkmale, die als negativ empfunden werden, sind insbesondere unzureichende Qualität, ein verhältnismäßig zu hoher Preis, die fehlende Integrierbarkeit und die viel zu hohe Komplexität

der Produkte. Die Kleinteiligkeit der Produkte am Markt wird ebenfalls als sehr negativ empfunden. Auch die ingenieurgetriebene Denkweise, alles muss perfekt und vollkommen sicher sein, ist hier fehlplatziert. Hier sind durchaus auch Abstufungen gewünscht, bei der es nicht immer nur die beiden Extreme gibt. Auch die fehlende digitale Souveränität und die faktisch bisher nicht vorhandene IT-Replaceability missfallen den Befragten stark.

Ein weiterer Punkt ist ebenfalls nicht unerheblich: Hier wurde die eigentlich schlechte Nachvollziehbarkeit der Wirkung von IT-Sicherheitsprodukten angemerkt. Es ist oft unklar, wie gut, wirkungsvoll und den Behauptungen des Herstellers entsprechend eine Lösung wirklich arbeitet.

Die Frage nach den wichtigsten Merkmalen, die von einer IT-Sicherheitslösung erwartet werden, wurde ebenfalls differenziert beantwortet. Die gegenübergestellten Antworten sind nachfolgend in Tabelle 19 dargestellt.

Hier sind ebenfalls einige Punkte deutlich hervorzuheben. Insbesondere ist der Wunsch, den CISO Job zu erleichtern, sehr deutlich artikuliert worden. Auch Transparenz war ein großer Wunsch. Eine Lösung soll durch den Nutzer praktisch nicht wahrnehmbar sein, auch wenn sie vorhanden ist und wirkungsvoll arbeitet. Vergleichbar wäre das mit dem Einzug von Fingerprint-Scannern im Bereich der Smartphones. Beim Entsperren der Geräte nimmt der Nutzer die dahinter ablaufende Sicherheitsprüfung und Eingabe seines Passwortes heute gar nicht mehr wahr.

Qualität Betriebbarkeit → läuft auf Standardprodukten
Hält was sie verspricht Den CISO Job/bzw. der jew. Verantwortungsträgers erleichtert
Zuverlässigkeit Keine Störung des Geschäftes/Betriebes
Genau das tut, was sie soll Läuft transparent einfach mit
Das sie funktioniert! Dass sie vorhanden ist!
Ergebnisse (echtes Plus von Sicherheit, hohe Ausfallsicherheit) Transparente Produkte
Dass sie verlässlich ist Leicht zu implementieren ist (Rollout) inkl. Betrieb und Entstörung (→ Lifecycle) Performance & Transparenz(!) + „Smoothness“ → Leute sollen es gar nicht wahrnehmen Behindert nicht das Business
Funktionalität und Qualität (gleichartig) Proaktive Elemente und nicht nur reaktiv
Muss effektiv sein Muss Nutzen erzeugen → Nutzen muss transparent sein
Sicherheit! Hoch performant + sicher + Preis muss stimmen
Resilienz Mandantenfähigkeit (Perspektive: Zentrale ↔ Außenwerke)
Managementfähigkeit Interoperabel
Operative Zwecke erfüllen Weltweite Rolloutfähigkeit

Tabelle 19: Erwartungen an die IT-Sicherheitsprodukte hinsichtlich Merkmalen

Weitere hervorzuhebende Punkte sind die Verlässlichkeit und die durch den Hersteller zugesicherte Funktionsfähigkeit.

Auch der IT-Sicherheitsanbieter selbst sollte in den Fokus gestellt werden und nicht nur ausschließlich die Produkte. Aus diesem Grund wurde die Frage nach den Erwartungen an den IT-Sicherheitsanbieter selbst gestellt. Eine Gegenüberstellung der gegebenen Antworten auf die Frage nach den Erwartungen an den IT-Sicherheitshersteller findet sich in der nachfolgenden *Tabelle 20*.

Die gemachten Angaben spiegeln wie in den anderen Gegenüberstellungen die offene Meinung der jeweiligen Personen wieder. Ein deutliches Querschnittsthema ist hier der immer wieder gewünschte weltweite Support und das tiefe Verständnis für das Business der jeweiligen Anwender.

Zuverlässigkeit Guter Support
Versteht die Probleme des CISO/Verantwortungsträgers und ihm hilft Nicht den Profit im Auge hat
Zuverlässigkeit auf allen Ebenen (Zusagen, Pattern, Patches, Pflege, ... & Betrieb) Breites Portfolio
Kompetenz Kompatibilität
Produkte halten, sie versprechen Business der Anwender verstehen
Reaktionsschnelligkeit Fähigkeit unsere Probleme zu verstehen
Ehrlichkeit Flexibilität
Zuverlässigkeit „Responsiveness“ (dynamische Anfragen umsetzen) → Qualität
Kompetenz Vertrauenswürdigkeit
Qualität und Zuverlässigkeit Reaktionszeit
Weltweiter Support (!) Zurückhaltung
Ansprechbarkeit Langfristige Partnerschaft und nicht nur zyklusbasierter Umsatz alle paar Monate → Dialog
Kostengünstig Schnelligkeit
Bewertung rund um den Betrieb und Einführung von Produkten NO GO: Anbieter klopft beim Management
Exzellenter Support weltweit Schnell verfügbar
Interoperabilität Offene Standards
Hohes Maß an Vertraulichkeit und Integrität (Diskutieren) Flexible Dienstleistung (Hilfe bekommen, Migration, Fallstudie, Planung, Shared Management, ...)

**Tabelle 20: Erwartungen an die IT-Sicherheitshersteller hinsichtlich Merkmalen**

Einige der wichtigsten Aspekte waren weiterhin, dass die Hersteller ihre Versprechen halten, an einer längerfristigen Partnerschaft interessiert sind und Interoperabilität erlauben. Was absolut nicht erwünscht war und auch als Erwartungshaltung an die Hersteller formuliert wurde, dass der

Hersteller keinesfalls den Weg über das Management des Unternehmens suchen sollte – also am IT-Sicherheitsverantwortlichen bzw. Entscheider vorbei.

### Implikationen

- ▶ IT-Sicherheitsprodukte halten nicht was sie versprechen, erlauben keine Grautöne hinsichtlich der Sicherheit, sind zu komplex und schlecht bedienbar – insbesondere diese Punkte „nerven“ die Großanwender und müssen zukünftig aufgearbeitet werden
- ▶ Weiterhin sind die am häufigsten erwarteten Merkmale von IT-Sicherheitsherstellern: Zuverlässigkeit und Vertrauenswürdigkeit
- ▶ Für eine erfolgreiche Positionierung muss durch die Anbieter eine langfristige echte Partnerschaft angestrebt werden
- ▶ Zukünftige Produkte sollten halten, was sie versprechen und die erreichte Sicherheit bzw. Wirkung sichtbar machen: Sie sollen wirklich genau das tun, was sie versprechen
- ▶ Die IT-Sicherheitshersteller sollten zukünftige Produkte transparent machen und die Usability deutlich steigern

#### 4.4.13 Fragmentierung des IT-Sicherheitsmarktes

Der IT-Sicherheitsmarkt in Deutschland ist groß und das Angebot entsprechend vielfältig, daher wurde hier nach der Meinung zum Fragmentierungsgrad des IT-Sicherheitsmarktes gefragt. Mögliche Antworten waren *zu stark* fragmentiert, *mittelmäßig*, *für uns in Ordnung* und *weiß nicht*.

Im Ergebnis ist eine deutliche Tendenz zu einer zu starken Fragmentierung des Marktes für IT-Sicherheit in Deutschland sichtbar. Dies finden 58% (7) der Befragten. Einer fand den vorherrschenden Zustand so in Ordnung mit der Begründung, dass es so genügend Auswahl und Alternativen gibt. Ein Diversifizierter Markt hat aus seiner Perspektive und Einschätzung also demnach auch Vorteile.

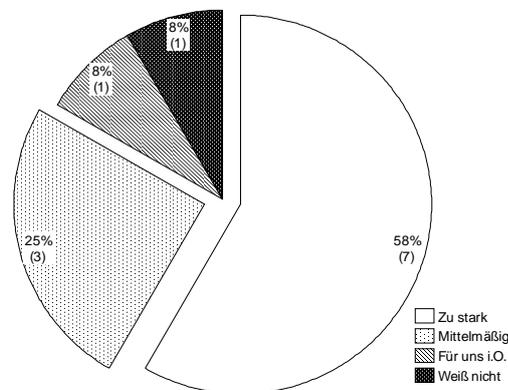


Abbildung 21: Beurteilung der Fragmentierung des IT-Sicherheitsmarktes

Bei einer gemeinsamen Betrachtung von *zu stark* und *mittelmäßig* ergibt dies 83% (10) und damit den Löwenanteil der Ergebnisse. Das deutet auf den Wunsch einer Marktkonsolidierung in diesem Bereich hin, weg von der Kleinteiligkeit und hin zu größeren Playern mit größerem Portfolio und einer deutlich stärkeren Marktpräsenz.

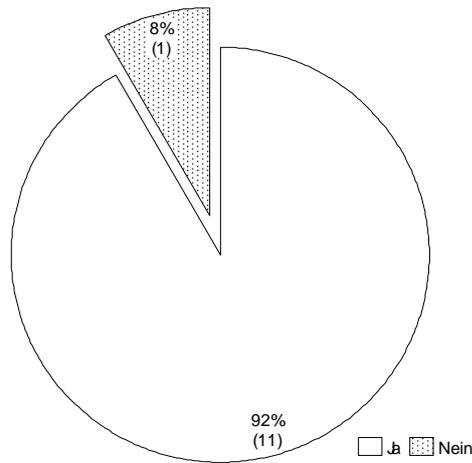
### Implikationen

- ▶ Die Hersteller müssen sich zukünftig zusammenschließen, in welcher Form auch immer

#### 4.4.14 Bewusste Akzeptanz von IT-Sicherheitsgefahren

In diesem Abschnitt wurde gefragt, ob Großanwender bewusst Risiken in Kauf nehmen, durch die Nichtnutzung von IT-Sicherheitsprodukten. Anschließend sollte die gegebene Antwort begründet

werden und eine mögliche Erläuterung angegeben werden, wie diese Risiken am Ende getragen werden.



Die Risiken werden jedoch nicht gänzlich ignoriert, sondern selbstverständlich anderweitig adressiert und stets berücksichtigt. Zudem werden diese Risiken nicht nur akzeptiert, sondern auch getragen, wenn auch nicht immer auf die gleiche Weise.

Grund für Akzeptanz von Risiken	Maßnahme um diese Risiken zu tragen
Aufwand vs. Schutz (Pareto Prinzip) Bewusst	Risikoprozesse → Risikomeldung, je nach Größe/Kritikalität sogar bis zum Vorstand
Begrenzte Budgets und Ressourcen	Versicherung für „Dellen in der Bilanz“
Individuelles/Funktionales - Risiken vs. Kosten (Graph)	Interner Risikobericht (Enterprise Risk Management)
Business kann das Risiko tragen	durch Akzeptanz
Kostenfaktor	Risikomanagement
Risiken vs. Schadenshöhe	
Weil Sicherheit ohne Risikomanagement nicht möglich ist	Durch ordentliche Prozesse mit externer Zertifizierung (ISO 27000)
Extrem viele Regularien weltweit (ca. 15.000?)	Risk Acceptance klar strukturiert
Aufgrund der Betriebsprozesse	Risikoakzeptanz gemäß ISMS
Produkte passen nicht in Infrastruktur, weil Erwartungen nicht erfüllt	Risikobericht
Monetäre Gründe	Management, das priorisiert und entscheidet
Personelle Ressourcen → Prioritäten setzen (Zeit/Geld)	
Strategie: Abwägung und Sicherheitsnutzen	Risikoabwägung → Risikomanagementprozess Versicherungspolicen
Man läuft den Bösen hinterher	Erst müssen sie aufgedeckt werden und dann bewertet
Kosten/Nutzen ist irgendwann zu sehr defizitär	Risikobericht
So gut wie möglich aber nicht perfekt (→Kosten)	Jour-Fixe mit CFO/CEO
Trust ist ein hohes Gut, auch in das eigene Unternehmen	Zum Teil vertraglich → Partner od. Units (Töchter)
Risikobasiert	Zum Teil Versicherungspolicen
Budgetprobleme	Im Rahmen des Enterprise Risk Management Berichtes
Abstimmungsprobleme mit IT-Organisation	Informationssicherheit-Review mit Vorstand
Konflikt zwischen IT und IT-Sicherheit → IT-Eitelkeit bekämpfen (→ Allgemeinmedizin vs. Facharzt)	
<i>Zusammenfassung (Interpretation)</i>	<i>Für die letzten Prozentpunkte an Sicherheit fehlt das Geld. Aus diesem Grund werden Risiken klassifiziert und dokumentiert, statt entsprechende Produkte zu kaufen. Tragen der Risiken durch Akzeptanz und entsprechendes Risikomanagement. Zudem wird letztendlich auch in Versicherungspolicen investiert, statt in IT-Sicherheitsprodukte.</i>

Tabelle 21: Gegenüberstellung der Gründe für Akzeptanz von Risiken und Maßnahmen um diese zu tragen

Die Gegenüberstellung zeigt ein ausgeprägtes Bewusstsein für die Grenzen der Sicherheitslösungen und die verbleibenden Risiken. Hier ist das häufigste Argument die negative Bilanz zwischen den Kosten und dem Erreichen eines noch höheren Schutzes. Am Ende des Tages wird es immer Restrisiken geben, da sich hier alle Einig sein: Absolute Sicherheit gibt es nicht.

Auch die Art des Umgangs mit den Risiken ist klar definiert. In den meisten Fällen finden sich diese Restrisiken im internen Risikobericht. In einigen Fällen existieren entsprechende Versicherungspolice „gegen Dellen in der Bilanz“. Grundsätzlich wurde klar dargestellt, dass Sicherheit ohne Risikomanagement nicht möglich ist.

### Implikationen

- ▶ In der Konsequenz, dass die letzten Prozentpunkte Sicherheit meist über dem Budget liegen, setzt die Masse heute auf das Pareto Prinzip, also einen Grundschutz mit Hilfe von Basisprodukten für eine hohe Effektivität und einen geringeren Anteil von Speziallösungen
- ▶ Es gilt ggf. bei der Argumentation eines Einsatzes weiterer Produkte auch den ROI zu berücksichtigen (Return on Investment)
- ▶ Für den Einsatz einiger Produkte ist das nötige Personal nicht vorhanden, auch wenn das Budget für die Beschaffung da wäre, daher sollte der Rolloutaufwand geprüft und optimiert werden
- ▶ Es gilt zu prüfen, um welche Produkte es sich genauer handelt, die nicht beschafft werden und ob hier mit anderen Preismodellen Abhilfe geschaffen werden kann

#### 4.4.15 Hochsicherheitslösungen

Im Bereich der Sicherheit gibt es bekanntermaßen verschiedene Abstufungen. Auch im Bereich der IT-Sicherheit ist es möglich Hochsicherheitslösungen einzusetzen, die besonders robust und höherwertig sind. Hier wurde die Frage gestellt, ob die Großanwender prinzipiell gerne mehr Hochsicherheitslösungen einsetzen würden. Hierzu zählen beispielsweise hochsichere VPN, gehärtete virtualisierte Arbeitsumgebungen, etc.

Nachfolgend wurde also gefragt, ob Hürden gesehen werden, dies zu tun, wo diese sind und für welche Szenarien der Einsatz dieser höherwertigen Technologien denkbar wäre.

Die Meinung hinsichtlich des Einsatzes von Hochsicherheit ist sehr gespalten. Hier liegt Aufteilung genau bei 50% dafür und dagegen.

