Sebastian Barchnicki, Norbert Pohlmann

Was IT-Sicherheitsindustrie und Anwender voneinander lernen können

Die Kooperation zwischen Anwendern und Herstellern wird wichtiger.

Bei der heutigen und zukünftigen Rolle der IT und damit auch der IT-Sicherheit sind sich alle einig, dass ein hohes Sicherheitsniveau erreicht werden muss, um unseren Wirtschaftsraum und unsere Wissensgesellschaft zu schützen. Ideen, wie sich dies in der Breite umsetzen lässt, hat die „DAX 30 Studie" adressiert, die als Basis für diesen Beitrag dient. Für eine stichhaltige Datenbasis wurden persönliche Befragung der DAX30 CIOs und CISOs durchgeführt. Die Ergebnisse könnten interessanter nicht sein und bilden einen einzigartigen tiefen Einblick in die Denkweise, Bedürfnisse und Erwartungen der Anwender.

1 Einführung und Zielbestimmung

Im Sommer 2016 begannen die ersten Gespräche und Vorbereitungen für eine Studie im Bereich der Internet-Sicherheit, welche es bisher in dieser Form noch nicht gegeben hat. Die initiale Idee war ein Dialog zwischen dem Bundesverband IT-Sicherheit – TeleTrusT, dem Bundesverband der IT-Anwender– VOICE und dem ASW Bundesverband, der eine Allianz für Sicherheit in der Wirtschaft bildet. Das ganze Projekt wurde im Kontext einer möglichen Kooperation zwischen den Anwendern und der IT-Sicherheitsindustrie betrachtet. Für die Zielgruppe wurden die DAX30 ausgewählt und mit 12 Teilnehmern gelang es, die nachfolgenden 40% von ihnen zu adressieren: Allianz, Bayer, E.ON, Infineon, Lufthansa, Pro7Sat1, RWE, Siemens, thyssenkrupp, T-Systems/Telekom, Volkswagen und Vonovia.

Sebastian Barchnicki

war wissenschaftlicher Mitarbeiter am Institut für Internet-Sicheiheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen. Heute ist der im Bereich Unternehmensstrategie & Alliance Management bei der secunet Security Networks AG in Essen tätig. Hier beschäftigt er sich u.a. mit Themen rund um die heutigen und zukünftigen Herausforderungen im Bereich der IT-Sicherheit.
E-Mail: sebastian@barchnicki.de

Prof. Dr. Norbert Pohlmann

ist Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.
E-Mail: pohlmann@internet-sicherheit.de

1.1 IT: Grundpfeiler unserer Gesellschaft

Ein ganz zentraler Punkt ist die Rolle der IT: Die Unternehmenswelt besteht heute maßgeblich aus IT-Produkten, die 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 potenzielle 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.

1.2 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 sind die Wirtschaftskraft und das Wohlergehen unserer Gesellschaft sehr wichtig.

Mit Hilfe von Produkten, Lösungen und Services aus dem IT-Sicherheitsbereich lässt sich zwar den meisten Bedrohungen

entgegenwirken, aber eine vollständige IT-Sicherheit gibt es nicht. Ohnehin sollte es auch nicht das primäre Ziel sein, diese zu erreichen. Viel wichtiger ist es, IT-Sicherheitsmaßnahmen zu treffen und Prozesse anzupassen, um damit die Hürde für einen Angreifer so hoch wie nur möglich zu legen. Hierbei spielt der Faktor Mensch eine wichtige Rolle.

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 mit den ausländischen Marktführern, allerdings werden sie weniger häufig eingesetzt. Die starke Fragmentierung des IT-Sicherheitsmarktes in Deutschland und die sehr ingenieur-getriebenen Produkte sind dabei ein nicht unerheblicher Grund.