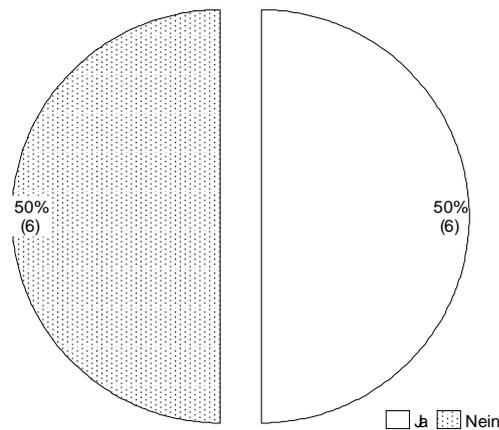


Abbildung 22: Wunsch nach Einsatz von mehr Hochsicherheitslösungen

Selbstverständlich gibt es für die jeweiligen Positionen auch Gründe, die in der nachfolgenden Darstellung in *Tabelle 22* genauer beleuchtet werden. Hierbei wurden jeweils die Hürden, die gegen Hochsicherheit Sprechen dokumentiert als auch Szenarien, für die Hochsicherheit durchaus denkbar ist.

Hürden, die gegen Hochsicherheit sprechen	Szenarien, für die Hochsicherheit denkbar ist
Angemessenheit (Pareto Prinzip)	Kronjuwelen sichern (wenige Prozent) Kleiner Bereich z.B. Design Center Potsdam
Kosten sind zu hoch Zu hohe Komplexität Integration schwierig in IT und OT, Risikoabwägung & Schutzbedarf → Gießkanne (Widerspruch)	Kritische Infrastrukturen für Siemens oder als Lieferant für KRITIS (Windturbine → Windpark) Windenergie as a Service z.B. öffentliche Verkehrsmittel → Transport, der zu gewissen Wahrscheinlichkeit zur Verfügung steht
Usability mangelhaft Kosten sind zu hoch Kosten sind zu hoch Komplexität (auch Nutzung)	Kernkraft Überall dort wo regulatorisch gefordert (VS) weniger VIP (R&D)
Kosten sind zu hoch Regelungslage schwierig (Gesetzeslage schwierig)	Je nach Klassifizierung von Themen Kommunikation/Daten Identifikation von wertvollen Daten → Hochsicherheitslösungen
Nutzerakzeptanz und Akzeptanz im Allgemeinen Kosten sind zu hoch	Sichere Zonen in R&D Kritische Produktionsbereiche Innovative Produkte und IOT-Themen
Keine Gesetze, die uns dazu zwingen, keinerlei Antrieb	Absicherung der vorhandenen SAP-Systeme

"3.000 iPads draußen → Zugriff auf Daten"	Kaskadeneffekte verhindern an neuralgischen Punkten
Da wo es notwendig ist	Investment vs. Schadensvermeidung
Risikoabhängig	→ Kronjuwelen → hoher Schaden & Existenzabhängigkeit
Praktikabilität und Usability	1. Klassifizierung → Golden Nuggets
Integrierbarkeit	2. Kritische Personenkreise
Kosten sind zu hoch	Kernkraft und Netze (woanders ist der Schutzbedarf nicht so hoch) Kundendaten und Mitarbeiterdaten im Allgemeinen
Kosten sind zu hoch	Abwicklung finanzieller Dinge des Unternehmens
Inbetriebnahme aufwändig (Change Projekt massiv aufwändig)	Alles was mit Cyber Security zutun hat (Admin, ...) (Group Privilege Access Management)
IAM eher schützenswert hinsichtlich Verfügbarkeit	
Kein Leib und Leben Problem (Finanzindustrie)	
Nicht verfügbar mit dem weltweiten Support unter den wirtschaftlichen Aspekten	Alles was strictly confidential ist

Tabelle 22: Hürden gegen Hochsicherheit und mögliche Einsatzszenarien

In beinahe allen Unternehmen wurden die zu hohen Kosten angeführt, die gegen den Einsatz von Hochsicherheit sprechen. Auch ist die Gesetzgebung hier ein Treiber: Anwendung findet Hochsicherheit dort, wo es die Regularien verlangen. Auch der Schutz von Leib und Leben, den „Golden Nuggets“ bzw. Kronjuwelen eines Unternehmens oder streng vertraulichen Informationen wird den Hochsicherheitsprodukten anvertraut. So vertritt unter anderem die Unternehmensberatung KMPG die These, dass etwa 5% aller Unternehmensdaten kritisch und besonders schützenswert sind. [6] Da dies immer nur sehr kleine Nischen eines Unternehmens sind, wäre im Falle einer Ausweitung dieser Technologien auf einen deutlich größeren Teil hochinteressant für die insgesamt überschaubare Anzahl von Herstellern entsprechender Produkte in Deutschland.

### Implikationen

- ▶ Hochsicherheitsprodukte sind wichtig, allerdings teuer und von hoher Komplexität
- ▶ 5% aller Unternehmensdaten sind kritisch und besonders schützenswert, was einen insgesamt bedeutenden Markt ergibt
- ▶ Hersteller von Hochsicherheitsprodukten sollten zukünftig prüfen, wie sich die Bedienung der Produkte weiter verbessern und erleichtern lässt

## 4.5 Marktsituation und Defizite

Dieses Kapitel befasst sich mit Themen der Marktkonsolidierung, fehlenden Produkten, Sicherheitsanforderungen in 5 – 10 Jahren, der Beurteilung der Leistungen unserer Sicherheitsbehörden, möglichen zukünftigen staatlichen Aufgaben, der aktuellen Diskussion „sichere Verschlüsselung vs. Backdoors“ und der aktuellen Beurteilung der IT-Sicherheitslage.

### 4.5.1 Wunsch nach Konsolidierung des Angebotes: Zusammenfassung von Produkten

In diesem Abschnitt wurde das Thema der Marktkonsolidierung aufgegriffen und gefragt, welche Produkte die Großanwender am liebsten gerne zusammenfassen würden zu einem stimmigen Gesamtpaket.

Die von den befragten gemachten Vorschlägen zur Zusammenfassung von Produkten:

- Ein komplettes Bundle im Monitoring Bereich als echte „*Security Analytics Platform*“: Zusammenführung von Firewall, IDS und Kommunikationslagebilder zu einem Produkt mit, Sensorik (TAP) + User Awareness, interne Angriffe, Verhalten und einer mächtigen Funktion zur Generierung von Management-Reports, mit denen sich Budgets begründen lassen.
- Integratives Endpoint-Security Produkt, welches die heute 15 verschiedenen notwendigen Deemons überflüssig macht.
- Incident & Event Monitoring in Kombination (Splunk und Arcside).
- Kombination aus Vulnerability Management, Capture Management und Infrastruktur.
- Information Security Management System (ISMS) & Enterprise Risk Management (ERM) mit Speisung aus internen Audits.
- Verschlüsselung auf Firewall-Ebene mit Peer2Peer für Cloud-Dienste.
- Anomalie Erkennung in Kombination mit SIEM Systemen in Verbindung mit Multi Faktor Authentikation (MFA) und Hochsicherheitsadministration.

Zusammenfassend sind Produktkombinationen erwünscht, welche Arbeitsabläufe vereinfachen ohne „Klebstoff“ verwenden zu müssen und die „Brüche“ verursachen, also eine entsprechende Durchgängigkeit besitzen.

Die Frage der Konsolidierung wurde insgesamt als sehr gut bewertet aber in der Beantwortung durchaus schwierig. Immer komplexere Produkte bedeuten auch ein lohnendes Angriffsziel. Auch neue Trends, wie beispielsweise Software Defined Networks (SDN), verschärfen diese Entwicklung aus der Sicht der Großanwender.

Einige Teilnehmer gaben an, die Divergenzen am Markt aus Gründen des Wettbewerbes und verteilten Risiken zu begrüßen. Eine weitere Begründung war, dass native spezialisierte Lösungen besser seien als hybride.

#### Implikationen

- ▶ IT-Sicherheitsprodukte sollten keine „Brüche“ in Nutzung, sowie ihren Schnittstellen verursachen und interoperabel werden
- ▶ Es sollte in Monitoring Werkzeug zur Verfügung stehen, welches die Kommunikation mit allen sich im Einsatz befindlichen IT-Sicherheitsprodukten erlaubt
- ▶ Es muss eine mächtige *Advanced Security Analytics Platform* zur Verfügung stehen, die sämtliche wichtigen Funktionen in sich vereinen kann

#### 4.5.2 Wunsch und Suche nach gänzlich fehlenden IT-Sicherheitsprodukten

Dieser Abschnitt widmet sich den Lücken auf dem IT-Sicherheitsmarkt und der Suche nach Produkten, die aktuell fehlen. Die konkrete Frage war, nach welchen IT-Sicherheitslösungen die Großanwender derzeit suchen, die es gerade nicht oder nicht genug gibt.

Die von den befragten gemachten Vorschlägen für mögliche neue Produkte:

- Integrierte Sicherheitsarchitektur auf dem Weg in die Cloud.
- (Wirklich) Smarte Endpoint Security.
- Vollständig einheitliche und integrierten Mail-Verschlüsselungs-Standard.
- Sichere und gute Authentifizierung & Authentisierungsverfahren für häufig wechselnde Nutzer an festen Arbeitsplätzen, anpassbar an die eigenen Prozesse.
- Produkte, die trotz hoher Dynamik der Menschen und Geräte in Netzen die Absicherung sicherstellen. Die Denkweise der „hohen Zäune“ aus der Vergangenheit ist hier wirkungslos.
- Gut bedienbare, benutzbare und voll integrierbare IAM-Lösungen (Identity and Access Management).
- Die Möglichkeit eines sicher verschlüsselten externen „WAN-Drives“ (Zero-Knowledge).
- Wirksamen Schutz von IoT in der Roboterwelt.
- Absicherung der Kommunikation von Auto und Maschine.
- Mobile Geräte + Sicherheit (iOS & Android) inkl. Arbeitsfähigkeit + BYOD/privatem Einsatz inkl. VPN + getrennter Datenhaltung.

Einige der genannten Produkte mag es auf den ersten Blick so oder in ähnlicher Form geben, diese erfüllen jedoch offenbar die Bedürfnisse der Großanwender im alltäglichen Einsatz nur bedingt.

#### Implikationen

- ▶ IT-Sicherheitsprodukte sollten keine „Brüche“ im Bereich der Nutzung und Schnittstellen verursachen
- ▶ Interoperabilität von Produkten ist ein wichtiges Thema, das es durch die Hersteller aufzugreifen gilt
- ▶ Im Kontext der stattfindenden Cloudifizierung gibt es hinsichtlich deutscher Produkte Nachholbedarf
- ▶ Bei den Verschlüsselungsprodukten im Bereich E-Mail, sollte es zukünftig einen *einfachen* gemeinsamen breit einsetzbaren Standard geben

#### 4.5.3 Sicherheitsanforderungen der Zukunft in 5 und 10+ Jahren

In diesem Bereich wurden die Sicherheitsanforderungen in den nächsten 5 Jahren und in 10 Jahren thematisiert. Zum einen wurde gefragt, wie die IT-Sicherheit in 3 – 5 Jahren aussehen sollte. Zum anderen wurde nach einer visionären Einschätzung für 10+ Jahren gefragt, also im Grunde genommen die IT-Sicherheit im Jahre 2027 bis 2030. Am Ende wurde die Frage gestellt, wer im Konzern für die IT-Sicherheit verantwortlich sein sollte.

In der nachfolgenden *Tabelle 23* finden sich die jeweils gegebenen Antworten. Dabei gibt es viele Aspekte, die sich auf heutige Probleme beziehen. In der Zukunft werden diese heutigen Herausforderungen als gelöst betrachtet. Dazu zählen umgesetztes Security by Design, vollkommen transparente aber resiliente Sicherheit und der breite Einsatz von Artificial Intelligence, sowohl auf Angreifer als auch auf Abwehrseite. Es wird sogar angenommen, dass beide Seiten irgendwann voll autonom handeln werden.

## Ergebnisse der Datenerhebung bei den Großanwendern der DAX30

IT-Sicherheit und Herausforderungen in 3-5 Jahren	IT-Sicherheit und Herausforderungen in 10+ Jahren
Build-In Security: Security by design wird umgesetzt sein Neue Bedrohungsszenarien	Volle Transparenz: Es ist was da, als Nutzer merkt man nichts, aber es gibt 100% Sicherheit „a la Star Trek“
Job „9 to 5“ Vereinfachung/Entlastung des CISO Lebens bzw. des IT-Security Alltags	Bewusstsein wird höher werden und auch die Bereitschaft auch etwas zu tun  Deutlich höhere Usability und Transparenz
Vollkommen transparent für User Hoch kollaborativ In der Lage den aktuellen Bedrohungen wirksam gegenüber zu stehen Bezahlbar bleiben Routineübungen in Unternehmen neu zu erfinden	Vollkommen Resilienzen-fähig gegen zukünftige Vollprofi-Angreifer  IT-Sicherheit klassische Legacy in allen Unternehmen sein Genfer Konvention für Endanwender im Internet, Privatanwender wird das nie leisten hinsichtlich der erforderlichen Sicherheit und sonst massiv unter der Nachlässigkeit leiden (z.B. IoT)
Europäisch! → EU Produkte / Technologien Europäische Hersteller als Gegengewicht zu CISCO und Huawei Europäische digitale Souveränität	Härterer Schutz der Infrastruktur Geschäftsmodelle für KRITIS-Sabotagen kommen, wenn sie keiner stoppt
Sehr starke Serviceorientierung Out of the Box-Lösungen Stark Cloudbasiert Mühelose Integration Industrielles Prüfsiegel (nicht BSI!), weil andere Anforderungen Cloudsecurity Ausgefeiltere Tools auf Defence- und Angriffsseite	Sollte sehr stark KI getrieben sein  Mobil und sehr stark Cloud getrieben (um bewegliche Objekte zu schützen)  1. IoT Schutz komplett 2. intelligente Cloud Layouts zulassen (I4.0) 3. Biometrie, aber transparent  Identifikation im Bereich I4.0
Architektur wird sich im DAX7 stark ändern → starkes Identity Management SAP in Verbindung mit AD und IAM (als Kern) Möglicherweise eine Verlagerung des gesamten Rechenzentrums in eine Cloud	Alles wird auf Personen heruntergebrochen sein: Fingerprint, Gesichtserkennung  Gutes Personal um die Maschinen zu steuern („Robowars“)
Mitarbeiter ist zentrales Thema Heute technischer Schutz dann nicht leistbar (Stuxnet, Bundestrojaner, ...) Große Masse der Bedrohungen bewältigen	Ganz sicher  Kommunikationslagebilder, bei Präventivem läuft man hinterher Robuste Software und Hardware
Sicherheit sollte primär in Services und Produkten integriert sein → diese Integration zu leisten will man schon heute nicht mehr Security muss eingebettet sein	Wir erreichen einen guten Sicherheitslevel Schutz vor möglichst allen Bedrohungen, so dass man Herr der Lage werden kann Potential Erkennung → SIEM
Viel proaktiver als heute Viel simpler: Weniger Produkte nutzen müssen Zentral gesteuert (weiter zentralisiert)	Wie geht die IT-Sicherheitsindustrie mit der Cloudifizierung um? DAX10 schließt in 5 Jahren die eigenen Rechenzentren
Integration Herausforderungen werden größer Komplexe Lösungen + komplexes Problem (→ Widerspruch) Gut. Sollten als eigenständige Businessabteilung im Unternehmen anerkannt und dotiert werden → organisatorische Einbindung → Gleichstellung mit Sales, IT, ...	Cloud (Rechenleistung) AI auf beiden Seiten Vollautonome Defense Vollautonome Hacker werden kommen  Es gibt einen Informationssicherheitsvorstand
<i>Delta zwischen 3-5 → 10+ Jahren (Interpretation)</i>	<ul style="list-style-type: none"> <li>▪ Vollständige Cloudifizierung im Gegensatz zur teilweisen Nutzung von Cloud-Diensten</li> <li>▪ Das vgl. mittelmäßige Sicherheitslevel von heute wird ein annähernd optimales Maß erreichen</li> <li>▪ Artificial Intelligence wird aus der Nische austreten und sowohl im Angriff als auch Verteidigung eingesetzt</li> <li>▪ Software und Hardware wird die heutige Robustheit deutlich übertreffen</li> <li>▪ Sicherheitsprodukte werden ein hohes Maß an Transparenz erreichen und für den Nutzer unsichtbar</li> </ul>

- Geschäftsmodelle von Angreifern werden sich professionalisieren und auf KRITIS ausgerichtet werden

Tabelle 23: Herausforderungen und IT-Sicherheit in 3-5 und 10+ Jahren

Des Weiteren wird den Herstellern in der nahen Zukunft eine sehr starke Serviceorientierung unterstellt. Auch die Verantwortung und Struktur innerhalb der Unternehmen wird sich bei dem Thema verändern. So wird die Sicherheit als eigenständige wichtige Institution wahrgenommen werden und die Verantwortlichkeit könnte dann bei einem eigens hierfür verantwortlichen Informationssicherheitsvorstand liegen.

### Verantwortung übernehmen: Aber wer?

Bei der Frage, wer für die IT-Sicherheit im Konzern zukünftig verantwortlich sein sollte, gab es sehr unterschiedliche Ansichten. Mehrere Personen sahen die Verantwortung unmittelbar beim CEO bzw. Vorstand, wobei auch ein Sicherheitsvorstand vorgeschlagen worden ist. Ebenfalls wurde die Position des CIO benannt, bei dem die Verantwortung gesehen wurde. Eine weitere Idee war die Verantwortung gänzlich dem CISO zu übertragen und auch ein entsprechendes unabhängiges eigenes Ressort im Unternehmen einzurichten.

Zudem wurde ergänzend zu den benannten Führungspositionen, die zukünftige Verantwortung für IT-Sicherheit bei jedem einzelnen Nutzer im Unternehmen gesehen.

### Implikationen

- ▶ Die Großanwender sollten im Hinblick auf die steigende Wichtigkeit des Themas IT-Sicherheit über ein eigenes Ressort und die Benennung eines IT-Sicherheitsvorstandes nachdenken
- ▶ Allen Nutzern im Unternehmen muss deutlich klargemacht werden, dass sie einen bedeutenden Anteil der Verantwortung bei der Informationssicherheit mittragen
- ▶ Die IT-Sicherheit wird zukünftig europäisch werden, was auch im Hinblick auf eine mögliche Marktkonsolidierung betrachtet werden sollte
- ▶ IT-Sicherheit wird in Zukunft proaktiver, simpler, zentral gesteuert und hoch kollaborativ sein
- ▶ Rechenzentren werden Schritt für Schritt vollständig in die Cloud verschoben, daher sollte die IT-Sicherheitsbranche sich die Frage stellen, ob sie passende Lösungen dafür hat

#### 4.5.4 Beurteilung der Leistung von Behörden (BSI, BKA, LKA, Polizei)

Sicherheitsbehörden spielen im realen Leben unter anderem eine sehr wichtige Rolle im Hinblick auf Prävention und Aufklärung von Straftaten, doch wie ist die erbrachte Leistung und Wahrnehmung der Großanwender im Bereich der IT-Sicherheit? Dies wurde in diesem Bereich adressiert und es wurden dazu zwei Fragen formuliert. Die erste ging der Frage nach, ob die Großanwender der Meinung sind, dass die Behörden einen ausreichenden Beitrag im Bereich der PRÄVENTION liefern. Im zweiten Schritt wurde gefragt, ob der Beitrag im Bereich der AUFKLÄRUNG von Vorfällen ausreichend ist. Die Antwortmöglichkeiten waren hierbei jeweils *leisten sehr gute Arbeit*, *leisten gute Arbeit*, *leisten weniger gute Arbeit* und *leisten keine gute Arbeit*.

Die Leistungsbewertungen der Behörden fielen den befragten Anwendern insgesamt nicht einfach und sind unbedingt sehr differenziert zu betrachten. Aus diesem Grund wurden auch mehrere Kategorien durch einzelne Anwender bewertet, da es hier in den verschiedenen Bereichen und Behörden deutliche Gefälle gibt. Diese wollten die Bewertenden an einigen Stellen unbedingt zum Ausdruck bringen, um ihre vergebenen Bewertungen transparenter zu gestalten.

Bei der Bewertung wurde nach einer Einschätzung der gesamten Arbeit über alle Behörden hinweg gefragt. In einzelnen Fällen wurden jedoch abweichend von der Gesamtbeurteilung zusätzlich auch andere Bewertungen in Abhängigkeit zur einzelnen Behörde vergeben. Diese sind in der rechten

Spalte dokumentiert. Dabei handelt es sich um explizite Angaben, die dokumentiert wurden, sofern welche gemacht worden sind.

### Beurteilung der Leistung im Bereich der Prävention

Die nachfolgende *Tabelle 24* stellt die Bewertungen für den Bereich der präventiven Arbeit dar. Dabei wurden den Behörden unterschiedliche Leistungen bescheinigt.

Der Bereich sehr gut hat insgesamt sehr wenig Zuspruch erhalten (6%) und wie den Anmerkungen zu entnehmen ist, bezieht sich diese positive Beurteilung nur auf die Arbeit des BSI.

Im Bereich guter Arbeit ist deutlich mehr Zuspruch zu finden (31%), wobei hier wiederum die Ergebnisse des BSI aber auch des LKA gewürdigt worden sind. Zudem gab es auch einen Teilnehmer, der dies in Form einer Gesamteinschätzung bewertet hat.

In der Kategorie weniger guter Arbeit beträgt die Quote insgesamt 38% der gegebenen Antworten und liegt damit, wenn auch nur geringfügig, an der Spitze. Hierzu sind keine weiteren Anmerkungen gemacht worden, die diese Entscheidungen begründen. Trotzdem ist mehrfach geäußert worden, dass die Tendenz in Richtung guter Arbeit geht – wie gesagt: Leider nur tendenziell.

Im Bereich der keinen guten Arbeit finden sich 25% der Bewertungen wieder. Hier bekommen insbesondere das BKA und die Polizeibehörden eine Erwähnung. Auch das LKA findet hier einmalige Erwähnung. Die Begründung lautet dabei insgesamt, dass die Behörden schlicht und einfach keine angemessene Arbeit leisten, wobei hier *angemessen* ausschlaggebend war.

Prävention				
Leisten sehr gute Arbeit		6%	1x <i>Hauptsächlich BSI</i>	
Leisten gute Arbeit		31%	1x <i>Hauptsächlich BSI</i> , 1x <i>Lagezentrum LKA</i> , 1x <i>Insgesamt betrachtet</i>	
Leisten weniger gute Arbeit		38%	-	
Leisten keine gute Arbeit		25%	1x „ <i>keine angemessene</i> “, 1x <i>LKA, BKA und Polizei</i> , 1x <i>Polizei</i>	
<i>Summe</i>		100%		

Tabelle 24: Beurteilung der Behördenleistung im Bereich der Prävention

Insgesamt gibt es im Bereich der Prävention in den verschiedenen Behörden in jedem Fall noch Potential nach oben. Die Teilnehmer sind an einer erfolgreichen Zusammenarbeit interessiert und für eine intensivere und produktive Arbeit offen. Diese sollte jedoch transparent, ausgeglichen und für alle Seiten zum Vorteil sein.

### Beurteilung der Leistung im Bereich der Aufklärung

Bei der Beurteilung der Behördenarbeit im Bereich der Aufklärung von Vorfällen, sind die Beurteilungen der einzelnen Behörden etwas anders gelagert. Diese sind in der nachfolgenden *Tabelle 25* dargestellt. Auch hier wurden die einzelnen ergänzenden Angaben in der rechten Spalte dokumentiert.

Aufklärung				
Leisten sehr gute Arbeit		12%	1x <i>Hauptsächlich BSI</i>	
Leisten gute Arbeit		6%	1x <i>BKA</i>	
Leisten weniger gute Arbeit		47%	1x <i>BKA und LKA</i> , 1x <i>LKA</i>	
Leisten keine gute Arbeit		35%	1x „ <i>keine angemessene</i> “, 1x <i>Polizei</i> , 1x <i>BSI und Polizei</i>	
<i>Summe</i>		100%		

Tabelle 25: Beurteilung der Behördenleistung im Bereich der Aufklärung

Sehr gute Arbeit bescheinigten den Behörden 12% der Befragten, wobei hier das BSI positiv hervorgehoben wurde.

Weitere 6% sehen die Arbeit als gut an, wobei hier in dieser Kategorie explizit die Leistungen des BKA gemeint sind, basierend auf den mit dieser Behörde gemachten Erfahrungen.

Im Bereich weniger guter Arbeitsergebnisse urteilten mit 47% die meisten der befragten Personen. In dieser Kategorie wurden insbesondere das BKA und mehrfach das LKA benannt.

Aus Sicht der Großanwender leisten 35% der Behörden eher keine gute Arbeit im Bereich der Aufklärung von Vorfällen, wenn auch hier die Tendenz in einzelnen Fällen immerhin zu weniger gut tendierte. Hierbei wurde einmalig angemerkt, dass die Arbeit einfach „nicht angemessen“ sei. Weiterhin wurde zweimal die Polizei und einmal das BSI für diese Kategorie nominiert.

Als negativ wird die Zusammenarbeit mit einigen Behörden empfunden hinsichtlich des Austauschs von Informationen: Die Unternehmen haben das Gefühl, dass Sie sich in einigen Fällen breit öffnen, um zu helfen. Sie liefern in diesem Fall verhältnismäßig viele Informationen, die Behörden geben daraufhin dann aber sehr wenig dafür zurück.

Gesamtheitlich betrachtet ist die Bewertung der Behörden aus verschiedenen Perspektiven, Positionen und Branchen zu berücksichtigen. Zudem spielt hier auch in einigen Fällen auch der regionale Charakter der Behörden eine Rolle, daher ist von einer Verallgemeinerung Abstand zu nehmen. Trotzdem lässt dieses Ergebnis den deutlichen Schluss zu, dass es hier an vielen Stellen Verbesserungspotentiale gibt.

#### 4.5.5 Verantwortung des Staates und seine Aufgaben

In gesellschaftlicher und regulierender Hinsicht hat der Staat eine Verantwortung gegenüber seinen Bürgern und Unternehmen, die er auch wahrnehmen muss. Dementsprechend wurde gefragt, welche Aufgaben der Staat in Zukunft übernehmen sollte. Mögliche Antworten dabei waren *Regulierung, Aufklärung von Vorfällen, Lagebilddarstellung und Prävention*.

Die zu dieser Frage gegebenen Antworten werden in der nachfolgenden *Tabelle 26* gegenübergestellt. Das Thema der Regulierung erhält mit 17% den niedrigsten Zuspruch. Insgesamt waren die meisten Teilnehmer der Ansicht, dass der Staat bei den Themen der Regulierung Zurückhaltung üben sollte. Im Falle einer Regulierung sollte sich diese auf Hersteller und KRITIS konzentrieren, nicht jedoch auf die Anwender.

Die Aufklärung von Vorfällen wurde mit 33% am wichtigsten bewertet. Diese sollte zukünftig von internationaler Tragweite sein. Dabei ist der Wunsch nach Unterstützung durch die entsprechenden Behörden, trotz der zuvor diskutierten Ergebnisse, insgesamt groß.

Welche Aufgaben sollte der Staat in Zukunft übernehmen?			
Regulierung		17%	
Aufklärung von Vorfällen		33%	
Lagebilddarstellung		25%	
Prävention		25%	
Summe		100%	

Tabelle 26: Zukünftige mögliche Aufgaben des Staates

Des Weiteren sind die Themen der Lagebilddarstellung und Prävention mit jeweils 25% ebenfalls als wichtig zu bewerten. Hier kann der Staat durchaus sinnvoll handeln, ohne regulierende Maßnahmen zu ergreifen – Mit Hilfe der Forschung zum Beispiel. Das große Thema, welches auch die Großanwender bewegte, ist die Awareness der Nutzer. Diese muss nicht nur weiter ausgebaut, sondern auch auf einem konstant hohen Niveau verankert werden. Auch hier ist eine mögliche internationale Tragweite gewünscht worden.

Um dieser Herausforderung zu begegnen, bedarf es informativer, gut aufbereiteter, professioneller und leicht zugreifbarer Informationen. Hier ist beispielsweise ein durch das Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen gefördertes Forschungsprojekt Cyberschutzraum<sup>25</sup>, praktisch der 7. Sinn im Internet, ein entsprechendes Vorhaben. Die bisherigen Beiträge, die mit Zusammenarbeit von BSI, Polizei und der Verbraucherzentrale NRW entstehen, beschäftigen sich mit aktuellen Problemen und Themen aus dem Bereich der IT-Sicherheit. Sie nehmen Bezug auf aktuelle Geschehnisse und bereiten das Thema kompakt, spannend und dennoch informativ auf.

Bei Lagebildern könnten Zusammenschlüsse regionaler Lagebildzentren helfen, umfangreiche Daten für ein konkretes gesamtheitliches Lagebild zu liefern. Diese sollten jedoch zweckdienlich und vor allem aussagekräftig sein. Auch hier könnte der Staat dabei helfen mit Hilfe von Förderung entsprechender Forschungsprojekte ein solches ehrgeiziges Vorhaben umzusetzen.

### Implikationen

- ▶ Die wichtigste zukünftige Rolle des Staates, die er in Zukunft stärker und effektiver ausgestalten muss, ist die Aufklärung von Vorfällen
- ▶ Die Darstellung von Lagebildern und Prävention sind wichtige Themen, die zukünftig stärker durch den Staat umgesetzt werden müssen
- ▶ Es sollte nur dann Regulierung stattfinden, wenn ausdrücklich darum gebeten wird

### 4.5.6 Verschlüsselung vs. Backdoors

Hintertüren in sicherer Verschlüsselung ist aktuell immer wieder ein Thema. Dabei birgt die absichtliche Schwächung von Kryptografie viele Risiken und hätte weitreichende Konsequenzen. Reflektierend zu der stattfindenden öffentlichen Diskussion wurden den teilnehmenden Großanwendern zwei zentrale Fragen gestellt. Zum einen, ob es mehr und einen breiteren Einsatz von Verschlüsselung geben sollte. Zum anderen wurde die Meinung abgefragt, ob der Staat die Möglichkeit erhalten sollte, reguliert alles entschlüsseln zu können. Die jeweiligen Antworten zu dieser Fragestellung sind in der nachfolgenden *Abbildung 23* dargestellt.

Bei den Antworten auf die erste Frage, ob es einen bereiteren Einsatz von Verschlüsselung geben sollte, antworteten 92% (11) der Befragten mit Ja. Hier wurde auch angemerkt, dass dies nur dann in Frage käme, wenn die Verschlüsselung homomorph wäre<sup>26</sup> – insbesondere im Kontext der bevorstehenden Cloudifizierung. Homomorphe Verschlüsselung bedeutet im Detail Datenoperationen unmittelbar auf den verschlüsselten Daten durchführen zu können. Bei dieser Technologie steht die Branche noch recht am Anfang aber es gibt hier bereits vielversprechende Ansätze. Lediglich einer der Teilnehmer (8%) hat diese Frage mit Nein beantwortet.