1.3 IT-Sicherheit made in Deutschland

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 äußerst divergent sein. Das prominenteste Beispiel ist die weltweit unterschiedliche Sicht auf die Stärke der einzusetzenden Verschlüsselung und den andernorts verlangten Hintertüren oder dem Verbot höherwertiger und sicherer Kryptografie. Die Komplexität dieser Problematik und die möglichen Konsequenzen sind oft tiefgehender 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 [1].

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. Die sehr ausgeprägte internationale Unternehmens-, Vertriebs- und Supportstruktur und Unternehmensgröße sind die wichtigsten Faktoren.

Auf dem heimischen Markt ist die IT-Sicherheitsindustrie aus Deutschland und Europa in vielen Punkten konkurrenzfähig. Ein Ergebnis der durchgeführten Untersuchung ist, dass die internationale Vertriebs- und Supportstärke noch ausbaufähig ist aber grundsätzlich sind das Potential und die Vielfalt der verfügbaren Technologien sehr breit und von hoher Güte.

1.4 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 [2]. Eine neue Fassung fordert in Zukunft die schriftliche Zusicherung, dass durch den Hersteller keine absichtlichen Backdoors eingebaut wurden.

1.5 Nutzerakzeptanz, Usability, Integrierbarkeit, Qualität

Bei aller Diskussion über Sicherheitshürden, Schutzbedarfe und wirkungsvolle IT-Sicherheitsprodukte sind auch die Erhöhung der Nutzerakzeptanz durch bessere Usability und Transparenz der eingesetzten IT-Sicherheitstechnologien wichtige Schritte auf dem Weg zu mehr IT-Sicherheit. Der Nutzer gehört am Ende im Hinblick auf den „Faktor Mensch" zu den attraktiveren Angriffspunkten aus Sicht der Angreifer und so ist eine transparente Sicherheitslösung oder zumindest eine leicht verständliche aber trotzdem wirkungsvolle entscheidend.

Des Weiteren ist es auch wichtig, dass die IT-Sicherheitsprodukte 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 wiederspiegeln. Dies ist heute in vielen Fällen nicht der Fall und muss zukünftig mit aller konstruktiven Ehrlichkeit berücksichtigt werden.

Das bedeutet letztendlich auch, dass es für den Anwender und den Markt passende IT-Sicherheitsprodukte geben muss, die die Erwartungshaltung der Nutzer erfüllen wird.

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

Die Frage nach dem Marktvolumen und den finanziellen Möglichkeiten ist von zentraler Bedeutung. Interessant im Kontext dieser durchgeführten Arbeit war daher ebenfalls 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 [3]. 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, wie die Ergebnisse der durchgeführten Arbeit zeigen, ca. 0,1% ihres Gesamtumsatzes in IT-Sicherheit investieren, ergibt dies einen potentiellen 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.

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

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

diesem Grund kann eine Fokussierung auf Großanwender helfen, neue IT-Sicherheitsarchitekturen gemeinsam einzuführen.

1.7 Bedürfnisse und Mehrwert von Anwendern

Anwender haben im Hinblick auf ihre IT-Sicherheitslandschaft verschiedene Bedürfnisse. In erster Linie sind ihnen Qualität, internationale Verfügbarkeit und faire Preise wichtig. Auch das Thema der „Backdoors" hat eine hohe Bedeutung. Die Erwartungshaltung an die IT-Sicherheitsindustrie ist dabei, dass die Hersteller ein tieferes Verständnis für das Business der großen Anwendungsfirmen 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. Basierend auf den dargestellten Problemen und Herausforderungen lassen sich entsprechende Thesen herleiten, die als Grundlage für die Studie genutzt wurden.