---

<sup>25</sup> Cyberschutzraum: Der 7. Sinn im Internet - Raum für mehr Sicherheit,

URL: <https://www.cyberschutzraum.de>

Stand: 15.07.2017, Zuletzt abgerufen: 15.07.2017

<sup>26</sup> ct Magazin: Rechnen mit sieben Siegeln - Verschlüsselt rechnen mit homomorpher Verschlüsselung,

URL: <https://www.heise.de/ct/ausgabe/2016-6-Verschlüsselt-rechnen-mit-homomorpher-Verschlüsselung-3119044.html>

Stand: Juni 2016, Zuletzt abgerufen: 15.07.2017

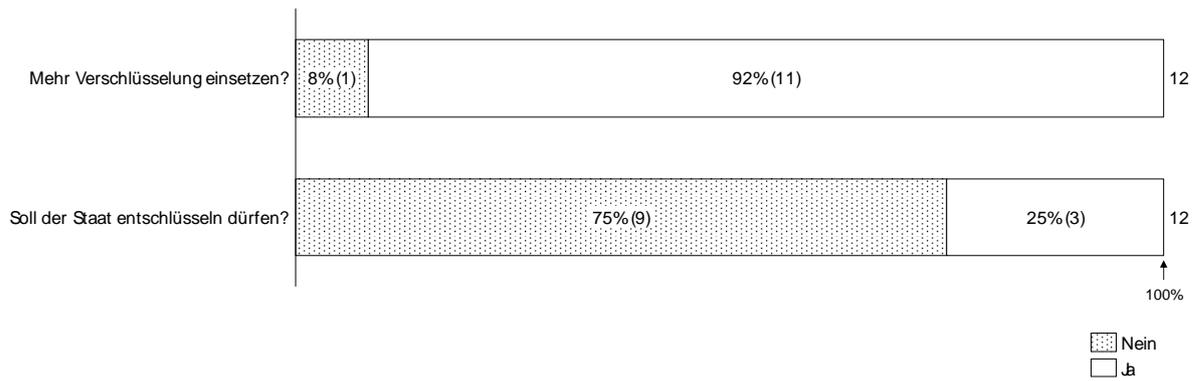


Abbildung 23: Abfrage nach einem breiteren Einsatz von Verschlüsselung und der regulierten Entschlüsselung durch den Staat

Bei der Frage, ob der Staat alles entschlüsseln dürfe, wenn auch reguliert, lagen die Antworten ein wenig anders gelagert. Immerhin 25% (3) der Befragten haben sich dafür ausgesprochen. Das Begründen waren dabei die sonst stattfindende „Entmachtung des Staates“ bzw. ausschließlich auf richterlichen Beschluss hin. Über die tiefergehenden Gründe respektive eine Diskussion über Missbrauch und Spionage konnte in dem Kontext leider aus zeitlichen Gründen nicht geführt werden.

Insgesamt 75% (9) der Befragten und damit der Großteil hat sich ausdrücklich gegen die Entschlüsselung durch den Staat ausgesprochen – unabhängig davon ob reguliert oder nicht. Auch ein Grund für die Ablehnung ist die klare politische und gesellschaftliche Position zu einem sehr hohen Niveau in diesem Bereich. Diese heute beinahe einzigartige Strategie der harten Kryptografie ohne Hintertüren spielt sowohl national als auch weltweit durchaus eine wichtige Rolle für Deutschland.

### Implikationen

- ▶ Es muss zukünftig ein breiteres Angebot an leicht nutzbaren Krypto-Produkten geben, damit diese breiter eingesetzt werden können
- ▶ Eine Entschlüsselung durch den Staat wird vom Großteil deutlich abgelehnt, denn bei Vorfällen und einer notwendigen Kooperation mit Behörden und Staatsanwaltschaft, verweigert niemand diesen den Zugriff auf verschlüsselte Daten
- ▶ Die Möglichkeit einer Entschlüsselung durch Dritte kann zum Missbrauch führen und stellt ein unberechenbares Risiko für eine Wissensgesellschaft dar

#### 4.5.7 Beurteilung der aktuellen IT-Sicherheitslage

Für diesen Abschnitt wurden die Großanwender gebeten die allgemeine Sicherheitslage für die kommende Jahresperiode zu beurteilen bzw. eine Tendenz abzuschätzen. Die möglichen Antworten waren dabei *besser*, *bleibt gleich* und *schlechter*.

Wie in *Abbildung 24* ersichtlich, ist der Großteil mit 75% (9) davon überzeugt, dass sich die IT-Sicherheitslage zunehmend verschlechtert. Lediglich einer (8%) ist der Meinung, dass sie gleich bleibt und 17% (2) sind optimistisch, dass eine Verbesserung eintritt.

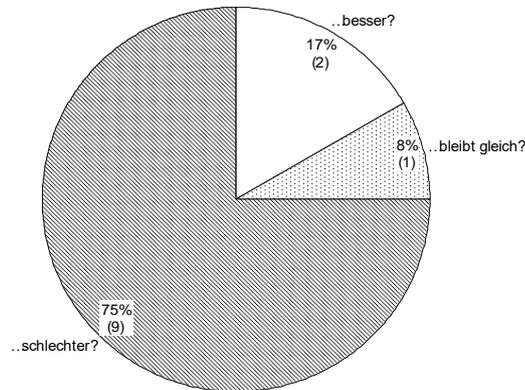


Abbildung 24: Beurteilung der jährlichen IT-Sicherheitslage und ihrer Tendenz

Die Einschätzung spiegelt durchaus die Realität wieder, denn die weltweiten Cyberangriffe auf Firmen und Behörden nehmen im Augenblick deutlich zu<sup>27</sup>. Auch wenn insbesondere „WannaCry“ weniger eine Cyberattacke und mehr ein Ausnutzen von Fahrlässigkeit im Patchmanagement der Opfer gewesen ist, so wird dank des medialen Echos und der breiten Wahrnehmung die Gefahr solcher Angriffe deutlich.

<sup>27</sup> Weltweite Cyberattacke: Massive Angriffe auf Firmen und Behörden,

URL: <https://www.tagesschau.de/wirtschaft/cyberangriff-123.html>

Stand: 28.06.2017, Zuletzt abgerufen: 15.07.2017

## 4.6 Bereitschaft zur Zusammenarbeit und Kooperation von Großanwendern

Dieses Kapitel beschäftigt sich mit der Bereitschaft einer möglichen Kooperation zwischen Großanwendern und der IT-Sicherheitsindustrie, Stichwort: Zusammenarbeit auf verschiedenen Ebenen zu verschiedenen Themen. Beispielsweise wurden Ideen und Wünsche hinsichtlich der Umsetzung einer solchen Kooperation erfragt und der Bereitschaft bei der Mitwirkung im Fall der Einführung von neuen und besseren IT-Sicherheitslösungen. Das Gleiche wurde auch in Bezug auf die Einführung von besseren Services und Kompetenzzentren erfragt.

Des Weiteren wurde auch thematisiert, wie die Bereitschaft für höhere Kosten ist, sofern größere Technologiesprünge gemacht werden könnten. Auch die Akzeptanz von Einschränkungen um Tausch für höhere Sicherheit und ein Bewusstsein zur eigenen Einkaufsmacht wurde am Ende abgefragt.

### 4.6.1 Zusammenarbeit mit IT-Sicherheitsherstellern und Umsetzungsideen

In diesem Bereich wurde die Frage nach der Bereitschaft gestellt, gemeinsam mit Herstellern Ideen und Konzepte von IT-Sicherheitslösungen zu erarbeiten. Zudem wurde gefragt, wie sich solch eine Kooperation bzw. Zusammenarbeit umsetzen lassen würde. Hier waren kreative Ideen der befragten erwünscht.

## Ja zur Zusammenarbeit: 100%

Im ersten Teil haben sich alle befragten Großanwender mit einem klaren Ja für die Zusammenarbeit mit den IT-Sicherheitsherstellern ausgesprochen.

Bei den Ideen, wie diese genau aussehen könnte, sind zum Teil sehr interessante Aspekte genannt worden. Allen voran die Idee Arbeitsgruppen zu gründen und Workshops zu veranstalten, um die Bedürfnisse und Anforderungen besser verstehen zu können. Die Großanwender könnten sich indes auch vorstellen, Zusammenschlüsse zu organisieren, um die Sicherheitsprodukte anschließend gemeinsam zu erwerben. In diesem Kontext ließen sich aus Sicht der Großanwender auch durchaus Forschungsprojekte umsetzen.

Das Format für eine Umsetzung wäre entscheidend, da zu viele Beteiligte den gesamten Prozess negativ beeinflussen könnten. Aus diesem Grunde würde es sich anbieten, Verbände für den Transport zu verwenden, da so eine 1:1 Kommunikation vermieden werden könnte. Es wäre möglich hier auch entsprechende themenspezifische Teams zu bilden, welche die jeweils relevanten Stakeholder berücksichtigen könnten. Auch das Format von Inhouse-Konferenzen und damit verbundenes gemeinsames Brainstorming wäre eine Möglichkeit.

Eine weitere interessante Idee war es, Großanwendern die Beteiligung in den Aufsichtsräten der IT-Sicherheitshersteller zu erlauben. Dies hätte eine durchschlagende Wirkung und könnte die Marktentwicklung der Hersteller prinzipiell durchaus in die gewünschte Richtung der Anwender steuern.

Da diese Art des Dialogs bisher gefehlt hat und die IT-Sicherheitsindustrie in diesem Bereich historisch gesehen sehr zurückhaltend gewesen ist, haben die Großanwender beschlossen selbst Schritte in Form der Gründung der bereits erwähnten DCSO zu unternehmen.

### Implikationen

- ▶ Ausnahmslos alle Großanwender haben sich für eine grundsätzliche Zusammenarbeit ausgesprochen
- ▶ Trotz unterschiedlicher Anforderungen sollte die Fokussierung eines Bereiches möglich sein, der sich bei allen Großanwendern wiederfindet – eben diesen gilt es zu adressieren
- ▶ Ein Arbeitskreis beim TeleTrusT e.V. zu diesem Thema befindet sich zum jetzigen Zeitpunkt bereits in der Gründung und nimmt in den nächsten Wochen seine Arbeit auf

#### 4.6.2 Bereitschaft bei der Mitwirkung der Einführung von neuen Lösungen, Services und Kompetenzzentren

Dieser Abschnitt beschäftigt sich mit der Bereitschaft, die Einführung von besseren IT-Sicherheitslösungen, Services und Kompetenzzentren gemeinsam mit anderen Großanwendern zu motivieren und koordinieren. Zudem wurde gefragt, ob dies bei den IT-Sicherheitslösungen innerhalb der Branche oder branchenübergreifend geschehen sollte. Weiterhin wurde gefragt, welche Services und Kompetenzzentren das im Einzelnen wären.

Bei der Frage nach der gemeinsamen Einführung von IT-Sicherheitslösungen mit anderen Anwendern (*Abbildung 25*), haben 83% (10) mit Ja geantwortet und 17% (2) lehnen dies ab. Zumindest einer dieser beiden hat das aber nicht dauerhaft ausgeschlossen und dies auf „im Moment nicht“ eingegrenzt.

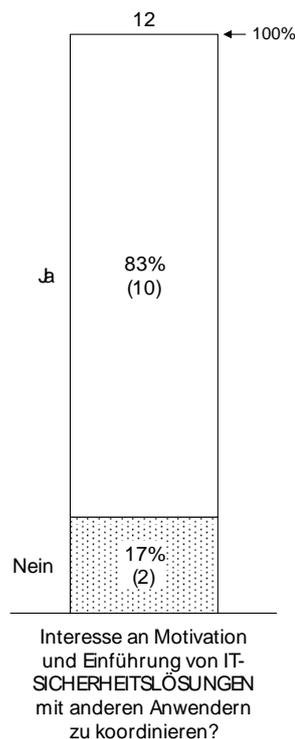


Abbildung 25: Interesse an Einführung von Sicherheitslösungen

Bei der Frage ob die Einführung von IT-Sicherheitslösung in der Branche oder eher branchenübergreifend durchgeführt werden sollte (*Abbildung 26*), gaben 33% (4) Befragte an, dies innerhalb der Branche tun zu wollen. Für eine branchenübergreifende Einführung stimmten 50% (6) der Befragten. Lediglich 17% (2) fanden „weder noch“ bzw. wollten keine Angabe dazu tätigen, da sie vorher bereits mit Nein gestimmt hatten.

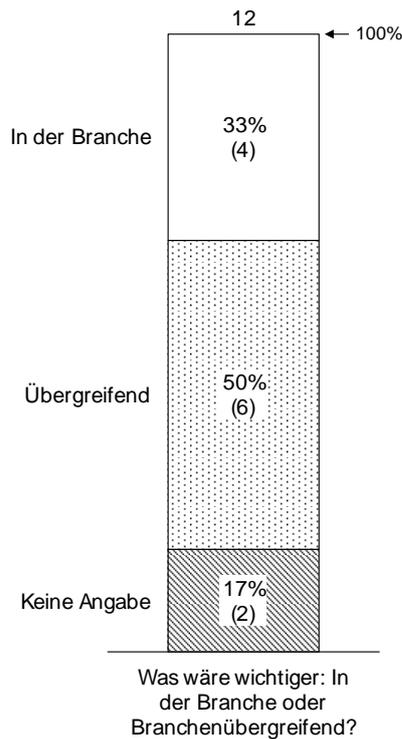


Abbildung 26: Einführung in der Branche oder branchenübergreifend

Die starke Befürwortung einer übergreifenden Einführung von IT-Sicherheitslösungen überrascht indes nicht, da sich dies auch positiv auf das Umfeld des jeweiligen Großanwenders auswirken kann.

Bei der Frage nach der gemeinsamen Einführung von Services und Kompetenzzentren waren sich die Anwender einig, daher decken sich die beiden in *Abbildung 27* und *Abbildung 28* dargestellten Ergebnisse. Hier gaben jeweils 92% (11) an, sich eine gemeinsame Einführung vorstellen zu können und lediglich 8% (1) lehnte dies ohne weitere Begründungen ab.

Bei den Services wurden die folgenden Ideen geäußert:

- Alle Themen, die mit Prävention zu tun haben
- Managed Security Services / Monitoring Services
- Gütesiegel und Zertifizierungen von Services
- (Security) Cloud Services
- Lagebilder, angepasst auf die jeweiligen Umgebungen
- Threat Intelligence, APT-Hunting und Active Response
- Austausch von Indikatoren
- RedTeam (Angriff) und BlueTeam (Verteidigung)

Im Bereich der Kompetenzzentren gab es die folgenden Ideen:

- Awareness
- Spezifische Themen aus der breiten Betrachtung aller Anwender
- Prävention
- Incident Reaction/Response/Handling
- Supply Chain Themen
- Cloud Themen
- Forensik
- EU-Weite Kooperationen als CERT-Verbund (z.B. SOC)

- ISMS für den Mittelstand, sowie kleinere Betriebe

Insgesamt sind die geäußerten Ideen nicht alle neu, jedoch in diesem Kontext bisher in dieser Form entweder so nicht umgesetzt oder finden nur in begrenzter Form Anwendung. Auch in diesem Bereich sind Themen wie Awareness und Reaktion bzw. Handling ganz zentral. Auch Lagebilder fanden hier Zuspruch.

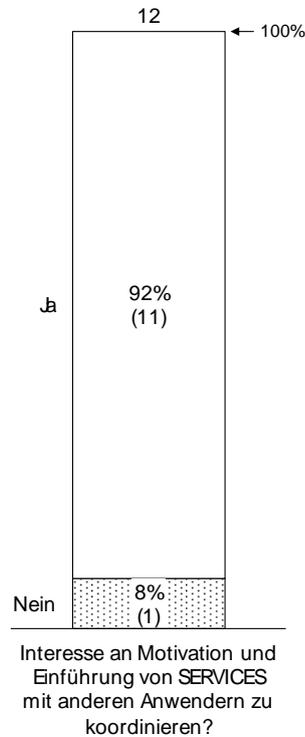


Abbildung 27: Interesse an gemeinsamer Einführung von Services

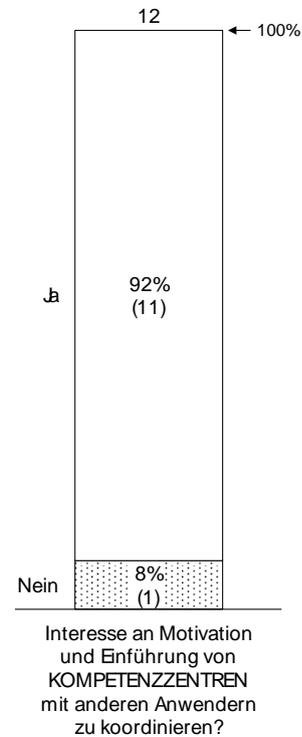


Abbildung 28: Interesse an gemeinsamer Einführung von Kompetenzzentren

Es lässt sich feststellen, dass es aktuell keine konkrete Zusammenarbeit gibt. Die Ergebnisse lassen jedoch den Schluss zu, dass eine zukünftige Zusammenarbeit in den verschiedenen Bereichen deutlich erwünscht ist. Dies belegen nicht nur die diskutierten Ergebnisse, sondern auch das am 20.03.2017 vorgestellte gemeinsame Thesenpapier „Das Manifest zur IT-Sicherheit – Erklärungen von Zielen und Absichten zur Erreichung einer angemessenen Risikolage in der IT“<sup>28</sup> des VOICE - Bundesverband der IT-Anwender e.V. und im Bundesverband IT-Sicherheit e.V. (TeleTrust).