Thesen der Studie

- Das Merkmal „made in Germany" hat für die Unternehmen eine besondere Bedeutung.
- Ein beträchtlicher Anteil der IT-Belegschaft kümmert sich um die IT-Sicherheit.
- Die Bereitschaft für den Sicherheitsaspekt mehr Geld zu investieren ist vorhanden, da ein höherer Schutzbedarf auch eine zusätzliche Investition bedeutet. Zudem sind die Unternehmen auch bereit, überproportional mehr Geld in größere Technologiesprünge zu investieren.
- Das Budget für IT-Sicherheit ist durchschnittlich höher als bei mittelständige Unternehmen.
- Alle Risiken werden identifiziert und mit Hilfe von Sicherheitstechnologien entgegengewirkt.
- Die Anwender sind aufgrund der Wichtigkeit von Open Source Projekten bereit, Geld für die Qualität, die Weiterentwicklung und Unterstützung von Open Source Projekten zu investieren.

Diese Thesen werden nachfolgend in den entsprechenden Themengebieten aufgegriffen und zusammen mit den tatsächlichen Ergebnissen sowie Implikationen diskutiert.

2 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 Wirtschaft und die Politik 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 jedes 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 wahrzunehmen und auszubauen.

Um diese Probleme zu lösen, ließe sich beispielsweise ein gemeinsames Gremium mit allen wichtigen Stakeholdern einrichten, um die Umsetzung der wichtigsten Aspekte voranzutreiben.

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.

3 Ergebnisse der Studie

Nachfolgend werden die wichtigsten Ergebnisse aus den verschiedenen Themengebieten mit den verschiedenen Schwerpunkten dargestellt, die in der Studie erarbeitet worden sind. Eine Veröffentlichung des gesamten und umfangreichen Papiers befindet sich zum heutigen Zeitpunkt in Vorbereitung und wird im Frühjahr 2018 auf den Webseiten der unterstützenden Verbände zum Download angeboten werden.

Mitarbeiter Im Bereich IT und IT-Sicherheit
Die befragten DAX30 verfügen insgesamt im Durchschnitt über 157.716 Mitarbeiter pro Konzern, von denen durchschnittlich 3.538 in der IT tätig sind und sich davon anteilig **131 Mitarbeiter im Bereich IT-Sicherheit** beschäftigt sind. Dies sind 3,1% der IT-Mitarbeiter und nur 0,1% Anteil in Relation zur Gesamtbelegschaft. Alle

DAX-Unternehmen zusammen haben 3.930 IT-Sicherheitsexperten und arbeiten mit vielen IT-Sicherheitsdienstleitern zusammen

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. Bei der Betrachtung der gemachten Angaben wird ersichtlich, dass die Ausrichtung der Schwerpunkte sehr unterschiedlich ist. Übergeordnet lassen sich jedoch Gemeinsamkeiten identifizieren. Die **häufigsten Schwerpunkte bei der IT-Sicherheit sind IT-Infrastrukturen, Awareness und Governance bzw. Compliance**.

Insbesondere das Thema Awareness bewegte die meisten der befragten Unternehmen sehr stark. Die Sichtweise ist, dass die vollständige Verantwortung nicht bei den Nutzern liegt und auch nicht liegen kann, sondern die Hersteller die Verantwortung tragen muss.

Weiterhin sind auch moderne neue Technologien für die Teilnehmer sehr wichtig. Was früher unter dem Begriff „Kommunikationslagebild für das eigene Netzwerk" als sinnvoll erachtet worden ist, wird heute als „Security Advanced Analytics Platform" als notwendig und wichtig empfunden. So setzen 10 der 12 Konzerne auf Lagebilder und haben damit überwiegend gute Erfahrungen gemacht. Analytics Plattformen sind aus der Sicht der Anwender ein spannender Trend, den sie verfolgen.

Ein wesentlicher Punkt war das Thema der Hochsicherheit. Hier legten sich die Verantwortlichen klar auf IT-Sicherheitsprodukte fest, die besonders starken Schutz versprechen, die jedoch heute noch nicht in der Breite eingesetzt werden, obwohl dies in den meisten Fällen sinnvoll wäre – je nach Branche und Unternehmensbereich. Genutzt werden Hochsicherheitsprodukte heute insbesondere beim Schutz der eigenen „Golden Nuggets" des Unternehmens. Dies sind beispielsweise Produktentwicklung, Forschung und hochkritische Informationsbereiche.