Dazu haben sich die IT-Sicherheitsexperten aus beiden Verbänden zusammengetan, um die vorhandenen IT-Sicherheitsprobleme zu analysieren und Auswege aufzuzeigen, wie wir gemeinsam zu mehr IT-Sicherheit kommen können. [7, S. 2]

Basierend auf den hier dargestellten Ergebnissen und Thesen des Manifests wird deutlich, dass eine Zusammenarbeit zukünftig und dauerhaft etabliert werden muss. Nur so lassen sich die gemeinsamen Aufgaben, die in dieser Arbeit und dem Manifest zur IT-Sicherheit formuliert worden sind, lösen.

<sup>28</sup> VOICE - Bundesverband der IT-Anwender e.V., Bundesverband IT-Sicherheit e.V. (TeleTrust): Das Manifest zur IT-Sicherheit – Erklärungen von Zielen und Absichten zur Erreichung einer angemessenen Risikolage in der IT,

URL: [http://www.voice-ev.org/sites/default/files/IT%20Manifest%20Final%20096dpi\\_3.pdf](http://www.voice-ev.org/sites/default/files/IT%20Manifest%20Final%20096dpi_3.pdf)

Stand: 20.03.2017, Zuletzt abgerufen: 15.07.2017

### 4.6.3 Akzeptanz höherer Kosten für große Technologiesprünge

In diesem Abschnitt wurden die Großanwender gefragt, ob sie bereit wären für größere Technologiesprünge ein übermäßiges Budget zu investieren.

Wie in der nachfolgenden *Abbildung 29* dargestellt, ist ein Großteil der Befragten (75% / 9 Teilnehmer) durchaus bereit eine übermäßig hohe Investition zu tätigen. Hingegen gaben 25% (3) an, dies anders zu sehen und haben dies prinzipiell verneint. Einer dieser drei hätte aus persönlicher Sicht jedoch durchaus den Wunsch dies zu tun.

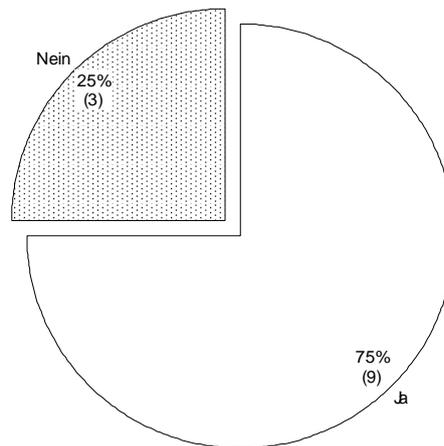


Abbildung 29: Bereitschaft für größere Technologiesprünge ein übermäßiges Budget zu investieren

Einer der Befürworter gab zudem ergänzend an, statt übermäßige hier eher größere Budgets zu meinen. Dies auch nur ausschließlich dann, wenn mit diesem Schritt gleichzeitig die gesamte Legacy-Landschaft abgelöst werden würde, mit dem Verweis auf das „Return on Investment“ Prinzip (ROI).

Dies zeigt, dass die Großanwender durchaus bereit sind, übermäßige Investitionen zu tätigen, sofern die hierfür notwendigen Technologien zur Verfügung stehen würden. Dies kann als eine Motivation für die Hersteller solcher Produkte verstanden werden, in naher Zukunft entsprechende Produkte und Services zur Verfügung stellen zu können.

#### Implikationen

- ▶ Hinsichtlich größerer Technologiesprünge müssen genaue Ziele definiert werden, die Großanwender bereit sind zu finanzieren
- ▶ Finanzieren die Anwender diesen Sprung, sind die Hersteller in der Pflicht entsprechende innovative Lösungen und Produkte zu liefern
- ▶ Hersteller und Anwender müssen einen gemeinsamen Weg beschreiten, damit wirklich größere Technologiesprünge entstehen können

#### 4.6.4 Akzeptanz von Einschränkungen im Tausch für höhere Sicherheit

Hier war eine mögliche Einschränkung der eigenen Nutzer das Thema. Konkret ging es darum, ob eine Reduktion von Freiheitsgraden und dem Erreichen eines höheren Sicherheitsniveaus, also dem Einsetzen von Hochsicherheitsprodukten, im eigenen Unternehmen durchsetzbar wäre.

Die Ergebnisse, wie in der nachfolgenden *Abbildung 30* dargestellt, teilen sich hier genau in 50% für Ja zu 50% für Nein. Im Allgemeinen ist dies realistisch betrachtet für wirkliche alle Bereiche selten denkbar, insbesondere für die allgemeinen umsatzgetriebenen. Innerhalb der IT-Kernbereiche und dem Schutz kritischer Bereiche ist dies deutlich einfacher durchsetzbar und finanziell argumentierbar.

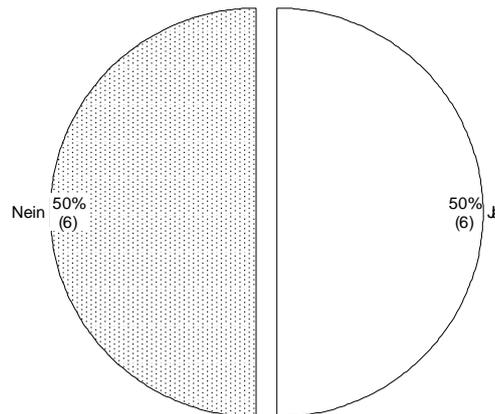


Abbildung 30: Akzeptanz von Hochsicherheitsprodukten für höhere Sicherheit mit gleichzeitiger Einschränkung von Freiheitsgraden der Nutzer

Auch wenn die Anwender dieser Idee aus der eigenen Perspektive durchaus positiv gegenüberstehen, so sehen sie hier im Hinblick auf ihre Kunden oder Supply Chain eher größere Schwierigkeiten.

Andere sehen das indes als ein schwieriges Thema, welches irgendwo zwischen einer liberalen und strikten Denkweise liegt, aus diesem Grund ist auch die Antwort in der Realität irgendwo zwischen Ja und Nein zu sehen. Einige gaben gleichzeitig an, dass dies leider fast nicht denkbar sei, auch wenn sie dies in manchen Bereichen stark begrüßen würden.

Der Wunsch nach einem breiteren Einsatz von Hochsicherheit ist zwar vorhanden, dies bleibt jedoch in den meisten Unternehmen aufgrund der Akzeptanz durch die Nutzer und den heute deutlich höheren Kosten ein Nischenthema.

#### 4.6.5 Beurteilung der Einkaufsmacht von Großanwendern

Durch die hohen IT-Budgets der Großanwender stellt sich die Frage nach einer möglichen Macht, durch Kauf oder bewussten Nichtkauf Dinge positiv oder negativ beeinflussen zu können. So beschäftigte sich die erste Frage damit, ob die Großanwender glauben, dass sie mit ihrem Einkauf die Macht haben, Dinge umzusetzen. Dem folgend wurde ergänzend gefragt, ob dies leichter wäre, wenn es die ganze Branche tun würde.

Die in nachfolgender *Abbildung 31* dargestellten Ergebnisse im Hinblick auf die eigene Einkaufsmacht zeigen einen überwiegenden Optimismus. Insgesamt glauben 58% (7) hier solch eine Macht zu besitzen Dinge umzusetzen. Jedoch sehen dies 42% (5) der Befragten anders und antworteten mit einem Nein. Diese Zahl fällt deutlich höher aus, als zunächst angenommen, da die DAX Konzerne über sehr große Budgets verfügen und für entsprechend hohe Summen jährlich Produkte einkaufen.

Aus diesem Grunde wurde im zweiten Schritt, bei der konkreten Frage, ob es einfach wäre, wenn es die ganze Branche tun würde, ein weiteres Meinungsbild abgefragt. Dieses ist in der nachfolgenden *Abbildung 32* dargestellt und zeigt eine massive Verschiebung zu Ja (92%, 11 Stimmen). Lediglich ein Teilnehmer hat hier mit Nein geantwortet und begründete dies gleichzeitig mit der Individualität der Entwicklungen und Entscheidungen.

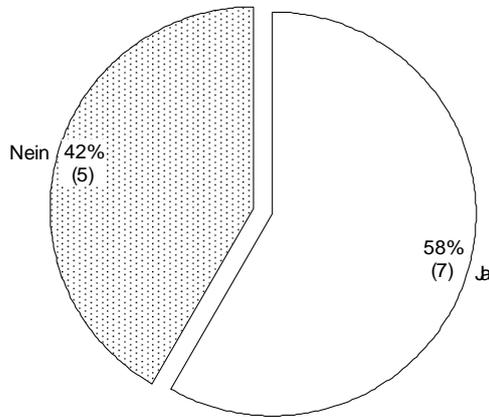


Abbildung 31: Glaube daran, mit dem eigenen Einkauf Macht zu haben Dinge umzusetzen

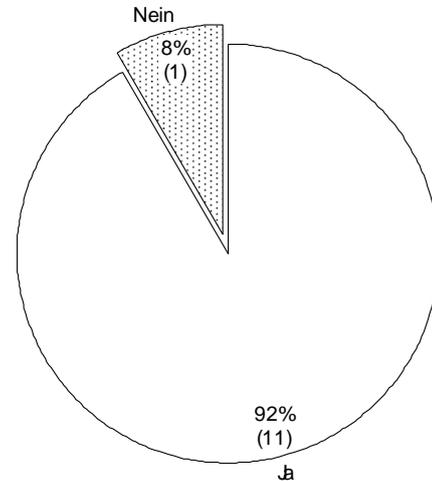


Abbildung 32: Glaube daran, mit dem Einkauf der gesamten Branche Macht zu haben Dinge umzusetzen

Das Gesamtergebnis zeigt sehr deutlich, dass die Großanwender sich ihrer finanziellen Macht durchaus bewusst sind. Dies spiegelt auch die These im Manifest wieder.

Die Großanwender sehen hier zusammenfassend Potential um die Anbieter am Markt entsprechend zukünftig beeinflussen zu können, frei nach dem Motto: Der Kunde ist König und was alleine nicht funktioniert, ist gemeinsam einfacher zu bewältigen.

#### Implikationen

- ▶ DAX Unternehmen verfügen im Schnitt über ein Einkaufsvolumen von 55,2 Mio. EUR, was auf alle DAX30 hochgerechnet einer Einkaufsmacht von schätzungsweise 1,656 Mrd. EUR pro Jahr entspricht
- ▶ Es sollte eine genaue Prüfung von möglichen Einkaufsgemeinschaften geprüft werden, um mit Hilfe des gemeinsamen Etats Dinge umsetzen zu können

#### 4.6.6 Gemeinsame Sicherheitsstrategie von Großanwendern und deren Messbarkeit

Sollen Dinge erfolgreich umgesetzt werden oder Ziele schnell und erfolgreich umgesetzt werden, ist eine konstruktive Zusammenarbeit der relevanten Stakeholder ein wichtiger Bestandteil. Aus diesem Grund wurde gefragt, ob eine gemeinsame Sicherheitsstrategie mit klaren messbaren Zielen zum Erfolg führen würde.

Die nachfolgende *Abbildung 33* zeigt eine deutliche Tendenz zu Ja (92%, 11 Stimmen). Die formulierte Idee wurde unkommentiert und deutlich befürwortet. Es gab aber eine Stimme, die das ganz anders sieht.

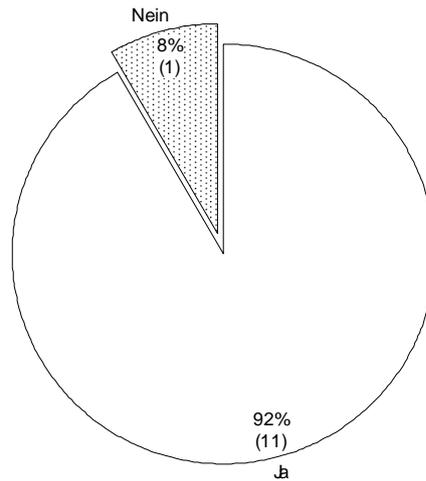


Abbildung 33: Antworten auf die Frage für den Erfolg einer gemeinsamen Sicherheitsstrategie

Ein Teilnehmer hat wie dargestellt mit Nein geantwortet und begründet dies mit den starken Divergenzen der jeweiligen Unternehmen. Aus seiner Sicht sollte solch eine Strategie immer individuell sein, da aus der unternehmerischen Perspektive unterschiedliche Kulturen mit verschiedenen Anforderungen aufeinandertreffen. Die Meinung, dass Unternehmen diametral zueinander sind ist, dass am meisten angeführte Argument, wenn es um Themen der Zusammenarbeit geht. Grundsätzlich ist jedoch anzunehmen, dass es möglicherweise bei genauer Betrachtung trotzdem Schnittpunkte gibt, die thematisch zu allen Unternehmen passen. Diese könnten erarbeitet und bei einer Umsetzung entsprechend berücksichtigt werden.

#### 4.6.7 Zusammenarbeit mit ausgewählten relevanten Stakeholdern

Basierend auf der Frage einer gemeinsamen konkreten Sicherheitsstrategie und der nötigen Kooperation der relevanten Stakeholder wurde gefragt, welche Stakeholder für eine Zusammenarbeit wichtig wären und mit welcher Gewichtung. Die möglichen Antworten waren dabei *Staat*, *Forschung*, *Industrie*, *Anwender* und *Politik*. Diese konnten mit Punkten bewertet werden: 0 Punkte = unwichtig, oder 1-3 Punkte, wobei 1 = wichtig, 2 = sehr wichtig und 3 = am wichtigsten repräsentiert. In der Gesamtheit wurden 119 Punkte vergeben, was in dieser Betrachtung 100 Prozent bedeutet.

In der nachfolgenden *Abbildung 34* sind die jeweiligen Ergebnisse der Punkteverteilungen dargestellt. Dabei zeigt sich, dass der Staat mit seinen regulatorischen Möglichkeiten den wenigsten Zuspruch erhält hinsichtlich einer gewünschten Zusammenarbeit. Sollte der Staat nämlich eingreifend aktiv werden, sehen hier die Befragten davon ausgehende Gefahren.

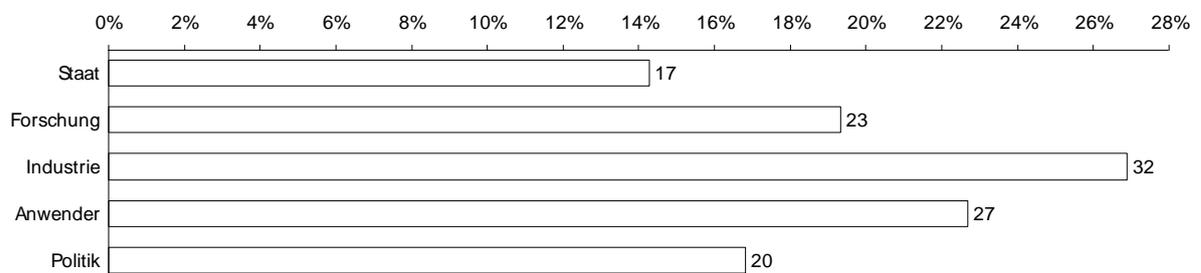


Abbildung 34: Relevanz der jeweiligen Stakeholder bei einer Zusammenarbeit in Prozent

Die Politik (Legislative) wird hier zum Großteil in einer anderen Rolle verstanden als der Staat (Exekutive) insgesamt. Hier spielen Fragen eine Rolle, die mit der stattfindenden Digitalisierung zusammenhängen. Die Politik wird auch als übergreifendes Bindeglied gesehen, denn bei den technologi-

schen Fragestellungen handelt es sich um neue gesellschaftliche Umstände, bei denen etwa auch die Perspektiven von Soziologen und Psychologen eine wichtige Rolle spielen.

Führend dabei ist die Rolle der Industrie mit 32% und die der Anwender mit 27%. Auch die Forschung wurde als ein sehr wichtiges Instrument gesehen und mit 23% bewertet. Diese kann dabei behilflich sein, Problemlösungen mit Hilfe neuer Ideen und Innovationen aufzuzeigen und umzusetzen.

Die Top 3 Bereiche sind demnach die Industrie, die Anwender und die Forschung, denen in der Weiterverfolgung dieses Themas besondere Beachtung geschenkt werden sollte. Im Falle einer Umsetzungsstrategie gilt es diese drei genannten Stakeholder in jedem Fall zur gemeinsamen Arbeit zusammenzubringen.

### Implikationen

- ▶ Eine gemeinsame Sicherheitsstrategie ist von fast allen Großanwendern gewünscht
- ▶ Es müssen Gemeinsamkeiten bei Problemen identifiziert werden, was bei einer Lösungsfindung breitere Unterstützung findet
- ▶ Wenn Stakeholder wissen, was das gemeinsame Ziel ist, ist eine Umsetzung einfacher
- ▶ Es besteht die Notwendigkeit eines „runden Tisches“ der drei wichtigsten Stakeholder: Forschung, Industrie und Anwender, wie bereits konzeptionell in der Vergangenheit in der „IT-Sicherheitsstrategie für Deutschland“ vorgeschlagen [8, S. 83]

#### 4.6.8 Identifikation von Gründen gegen eine Zusammenarbeit

Wird eine mögliche Zusammenarbeit verschiedener Parteien diskutiert, birgt diese Überlegung stets auch mögliche Gründe, die gegen eine Zusammenarbeit sprechen könnten.

Aus diesem Grund wurden die Befragten nach Aspekten gefragt, die aus ihrer Sicht gegen eine Zusammenarbeit sowohl mit anderen Anwendern als auch mit IT-Sicherheitsherstellern sprechen würden.

Nachfolgend werden die angeführten Bedenken gegenübergestellt und diskutiert, sofern es welche gab.

Zwei der Befragten sahen bei der Zusammenarbeit mit anderen Anwendern überhaupt keine Gründe, die dagegensprechen würden. Bei der Zusammenarbeit mit Herstellern sahen fünf der Befragten ebenfalls keinerlei Gründe, die im Widerspruch stehen könnten.

#### Gründe gegen die Zusammenarbeit mit anderen Großanwendern

Sofern Gründe geäußert worden sind, lagen diese meistens im Bereich der Wahrung von Geschäftsinteressen und Compliance. In erster Linie könnte also die Vertraulichkeitswahrung im Kontext dieses Themas ein Grund gegen eine Zusammenarbeit sein. Hier sind Wettbewerbseffekte relevant, die eine entscheidende Rolle spielen könnten. Nicht durchführbar, wenn also Geschäftsmodelle davon abhängen. Auch unterschiedliche Anforderungen und Reifegrade sprechen aus der Sicht eines Anwenders klar dagegen. Die notwendige Preisgabe von Firmeninterna und Wahrung von Vertraulichkeit verhindert ebenfalls eine mögliche Kooperation.

Im Bereich der Regulierung und Berichterstattung wird deutliche Skepsis sichtbar. Auch im Falle einer Öffnung gegenüber anderen wird eine große Gefahr gesehen, dass die Informationen schließlich in der Presse zu finden sind.

Eine Zusammenarbeit bedeutet auch gleichzeitig Aufwand und ist ein Zeitfaktor, was Ressourcen bindet. Eine Zusammenarbeit wäre nur in einem größeren Kreis möglich, was ineffizient und komplex werden würde. Es wirkt also verlangsamen auf die eigenen Prozesse und verkompliziert diese.

Bei den bestehenden Plattformen, wie CISO-Arbeitskreisen, tauschen sich die Personen ausschließlich über Sicherheitsthemen aus und keinesfalls über Produkte, das ist dann durchaus akzeptabel

Der Austausch endet genau an der Stelle, wo Produkte und Dienste ins Spiel kommen. Ist dies also völlig losgelöst davon möglich, ist das in Ordnung.

### Implikationen

- ▶ Aufgrund auch zukünftig der sehr begrenzten Anzahl an Experten, müssen Möglichkeiten gefunden werden, um dem zu begegnen
- ▶ Die gemeinsame Arbeit bei DCSO und CSSA ist ein wichtiger und sinnvoller Schritt, steht jedoch erst am Anfang
- ▶ Der CISO sollte zukünftig stärker in die Entwicklung der Geschäftsstrategie eingebunden werden und wird als Treiber für Innovationen wichtig
- ▶ Es müssen Branchenstandards getrieben werden, um sichere Produkte zu motivieren, Regulierung zu „verhindern“ – dies kann nur in Form einer (CISO) Kooperation unter den Großanwendern funktionieren
- ▶ Die Etablierung einer Shared Community kann Kosten „sozialisieren“ und dazu beitragen, Zugriff auf die sehr begrenzte Anzahl von qualifizierten Mitarbeitern zu erhalten (z.B. Forensik)

### Gründe gegen die Zusammenarbeit mit Herstellern

Auch bei der Zusammenarbeit mit IT-Sicherheitsherstellern wurden Vorbehalte geäußert, auch wenn diese deutlich weniger waren als bei der Kooperation unter den Anwendern.

Hauptsächlich sehen einige Großanwender die Hersteller als mögliche Wettbewerber. Im Rahmen ihrer Tätigkeiten fertigen auch die Anwender Sicherheitstechnologien. Der Aufgriff und die Monetarisierung könnte eine Hürde darstellen. Mögliche Interessenskonflikte sind ein großes Thema aber die IT-Sicherheitshersteller müssen trotzdem wissen, in welche Richtung die Entwicklung vorangetrieben werden soll, um die Bedürfnisse der Großanwender befriedigen zu können. Ergänzend dazu wurde argumentiert, dass der Anwender dem Hersteller beim „schleifen des Produktes“ hilft, davon jedoch nichts hat. Durch eine Beteiligung wird auch der Abfluss von Wissen an Dritte befürchtet und die Finanzierung der Lernkurve von Herstellern. Zwar ist das insgesamt eine Frage des Geschäftsmodells, aber die eigene „tolle Idee“ wird schlussendlich durch Dritte in der Breite vermarktet.

Die eigenen „Shopfloors“ wurde mit Nachdruck als „No Fly Zone“ bezeichnet. Damit ist gemeint, dass die eigene Fertigung absolutes Sperrgebiet darstellt. Eine Zusammenarbeit wäre demnach ausschließlich außerhalb dieses Bereiches und auch nur dann möglich, wenn keine Wettbewerbssituation entsteht. Des Weiteren ist die Skepsis groß, dass der Aufwand sehr groß sein könnte, aber die Erfolgsaussichten als relativ klein angesehen werden.

### Implikationen

- ▶ Es sollte im Kontext der Zusammenarbeit im ersten Schritt ein begrenzter Zeithorizont definiert werden (3 Jahre) mit dem ernsthaften Ziel, gemeinsam „die Welt positiv beeinflussen zu wollen“, um am Ende als CISO *besser schlafen* zu können, aufgrund der dann erreichten hohen Sicherheit
- ▶ Nach dem Ablauf des definierten Zeitrahmens kann über eine weitere Zusammenarbeit nachgedacht werden, oder es werden wieder unterschiedliche Wege beschritten

#### 4.7 Abschließende Message an die IT-Sicherheitsbranche

Am Ende der Befragung sollte den Gesprächspartnern die Möglichkeit eingeräumt werden, eine abschließende klare Message an die Anbieter von IT-Sicherheitsprodukten zu formulieren.

Diese Gelegenheit wurde durch die Befragten genutzt, um der IT-Sicherheitsbranche einige wichtige Nachrichten zukommen zu lassen.

---

Die gesamte Branche sollte sich zukünftig nicht so „still“ verhalten und mehr Präsenz zeigen, um deutlich sichtbarer zu werden, insbesondere der Vertrieb. Hier mangelt es deutlich an Präsenz, denn die Konkurrenz aus Übersee marschiert vergleichsweise täglich durch die Türen vor Ort. Weiterhin sollten nur wirklich ausgereifte Produkte angeboten werden und müssen dann auch 100% halten, was sie versprechen. Dies ist heute nicht der Fall. Es ist vollkommen klar, dass es keine „eierlegende Wollmilchsau“ gibt aber es lassen sich zukünftig hoffentlich ergänzende Produkte zu einer Gesamtlösung konsolidieren.

Darüber hinaus sind Produkte mit weltweiter Verfügbarkeit notwendig. Auch eine hohe Performance in Verbindung mit guter Qualität zu einem konkurrenzfähigen Preis ist gewünscht. Bei der Entwicklung von Produkten der nächsten Generation sollten die aufkommenden Trends genauestens beobachten werden. Hier sollte das Ziel sein, ein Trendsetter und kein Follower zu werden. Auch sollte ggf. über einen Kulturwechsel nachgedacht werden, hin zu mehr Risikofreudigkeit. Bei der Entwicklung neuer Dinge, sollte der Anbieter nicht „klassisch an der Sicherheit kleben“, sondern eine angemessene Sicherheit mit der Funktionalität verbinden.

Insgesamt sind die DAX-Konzerne auf einem guten Weg, was ihre Sicherheitsmaßnahmen betrifft. Die Mittelständler in ihrer großen Masse sind die nächst größere Herausforderung. Hier muss zukünftig deutlich mehr gemacht werden als heute. Auch im Kontext des IT-Sicherheitsgesetzes muss deutlich mehr getan werden. Weiterhin braucht es bessere und integrierte Lösungen mit weniger Komplexität. Im Detail müssen mehr wichtige spezifische Probleme aus dem Tagesgeschäft adressiert werden. Dabei sollte stets die Perspektive der CISOs eingenommen werden und ein Gefühl für seine Situation entwickelt bzw. berücksichtigt werden. Es muss dabei auch der Tatsache Rechnung getragen werden, dass er letztendlich auch nur über sehr begrenzte personelle, zeitliche und finanzielle Ressourcen verfügt. Es muss also zusammenfassend die besondere Perspektive des CISO für das Tagesgeschäft eingenommen werden.

Die IT-Sicherheitsbranche sollte sich genauestens anschauen, wohin sich die Architektur der Firmen entwickelt. Darüber hinaus sollten sich die Anbieter untereinander verständigen und Zusammenschlüsse bilden, um zu integrierten Lösungen zu kommen. Sicherheit muss als integrative Komponente der IT gesehen werden. Die IT-Sicherheitsbranche sollte sich umso mehr mit ihren Kunden beschäftigen und den Unterschied bzw. Zusammenhang zwischen Sicherheitslösung vs. Problemlösung aufarbeiten. Sie muss auch dabei behilflich sein, Bedrohungen und Sicherheitslöcher besser zu verstehen. Ebenso ist es auch wichtig dabei zu helfen, die entsprechenden Nachrichten an das Management zu transportieren. Dies muss in Zukunft deutlich erleichtert werden.

Jeder Verantwortliche hat seine eigenen Befindlichkeiten und ggf. gesetzlichen Auflagen. Es gibt keine Generalisten mehr, wie es vielleicht früher der Fall gewesen ist, heute sind es eher Spezialisten. Produkte und Lösungen, die sich überlappen, sind nicht optimal. Konfiguration einer Musterlösung ist schwierig und langwierig. Updates auszurollen ist komplex und haben manchmal generische Fehler zur Folge. Ebenfalls wäre die Möglichkeit einer zentralen Verwaltung erwünscht.

Es herrscht in der eigenen Branche ein sehr hoher Kostendruck aufgrund der Konkurrenzsituation und es gibt häufig Zeitmangel. Im Bereich der Sicherheit gibt es große Herausforderungen und es fehlt an bestimmten Lösungen, wie den wechselnden Identitäten (IAM), welche gut einsetzbar wären.

Die IT-Sicherheitsbranche sollte etwas bauen, wo die Sicherheit tatsächlich gesteigert wird und dabei gleichzeitig sichtbar wird, wie zum Beispiel der 3-Punkt-Gurt in Kraftfahrzeugen. Im Moment versteht man es nicht! Darüber hinaus sollten Start-Ups unbedingt den Kontakt zu den großen Anwendern suchen. Die Branche sollte insgesamt den Kunden zuhören. Das tut sie heute meist nicht.

Zudem sollte sie den Versuch unternehmen, deutlich mehr Vertrauen zu schaffen und den Versuch unternehmen, gemeinsame Entwicklungen voranzutreiben. Wichtige Punkte sind die Integrierbarkeit und Interoperabilität. Die Zusammenarbeit und der Austausch müssen in Deutschland besser werden, damit wir zusammen stärker und besser werden. Dies kann nur auf Basis einer vertrauensvollen Arbeit funktionieren. Die IT-Security benötigt innovative Produkte und mehr digitale Souveränität. Da die Technik heute nicht aus Deutschland kommt, sind Layer dazwischen für Sicherheit und Vertrauenswürdigkeit wichtig. Das TeleTrust-Konzept und die Idee der IT-Replaceability sind wichtig und erstrebenswert.

### Implikationen

- ▶ Die DAX Unternehmen bekommen ihre Sicherheit in naher Zukunft in den Griff und werden sie dann beim Mittelstand einfordern, dabei kann und muss die IT-Sicherheitsindustrie mit passenden Lösungen behilflich sein
- ▶ Es müssen integrative, qualitative und gut bedienbare Lösungen zur Verfügung gestellt werden
- ▶ Es braucht bessere und integrierte Lösungen mit weniger Komplexität
- ▶ Die IT-Sicherheitsbranche muss zukünftig deutlich selbstbewusster auftreten und vertriebllich mehr Präsenz an den Tag legen, als es heute der Fall ist
- ▶ Ziele lassen sich nur erreichen, wenn sie klar formuliert wurden und der Weg gemeinsam beschritten wird

## 5 Thesenpapier der Großanwender in Zusammenarbeit mit dem VOICE e.V.

Das vom VOICE – Bundesverband der IT-Anwender e.V. und dem TeleTrusT - Bundesverband IT-Sicherheit e.V. gemeinsam vorgestellte Thesenpapier [9] ist im Rahmen des Workshops „Digital Security“ im Rahmen des „VOICE ENTSCHEIDERFORUM: Innovation meets Operational Excellence: IT Applied“ in Wien (Abbildung 35) im September 2016 diskutiert und gemeinsam erarbeitet worden.

Es ist anschließend offiziell im Rahmen der Cebit 2017 an das Bundesministerium des Innern (BMI) in Person von BMI-Staatssekretär Klaus Vitt, sowie den Leiter der Stabsstelle IT- und Cybersicherheit Andreas Könen und Arne Schönbohm, dem Präsidenten des Bundesamts für Sicherheit in der Informationstechnik (BSI) übergeben worden.

Die Idee hinter diesem Dokument war es, eine öffentliche Erklärung der beiden Verbände und damit der dahinterstehenden Unternehmen zu formulieren. Diese Erklärung entstand unter der Zusammenarbeit von Experten aus beiden Verbänden und enthält im Ergebnis sechs zentrale Thesen inkl. der hierfür jeweils relevanten und zu lösenden gemeinsamen Aufgaben.