Zudem sind die Unternehmen durchaus bereit für übermäßig größere Technologiesprünge auch ein übermäßig hohes Budget zu investieren.

Beschaffung: Budgets
Was steht den Unternehmen an finanziellen Mitteln zur Verfügung? Aus den veranschlagten Budgets für IT und IT-Sicherheit lassen sich durchaus Schlussfolgerungen auf Schwerpunkte und technologische Expansion ziehen. So gibt es erwartungsgemäß eine sehr breite Spanne der jeweiligen Budgets.
Ein Unternehmen gab ein IT-Budget von ca. 3,5 Mrd. EUR an, wovon etwa 175 Mio. EUR für IT-Sicherheit eingeplant waren. Im Durchschnitt hat ein DAX Konzern etwa 1,5 Mrd. EUR IT-Ausgaben angegeben, wovon etwa **80 Mio. EUR für IT-Sicherheit** veranschlagt worden sind. Dieser Durchschnitt bezieht sich lediglich auf die 12 befragten Unternehmen und begrenzt auf alle 30 Konzerne anwendbar, da dieser Wert im Einzelnen starken Schwankungen unterliegt. Für alle 30 DAX Unternehmen würde dies jedoch ein Gesamtbudget von ca. 2,4 Mrd. EUR ergeben. Dieser Wert liegt über dem erstgenannten Wert aus der prozentualen Betrachtung und hat ebenfalls einen Schätzungscharakter, jedoch einen anderen Betrachtungsansatz.

Die getätigten Angaben für IT und IT-Sicherheit lassen sich entsprechend im Durchschnitt betrachten. 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**.

Interpretation?
Bezugnehmend zu den aufgestellten Thesen, werden nun Ergebnisse in Verbindung mit möglichen Implikationen diskutiert. In diesem Bereich divergieren die Annahmen und Ergebnisse zum größten Teil.

Die aufgewendeten personellen und finanziellen Mittel liegen zwar meist höher als angenommen – je nach betrachtetem Unternehmen – sind jedoch nicht so hoch, wie angenommen. Zudem ist die Anzahl der Beschäftigten im Bereich der IT-Sicherheit deutlich niedriger als erwartet werden könnte. Nicht zuletzt ist dies jedoch auch dem Mangel an qualifizierten Experten am Markt zuzurechnen. Um diesem Umstand zu begegnen, werden Föderations- und Kooperationsmodelle unter den Anwendern diskutiert und ausprobiert, als auch externe IT-Sicherheits-dienstleister beauftragt.

3.1 Kriterien und Aspekte zur Beschaffung von IT-Sicherheitsprodukten

Interessant waren auch die Aspekte, die bei der Beschaffung von IT-Sicherheitsprodukten eine Rolle spielen. 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.

Keine große Rolle spielen demnach die Herkunft, die 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 ableiten, dass heute die Herkunft der Produkte eine untergeordnete spielt.

Hierzu gesellt sich auch die Kategorie „Marktführerschaft". Es spielt offenbar nur eine geringe Rolle, ob ein Anbieter mit seinem IT-Sicherheitsprodukt der Marktführer ist oder nicht, die anderen Kriterien sind tendenziell deutlich bedeutender.

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.

Interpretation?
Aus den Angaben lassen sich zwei wichtige Implikationen herleiten: Die wichtigsten Kriterien sind Qualität, Preis, Supportzeitraum und Internationaler Support.

Das Thema „Made in Germany" spielt in den Augen der Befragten heute keine wesentliche Rolle, sofern es sich nicht um den Schutzbedarf sensibler Bereiche und die eigenen „Kronjuwelen" handelt.

3.2 Angemessene Relationen: Anschaffungspreis IT und Kosten für IT-Sicherheit

Im Hinblick auf Verhältnisse zwischen den Kosten von Systemen und der zusätzlichen Sicherheit, 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 Strategiepapier „IT-Si-

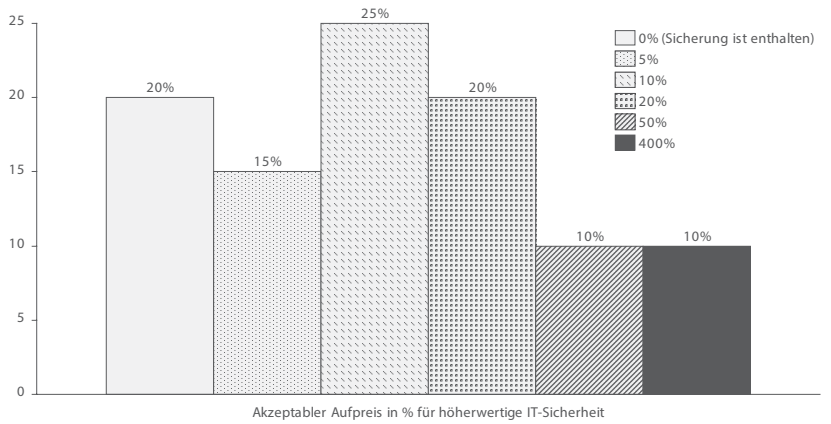
cherheitsstrategie für Deutschland“ [4] des TeleTrusT e.V. durchgeführt, bzw. jenes dort vorgestellte Wirkungsklassenmodell.

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, da es IT-Systeme mit sehr unterschiedlichen Schutzbedarfen gibt.

Viele tendierten zwar dazu, über die im Durchschnitt insgesamt ermittelten 20% hinaus, dass Sicherheit eigentlich integrativ dazugehört, es jedoch besonders sensible Bereiche gibt, wo die Abdeckung durch diese vollkommen unrealistisch erscheint. Wie bereits diskutiert, ist Hochsicherheit insgesamt für alle ein wichtiges Thema, daher wurde durchaus auch das Ende der Skala mit 400% Aufpreis als relevant angesehen.

Abbildung 2 | Akzeptabler Aufpreis in % für höherwertige IT-Sicherheit



Wie die Abbildung 2 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.

Im Detail gaben die Konzerne an, dass **der Preis im Prinzip nicht entscheidend** sei und die Entscheidung auf Basis einer eigenen Klassifikation des Business-Impacts festgestellt wird.

In manchen Fällen fiel die Bewertung schwierig unter dem Gesichtspunkt, dass Sicherheit heute (notwendigerweise) „State oft he Art“ sein muss. Einige Befragte gehen strikt risikobasiert vor, wobei der Schutz dem Wert der betrachteten „Juwelen“ entsprechen muss.

Interpretation?

Bei dieser Frage lassen sich die folgenden Implikationen festhalten: Ein Teil der Unternehmen erwartet einfach, dass eine angemessene Sicherheit integriert ist, aber es gibt durchaus den Bedarf, deutlich mehr Geld für IT-Sicherheit auszugeben.

3.3 Relevante Faktoren für Anschaffung von IT-Sicherheitsprodukten

Alle Beteiligten waren sich einig, dass eine dringliche Notwendigkeit für IT-Sicherheitsprodukte besteht. Was sind aber die relevanten Faktoren, die eine Anschaffung motivieren?

Die Auswertung der Ergebnisse 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.

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 zwar nur eine untergeordnete Rolle, allerdings übersteigt in der Gesamtbetrachtung irgendwann der gänzliche Aufwand den tatsächlichen Nutzen.

Interpretation?

Einige mögliche Implikationen wären an dieser Stelle: Die Vertriebsstrategie der IT-Sicherheitsanbieter sollte an die Beschaffungsstrategie angepasst werden, dies wäre ein beidseitiger Mehrwert.