Im Kern lauten die sechs Thesen:

1. Ohne Sicherheit gelingt keine nachhaltige Digitalisierung!
2. Gemeinsam mehr wirkungsvollere IT-Sicherheitslösungen nutzen!
3. Verschlüsselung und Vertrauen sind die digitalen Werkzeuge für die informationelle Selbstbestimmung!
4. Security-by-Design, Privacy-by-Design und nachvollziehbare Qualitätssicherung sind unabdingbar!
5. Wir brauchen eigene Souveränität von IT-Sicherheitsinfrastrukturen!
6. Cyber-War, Cyber-Sabotage und Cyber-Spionage werden immer bedrohlicher!

Diese sechs zentralen Thesen spiegeln die Bedürfnisse und Denkweise der Großanwender, aber auch der IT-Sicherheitsbranche wieder und bilden einen Querschnitt durch beide Bereiche. Sie zeigen auf, welche Herausforderungen es gibt und wie diese gemeinsam bewältigt werden können.

Das Manifest steht als freier Download<sup>29</sup> im Internet zur Verfügung und stellt im Grunde genommen das Fundament dieser vorliegenden Arbeit dar. Es war der Motivator für die Erarbeitung eines entsprechenden Katalogs von Fragen und der Aufnahme eines Dialogs mit den Großanwendern.

Aus diesem Grund ist es bei zukünftigen Aktivitäten in diesem Kontext wichtig, dieses Dokument stets zu berücksichtigen.



Abbildung 35: 1. VOICE Entscheiderforum, Wien;  
Quelle: VOICE

<sup>29</sup> VOICE - Bundesverband der IT-Anwender e.V., Bundesverband IT-Sicherheit e.V. (TeleTrusT): Das Manifest zur IT-Sicherheit – Erklärungen von Zielen und Absichten zur Erreichung einer angemessenen Risikolage in der IT,

URL: [http://www.voice-ev.org/sites/default/files/IT%20Manifest%20Final%20096dpi\\_3.pdf](http://www.voice-ev.org/sites/default/files/IT%20Manifest%20Final%20096dpi_3.pdf)

Stand: 20.03.2017, Zuletzt abgerufen: 15.07.2017

## 6 Fazit

Ein Gesamtfazit zu ziehen im Hinblick auf die verschiedenen Positionen und Meinungen, ist aufgrund der Gesamtkomplexität eine Herausforderung. Die Hersteller von IT-Sicherheitsprodukten betonen stets, die Produkte sind qualitativ gut, preiswert und für jeden Bedarf vorhanden. Auch die Bedienbarkeit ist angemessen und der höherwertigen Sicherheit geschuldet. Die Großanwender sehen dies anders: Ihnen ist die Qualität zu niedrig, die Preise zu hoch und die Bedienfreundlichkeit verbesserungsbedürftig. Es wurde auch moniert, dass die Wirkung der Produkte entweder unzureichend oder nicht bewertbar ist. Produkte sind nicht international verfügbar und die Lizenzierungsmodelle nicht mehr zeitgemäß. Auch die durch die Hersteller propagierte Herkunft aus Deutschland spielt für die Anwender nur eine untergeordnete Rolle.

Es wurden viele Äußerungen und Bewertungen sowohl zu den IT-Sicherheitsherstellern als auch ihren IT-Sicherheitsprodukten getätigt, die es bei der Weiterverfolgung dieses Themas zu beachten gilt.

Aus diesem Grund sind die Anwender durchaus der Meinung, es müsse etwas getan werden, um die verbesserungswürdigen Punkte anzugehen und zwar gemeinsam. Klar ist, dass die Hersteller zukünftig stärker zuhören sollten. Dabei sollten sie stets die Anwender nach ihren Wünschen und Bedürfnissen fragen, um diese Antworten in maßgeschneiderte Lösungen einfließen zu lassen. Das Übergehen der Verantwortlichen und die direkte Kommunikation des Herstellers über das Management Board ist in jedem Fall unerwünscht.

Innovationen sind für die Großanwender ebenfalls ein sehr zentrales Thema. Durch bestehende Prozesse und die Struktur einer großen Organisation ist dort oft kein Raum für die nötige Agilität. Nichts desto trotz wünschen sich die Unternehmen die Umsetzung innovativer Ideen und neuer Denkansätze. In dem Kontext wünschen sich sie sich die stärkere Einbindung der Forschung. Hier entstehende Start-Ups sollten unbedingt den Kontakt zu den großen suchen und sich trauen mit Ihnen zu sprechen.

Sollten Normen und Standards entwickelt werden, müssten diese aus Sicht der Anwender auf europäischer Ebene entwickelt werden, um hier zum Tragen zu kommen. Diese Perspektive ist nachvollziehbar, da die DAX Unternehmen international aufgestellt und weltweit tätig sind. Aus diesem Grunde muss in größeren Dimensionen gedacht werden als üblich.

Insgesamt müssen sowohl die Anwender als auch die Hersteller erst einmal unter sich zueinander finden. Die Anwender müssen konkret formulieren unter welchen Bedingungen sie sich eine Kooperation genau vorstellen könnten und wie diese erwünscht wäre. Die Hersteller müssen etwas Ähnliches tun, sich jedoch auch Gedanken über die Möglichkeit der Marktkonsolidierung machen.

Es gilt zu verstehen, welche Schritte strategisch unternommen werden müssen, um das Portfolio an den Bedürfnissen des Marktes auszurichten und international tätig werden zu können.

Mit der Kleinteiligkeit des Marktes wird es nicht möglich sein, den großteiligen Markt national und vor allem international zu adressieren. Dies ist sicher keine einfache Aufgabe und womöglich mit der deutschen Unternehmenslandschaft gar nicht umsetzbar, aber es sollten zumindest ernsthafte Gespräche unter den Herstellern stattfinden, um die Befindlichkeiten zu ermitteln und Bereitschaften zu diskutieren.

Erfreulich war die breite Nutzung von Open Source, wie auch die Bereitschaft viel Geld für Förderung von Projekten zur Verfügung zu stellen. Es sollte sich ein Betriebsmodell für einen DAX 30 Open Source Fonds finden lassen, damit die meisten Konzerne sich bereit erklären, Investitionen zu tätigen.

Bei der Bewertung der Behörden lässt sich insgesamt nur sagen, dass es hier durchaus in vielen Bereichen Verbesserungspotentiale gibt. Zwar schneidet das BSI in der Bewertung vor den anderen

Behörden besser ab, aber insgesamt sehen hier die Anwender großen Spielraum für Verbesserungen.

An dieser Stelle sei auch noch einmal auf die Zusammenfassungen der jeweiligen Kapitel verwiesen, die noch einmal die wichtigsten Eckpunkte, Aussagen und Aspekte kompakt in verdichteter Form aufgreifen. Die Branche tut gut daran, sich diese genauestens anzuschauen.

#### ***@IT-Sicherheitsbranche***

Vielleicht gelingt es global gesehen auf diese Weise, in vielen Bereichen der Cyber Security, nicht länger als Follower aufzutreten, sondern in naher Zukunft die Rolle des Leaders zu übernehmen.

## 7 Ausblick

Die vorliegende Arbeit soll keinesfalls den Abschluss, sondern einen wichtigen Meilenstein darstellen. Die Mitarbeit der Verbände zeigt die Wichtigkeit des Themas, wie auch die Bereitschaft der Großanwender durch die Teilnahme an der Befragung. Es sollten und werden die Aktivitäten fortgeführt werden. Ein weiterer wichtiger Schritt ist die Gründung eines Arbeitskreises innerhalb von TeleTrust, an dem sich sowohl die Mitglieder als auch der Vorstand aktiv beteiligen werden.

Des Weiteren gab es weitere Workshops beim 2. VOICE Entscheider Forum<sup>30</sup> in Berlin im September des letzten Jahres 2017. Zudem ist auch der ASW e.V. an der Weiterentwicklung des Themas interessiert und wird hier in naher Zukunft ebenfalls weitere Workshops und Veranstaltungen durchführen.

Die Fortführung dieses Themas erlaubt viele weitere verschiedene Blickwinkel, sowie andere Dimensionen und eine Weiterverfolgung unter strategisch-technischen Aspekten im Rahmen einer Dissertation wäre möglich.

### Weitere interessante Aspekte

Bei der Durchführung der Auswertung haben sich interessante weiterführende Fragen ergeben. Beispielsweise die Pro Kopf Ausgaben in IT und IT-Sicherheit könnten vereinzelt tiefergehend untersucht werden. Dies würde jedoch einen genaueren Blick an genau dieser Stelle in den jeweiligen Organisationen erfordern. In diesem Zusammenhang wäre auch eine historische Entwicklung der jeweiligen Zahlen sehr interessant.

Weiterhin wäre die Analyse der getesteteten aber am Ende nicht beschafften IT-Sicherheitslösungen interessant, insbesondere die genauen Gründe.

Auch die Untersuchung der aktuellen Größe der IT-Sicherheitsbranche in Deutschland und Europa wäre durchaus interessant, unterfüttert mit allen wichtigen Kennzahlen, die für eine strategische Ausrichtung deutscher Anbieter wichtig sind. Nur wer den Markt wirklich versteht, kann ihn mitbestimmen. Ferner wäre die reale vollständige Anzahl an ArbeitnehmerInnen im Bereich der IT-Sicherheit und in der IT-Sicherheitsforschung ebenfalls sehr spannend.

In jedem Fall lässt sich sagen: Die Kooperation zwischen Anwendern und Herstellern wird wichtiger.

---

<sup>30</sup> Dieser Workshop hat bereits im Rahmen des 2. Entscheiderforums in Berlin stattgefunden und Auszüge der Ergebnisse wurden dort in anonymisierter Form präsentiert.

*» Wege entstehen dadurch, dass man sie geht. «*

*Franz Kafka*

## 8 Literatur

1. STEVE MORGAN. Cybersecurity spending outlook: \$1 trillion from 2017 to 2021 [online]. Cybercrime growth is making it difficult for researchers and IT analyst firms to accurately forecast cybersecurity spending. *CSO Online by IDG*, 15. Juni 2016, 2016. Verfügbar unter: <http://www.csoonline.com/article/3083798/security/cybersecurity-spending-outlook-1-trillion-from-2017-to-2021.html>
2. BUNDESVERBAND IT-SICHERHEIT E.V. (TELETRUST) / ZVEI - ZENTRALVERBAND ELEKTROTECHNIK- UND ELEKTRONIKINDUSTRIE E.V. *Stärkung vertrauenswürdiger IT-Infrastrukturen in Deutschland und Europa - Ein wichtiger Beitrag zur digitalen Souveränität*. Frankfurt am Main / München / Berlin, 11/2015.
3. BUNDESMINISTERIUM FÜR WIRTSCHAFT UND ENERGIE. *Kompetenzen für eine digitale Souveränität. Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie*. Berlin, 06/2017.
4. MICHAEL KROKER, MARK FEHR, JACQUELINE GOEBEL, MATTHIAS KAMP, RÜDIGER KIANI-KREß und FLORIAN ZERFAß. Veraltete IT: Die Geißel deutscher Unternehmen [online]. Hohe Kosten für Wartung und Instandhaltung. *Wirtschafts Woche*, 24. Juli 2015 [Zugriff am: 20. Juli 2017]. Verfügbar unter: <http://www.wiwo.de/unternehmen/it/veraltete-it-die-geissel-deutscher-unternehmen/12093342-all.html>
5. UWE BERND-STRIEBECK. *Advanced Cyber Defense im Spannungsfeld zwischen Compliance und Wirksamkeit*. München, 12. Mai 2014.
6. PROF. NORBERT POHLMANN. *Das Manifest zur IT-Sicherheit. Thesenpapier von TeleTrust und VOICE*. Essen, 29. Juni 2017.
7. SEBASTIAN BARCHNICKI. *IT-Sicherheitsstrategie für Deutschland. Wirkungsklassen von IT-Sicherheitsmaßnahmen für unterschiedliche Schutzbedarfe*. [https://www.teletrust.de/fileadmin/docs/IT-Sicherheitsstrategien/2015-Barchnicki-IT-Sicherheits-Wirkungsklassen\\_09-03-2015.pdf](https://www.teletrust.de/fileadmin/docs/IT-Sicherheitsstrategien/2015-Barchnicki-IT-Sicherheits-Wirkungsklassen_09-03-2015.pdf), 9. März 2015.
8. PROF. DR. NORBERT POHLMANN, VORSTANDSVORSITZENDER BUNDESVERBAND IT-SICHERHEIT E.V (TELETRUST) und DR. THOMAS ENDRES, VORSITZENDER DES PRÄSIDIUMS VOICE - BUNDESVERBAND DER IT-ANWENDER E.V. *Das Manifest zur IT-Sicherheit: Erklärung von Zielen und Absichten zur Erreichung einer angemessenen Risikolage in der IT. Für ein höheres Maß an IT-Sicherheit und Vertrauenswürdigkeit*. Berlin, 15. Dezember 2016.

## 9 Abbildungsverzeichnis

Abbildung 1: Gesamtmarkt DE für IT-Sicherheit nach Gesamtumsatz Mittelstand und DAX .....	3
Abbildung 2: Durchschnittliche Gegenüberstellung MitarbeiterInnen im Konzern: Gesamt vs. IT vs. IT-Security .....	16
Abbildung 3: Akzeptabler Aufpreis in % für höherwertige IT-Sicherheit .....	23
Abbildung 4: Beurteilung des TeleTrusT-Wirkungsklassenmodells durch die befragten Entscheider.....	24
Abbildung 5: Einflüsse auf die Beschaffung von IT-Sicherheitsprodukten .....	24
Abbildung 6: Relevanz beim Einsatz von IT-Sicherheitsprodukten durch die Mitbewerber .....	27
Abbildung 7: Einschätzung der eigenen Situation direkt zu den Mitbewerbern und zur gesamten Branche .....	28
Abbildung 8: Übersicht über den Einsatz von Kommunikationslagebildern.....	29
Abbildung 9: Übersicht über gemachte Erfahrungen mit Kommunikationslagebildern; (11 Teilnehmer, einer unkommentiert) .....	29
Abbildung 10: Bereitschaft einer Beteiligung an einem gemeinsamen Lagezentrum .....	29
Abbildung 11: DCSO Logo; Quelle: DCSO .....	30
Abbildung 12: Mitglieder der CSSA; Quelle: CSSA.....	30
Abbildung 13: Gegenüberstellung des Vertrauens in deutsche IT-Sicherheitsprodukte.....	34
Abbildung 14: Beurteilung der Vertrauenswürdigkeit in Form des IT Security made in Germany Siegels als entscheidender Aspekt .....	35
Abbildung 15: Beurteilung der Bedeutung von Start-Ups im Bereich der IT-Sicherheit .....	38
Abbildung 16: Bereitschaft der Großanwender, Produkte von Start-Ups zu erwerben.....	40
Abbildung 17: Beurteilung der Wichtigkeit von internationalem Support.....	42
Abbildung 18: Definition des Begriffs "International" im jeweiligen Kontext des eigenen Unternehmens. ....	43
Abbildung 19: Bevorzugte Art der einzusetzenden IT-Sicherheitslösung.....	43
Abbildung 20: Open Source Fond DAX 30: Teilnahme und Zuwendung mit einer grundsätzlichen Beteiligung.....	44
Abbildung 21: Beurteilung der Fragmentierung des IT-Sicherheitsmarktes .....	49
Abbildung 22: Wunsch nach Einsatz von mehr Hochsicherheitslösungen.....	52
Abbildung 23: Abfrage nach einem breiteren Einsatz von Verschlüsselung und der regulierten Entschlüsselung durch den Staat .....	61
Abbildung 24: Beurteilung der jährlichen IT-Sicherheitslage und ihrer Tendenz .....	62
Abbildung 25: Interesse an Einführung von Sicherheitslösungen .....	64
Abbildung 26: Einführung in der Branche oder branchenübergreifend .....	65
Abbildung 27: Interesse an gemeinsamer Einführung von Services.....	66
Abbildung 28: Interesse an gemeinsamer Einführung von Kompetenzzentren .....	66
Abbildung 29: Bereitschaft für größere Technologiesprünge ein übermäßiges Budget zu investieren.....	67
Abbildung 30: Akzeptanz von Hochsicherheitsprodukten für höhere Sicherheit mit gleichzeitiger Einschränkung von Freiheitsgraden der Nutzer .....	68
Abbildung 31: Glaube daran, mit dem eigenen Einkauf Macht zu haben Dinge umzusetzen.....	69
Abbildung 32: Glaube daran, mit dem Einkauf der gesamten Branche Macht zu haben Dinge umzusetzen .....	69
Abbildung 33: Antworten auf die Frage für den Erfolg einer gemeinsamen Sicherheitsstrategie .....	70
Abbildung 34: Relevanz der jeweiligen Stakeholder bei einer Zusammenarbeit in Prozent.....	70
Abbildung 35: 1. VOICE Entscheiderforum, Wien; Quelle: VOICE.....	75
Abbildung 36 - Wirkungsklassenmodell mit den 5 Wirkungsklassen, Quelle: TeleTrusT e.V. / S. Barchnicki .....	84

Abbildung 37 - Definition einer Wirkungsklasse im Detail, Quelle: Bundesverband IT-Sicherheit e.V. (TeleTrust) / S. Barchnicki..... 86

*Sofern nicht anders angegeben, entstammen alle dargestellten Abbildungen aus eigener Quelle.*

## 10 Tabellenverzeichnis

Tabelle 1: Gesamtliste der deutschen DAX30, Quelle: finanzen.net .....	5
Tabelle 2: An der Befragung beteiligte Unternehmen in alphabetischer Reihenfolge.....	6
Tabelle 3: An der Umfrage beteiligte Unternehmen in alphabetischer Reihenfolge und der jeweilige Umsatz in Mrd. EUR; Quelle: Statista .....	14
Tabelle 4: Anzahl der Mitarbeiter im jeweiligen an der Umfrage beteiligten DAX Konzern in alphabetischer Reihenfolge; Quelle: Fincancial Reports/Befragte.....	15
Tabelle 5: Schwerpunkte der befragten Unternehmen bei der IT-Sicherheit im Einzelnen.....	17
Tabelle 6: Schwerpunkte der befragten Unternehmen bei der IT-Sicherheit als Schwerpunkte.....	17
Tabelle 7: Antworten zu der Frage nach den heute genutzten Lizenzierungsmodellen.....	20
Tabelle 8: Antworten zu der Frage nach den zukünftig präferierten Lizenzierungsmodellen .....	20
Tabelle 9: Kriterien zur Beschaffung von IT-Sicherheitsprodukten .....	21
Tabelle 10: Die wichtigsten Kennzahlen im Überblick.....	26
Tabelle 11: Besondere Kompetenzen der deutschen IT-Sicherheitsindustrie .....	33
Tabelle 12: Darstellung Gründe der Entscheidung für oder gegen die deutsche IT-Sicherheit.....	35
Tabelle 13: Zusammengefasste Beurteilung und Gewichtung relevanter Kriterien von IT-Sicherheitsherstellern .....	36
Tabelle 14: Gründe für Beurteilung der Bedeutung von Start-Ups im Bereich der IT-Sicherheit.....	39
Tabelle 15: Gründe, die für oder gegen den Erwerb von Start-Up-Produkten sprechen .....	41
Tabelle 16: Wichtige Aspekte als Definition für Kriterien der Qualität .....	41
Tabelle 17: Gegenüberstellung der Stärken ausländischer Anbieter und der Wünsche an die deutsche Sicherheitsindustrie .....	42
Tabelle 18: Negative nervende Eigenschaften von IT-Sicherheitsprodukten.....	46
Tabelle 19: Erwartungen an die IT-Sicherheitsprodukte hinsichtlich Merkmalen.....	47
Tabelle 20: Erwartungen an die IT-Sicherheitshersteller hinsichtlich Merkmalen .....	48
Tabelle 21: Gegenüberstellung der Gründe für Akzeptanz von Risiken und Maßnahmen um diese zu tragen .....	50
Tabelle 22: Hürden gegen Hochsicherheit und mögliche Einsatzszenarien .....	53
Tabelle 23: Herausforderungen und IT-Sicherheit in 3-5 und 10+ Jahren.....	57
Tabelle 24: Beurteilung der Behördenleistung im Bereich der Prävention.....	58
Tabelle 25: Beurteilung der Behördenleistung im Bereich der Aufklärung.....	58
Tabelle 26: Zukünftige mögliche Aufgaben des Staates.....	59
Tabelle 27 - Wirkungsklassen: Definition von Begriffen aus Anwendersicht.....	86
Tabelle 28 - Wirkungsklassen: Definition von Begriffen aus Bedrohungsicht.....	86

*Hinweise: Sofern nicht anders angegeben, entstammen alle dargestellten Tabellen aus eigener Quelle. Die Reihenfolge der Angaben erfolgt in pseudonymisierter z.T. ungeordneter Reihenfolge.*

## 11 Appendix 1: Wirkungsklassenmodell

Nachfolgend finden Sie eine verkürzte Erläuterung des *Wirkungsklassenmodells*, entnommen aus dem ursprünglichen Konzeptpapier „*IT-Sicherheitsstrategie für Deutschland: Wirkungsklassen von IT-Sicherheitsmaßnahmen für unterschiedliche Schutzbedarfe - Ein Aspekt der IT-Sicherheitsstrategie für DE*“ des TeleTrust e.V. – dem Bundesverband der IT-Sicherheitsindustrie. [8]

### Wirkungsklassenmodell

Das in Abbildung 36 nachfolgend dargestellte Wirkungsklassenmodell“ besteht aus fünf aufeinander aufbauenden sogenannte Wirkungsklassen (0 bis 4).

Jede Klasse enthält neben den eigenen Objekten auch jene aus der darüberliegenden Klasse. So deckt beispielsweise die Wirkungsklasse 0 als Gefahren die Angriffe auf die Privatsphäre und Cybercrime ab, wohingegen die Wirkungsklasse 1 zusätzlich zu den Elementen der Klasse 0 auch Cybercrime mit höherem Gefahrengrad und den gesetzlichen Datenschutz berücksichtigt.

Die Beschreibung unmittelbar rechts neben dem farblichen Reiter, beschreibt die Zielgruppe, für welche sie den Schutzbedarf deckt.

Die betitelten Kosten für jede Wirkungsklasse ergeben sich in den einzelnen Fällen aus dem Grundpreis für die Anschaffung eines IT-Systems (z. B. PC). Diese sind hier als prozentuale Kosten des „Grundbetrags“ veranschlagt, um das IT-System dem Bedarf entsprechend schützen zu können.

<b>Wirkungsklasse 0</b>	<b>Bürger mit privater Nutzung</b>
<ul style="list-style-type: none"> <li>• Gefahren: Privatsphäre, Cybercrime</li> <li>• Kosten: Grundbetrag +5%</li> </ul>	
<b>Wirkungsklasse 1</b>	<b>Unternehmen, Organisationen, Behörden</b>
<ul style="list-style-type: none"> <li>• Gefahren: Privatsphäre, Cybercrime mit höherem Gefährdungsgrad, <u>gesetzlicher Datenschutz</u></li> <li>• Schutzbedarf: mittel</li> <li>• Kosten: Grundbetrag +10%</li> </ul>	
<b>Wirkungsklasse 2</b>	<b>Unternehmen, Organisationen, Behörden, Infrastruktur</b>
<ul style="list-style-type: none"> <li>• Gefahren: <u>Industriespionage</u>, gezielte Angriffe auf Werte des Unternehmens, Cybercrime</li> <li>• Schutzbedarf: hoch</li> <li>• Kosten: Grundbetrag +20%</li> </ul>	
<b>Wirkungsklasse 3</b>	<b>Unternehmen, Organisationen, Behörden, Infrastruktur</b>
<ul style="list-style-type: none"> <li>• Gefahren: Wirtschaftsspionage (Nachrichtendienste) und Cyberattacken, <u>Cyberwar (Sabotagen)</u></li> <li>• Schutzbedarf: sehr hoch, inkl. VS-NfD</li> <li>• Kosten: Grundbetrag +50%</li> </ul>	
<b>Wirkungsklasse 4</b>	<b>Verschlusssachen</b>
<ul style="list-style-type: none"> <li>• Nationale Sicherheit</li> <li>• Schutzbedarf: gemäß Geheimschutzordnung GSO, ab VS/V</li> <li>• Kosten: Grundbetrag +400%</li> </ul>	

Abbildung 36 - Wirkungsklassenmodell mit den 5 Wirkungsklassen, Quelle: Bundesverband IT-Sicherheit e.V. (TeleTrust) / S. Barchnicki

## Definition der Begrifflichkeiten

Nachfolgend werden die im Wirkungsklassenmodell verwendeten Begrifflichkeiten näher definiert, um Missverständnissen vorzubeugen und Klarheit hinsichtlich der einzelnen Grundbegriffe zu schaffen. In der ersten Kategorie wird in Tabelle 27 die Anwendersicht berücksichtigt.

### Anwendersicht

<b>Wirkungsklasse</b>	<p>Grad/Stufe, welcher/e eine bestimmte Wirkung definiert. Abhängig von der Stufe deckt eine Klasse einen bestimmten Schutzbedarf ab und berücksichtigt dabei bestimmte Zielgruppen. Es gibt verschiedene Prinzipien von Wirkungen, mit deren Hilfe sich eine bestimmte Bedrohungsart abwehren lässt.</p> <p>Die Hierarchie ist aufeinander aufbauend als Vererbung zu sehen, die nächst größere Klasse beinhaltet immer die Aspekte der nächst kleineren Klasse.</p>
<b>Schutzbedarf</b>	Definiert den Umfang und die Stufe der Notwendigkeit an Sicherheitsmaßnahmen, die ein Anwender benötigt.
<b>Privatsphäre</b>	Berücksichtigt den eigenen höchst privaten Raum eines Anwenders.
<b>Kosten</b>	Definiert die prozentual geschätzten Zusatzkosten, die zusätzlich zur Anschaffung eines IT-Systems entstehen.
<b>Bürger mit privater Nutzung</b>	Juristische Person als Arbeitnehmer oder Selbstständiger und dem Einsatz der IT „Zuhause“.
<b>Unternehmen</b>	Alle Unternehmen
<b>Organisation</b>	Repräsentiert einen Konzern oder einen gemeinsamen Verbund von verschiedenen Unternehmen.
<b>Behörde</b>	Staatliches Verwaltungsorgan bzw. Dienststelle.
<b>(kritische) Infrastruktur</b>	<p>Laut dem Bundesministerium des Innern (BMI) und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe werden folgende Bereiche als „kritische Infrastrukturen“ angesehen:</p> <ul style="list-style-type: none"> <li>▪ Energie (Elektrizität, Gas, Mineralöl)</li> <li>▪ Informationstechnik und Telekommunikation (Telekommunikation, Informationstechnik)</li> <li>▪ Transport und Verkehr (Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik)</li> <li>▪ Gesundheit (Medizinische Versorgung, Arzneimittel und Impfstoffe Labore)</li> <li>▪ Wasser (Öffentliche Wasserversorgung, Öffentliche Abwasserbeseitigung)</li> <li>▪ Ernährung (Ernährungswirtschaft, Lebensmittelhandel)</li> <li>▪ Finanz- und Versicherungswesen (Banken, Börsen, Versicherungen, Finanzdienstleister)</li> <li>▪ Staat und Verwaltung (Regierung und Verwaltung, Parlament, Justizeinrichtungen, Notfall-/ Rettungswesen einschließlich, Katastrophenschutz)</li> <li>▪ Medien und Kultur (Rundfunk (Fernsehen und Radio), gedruckte und elektronische Presse, Kulturgut, symbolträchtige Bauwerke)</li> </ul> <p>Aber auch ein Verbund von IT-Systemen, die für den Austausch von Informationen elementar sind.</p>
<b>Nationale Sicherheit</b>	Gewissheit der Gesellschaft geschützt zu sein vor der Gefährdung des Staates und seiner Bürger, wie z. B. vor Übergriffen durch Kriminelle, Terrorismus und andere Staaten.
<b>Verschlusssache</b>	Der Geheimhaltung unterliegende Information oder Dokument. Unterschiedliche Stufen möglich.
<b>VS-NfD</b>	Geheimhaltungsstufe: „VERSCHLUSSACHE – NUR FÜR DEN DIENSTGEBRAUCH“
<b>GSO</b>	Geheimchutzordnung, Gesetz zum Geheimschutz als Vorschrift für die zu treffenden Vorkehrungen.
<b>VS/V</b>	Geheimhaltungsstufe:

„VERSCHLUSSACHE – VERTRAULICH“

Tabelle 27 - Wirkungsklassen: Definition von Begriffen aus Anwendersicht

In der nun folgenden Tabelle 28 werden die Begriffe der Bedrohungen bzw. der Gefährdungen definiert.

**Bedrohungen und Gefährdungen**

Cybercrime	Computerkriminalität (z. B. Betrug, Phishing)
Cybercrime mit höherem Gefährdungsgrad	Computerkriminalität mit erhöhtem Schadenspotenzial (z. B. Sabotage, digitale Erpressung)
Gesetzlicher Datenschutz	Beinhaltet das Grundrecht auf informationelle Selbstbestimmung und den Schutz vor Missbrauch persönlich relevanter Daten. (Gehaltsdaten, Krankheitsdaten, Personaldate, ...)
Industriespionage	Gezielter Diebstahl von wichtigen Daten aus der Industrie wie Know-how, Pläne und Programmcode durch Konkurrenzunternehmen.
Gezielte Angriffe auf Werte des Unternehmens	Komplexe zielgerichtete Bedrohungen, die sehr punktuell durchgeführt werden und dadurch sehr schwer zu identifizieren sind.
Wirtschaftsspionage	Angriff und illegale Erbeutung von Informationen aus der Wirtschaft durch ausländische Nachrichtendienste.
Cyberattacken	Cyberangriff auf spezifische Bereiche einer Infrastruktur größeren Ausmaßes.
Cyberwar (Sabotage)	Cyberkrieg als alternatives Mittel zum Einsatz von Truppen, enormen finanziellen Mitteln und Waffen zur Durchsetzung von Zielen einer Regierung.

Tabelle 28 - Wirkungsklassen: Definition von Begriffen aus Bedrohungssicht

Die Wirkungsklasse im Detail: Nachfolgend werden die Wirkungsklassen im Detail diskutiert. Beleuchtet werden dabei sowohl die zu den jeweiligen Klassen gehörenden IT-Sicherheitsmaßnahmen, als auch die notwendigen personellen Maßnahmen.

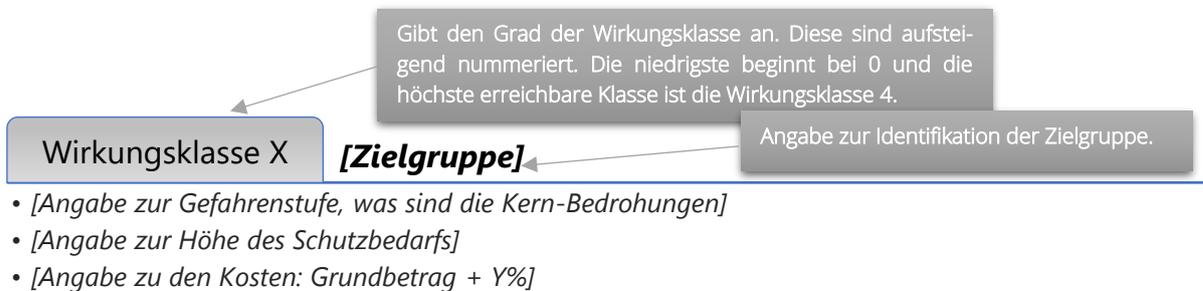


Abbildung 37 - Definition einer Wirkungsklasse im Detail, Quelle: Bundesverband IT-Sicherheit e.V. (TeleTRuST) / S. Barchnicki