Weiterhin ist eine Preisanpassung im Kontext der „letzten Meile“ zu prüfen, denn der Kauf von Produkten ist aufgrund zu hoher Kosten ab einem Punkt nicht mehr attraktiv. Hier empfiehlt sich unter diesem Aspekt die Prüfung einer Neuausrichtung des Portfolios.

3.4 Bewusste Akzeptanz von IT-Sicherheitsgefahren

Eine vollständige Sicherheit kann es nicht geben – in diesem Punkt sind sich alle Parteien einig. Auch Anwender, ganz egal welcher Größe, **nehmen bewusst Risiken in Kauf**. Dies bedeutet, dass diese nicht einfach ignoriert werden. Die Gründe sind sehr unterschiedlich, es gibt aber stets gemeinsame Nenner: Für die letzten Prozentpunkte an IT-Sicherheit fehlt das Geld. Aus diesem Grund werden **Risiken Klassifiziert und dokumentiert**, statt entsprechende Produkte zu kaufen.

Die Maßnahme liegt dabei meist beim Tragen der Risiken durch Akzeptanz und entsprechendes Risikomanagement. Zudem wird letztendlich auch in Versicherungspolicen investiert, statt in IT-Sicherheitsprodukte.

Interpretation?

Die Implikationen sind im Hinblick auf die befragten Meinungen relativ synchron: In der Konsequenz, dass die letzten Prozentpunkte IT-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 hochqualifizierte Personal nicht vorhanden, auch wenn das Budget für die Beschaffung da wäre, daher sollte der Rolloutaufwand geprüft und optimiert werden.

3.5 Open Source ein wichtiger Faktor

Open Source ist heute ein essentieller Bestandteil aller verwendeten IT-Produkte. Insgesamt gaben alle 12 der Befragten an, Open Source im Bereich der IT und IT-Sicherheit zu nutzen. Mangelnde Ressourcen in der Open Source Community haben Sicherheits- und Qualitätsprobleme zur Folge. Daher 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. Hinsichtlich der genannten Größenordnung einer finanziellen Aufwendung sind Summen zwischen 10.000 EUR und 5.000.000 EUR p.a. genannt worden. Bei der Organisation dieses Sponsorings würde sich ein DAX Open Source Fond Modell anbieten. Dabei wäre es jedoch wichtig die Priorisierung der jeweiligen Stakeholder zu berücksichtigen, damit das verfügbare Budget als Mehrwert zurückfließen kann.

Interpretation?
Die These zur Wichtigkeit und Unterstützung von Open Source ist bestätigt worden und hat die aufgestellten Erwartungen sogar übertroffen. Der Wille positiv auf bestehende Open Source Projekte zu wirken und hierfür Geld zu investieren ist gegeben. Dies bedeutet auch, dass mit der Gründung eines Open Source Fonds auf einen Schlag beträchtliche Mittel zur Verfügung stehen würden, die heute ungenutzt sind. Eine der Hürden ist die Entwicklung einer entsprechenden Strategie, wie möglichst alle Anwender zu einer Teilnahme an einem gemeinsamen Fonds motiviert werden könnten.

3.6 Ein Blick in die Zukunft: 10+ Jahre

Bereits heute stehen sich ausgeklügelte IT-Sicherheitssysteme, Architekturen, sowie Gegenmaßnahmen und immer professioneller werdende Angreifer gegenüber. Aus der Historie heraus ist dieses Wettrüsten aus anderen Bereichen bereits bekannt und eine Prognose darüber, wer am Ende die besseren Chancen hat, fällt schwer. Im Hinblick auf die Zukunft stellt sich die Frage, welche Innovationen die Anwender beider Seiten erwarten – also im Grunde genommen die IT-Sicherheit und Bedrohungslage im Jahre 2027 bis 2030. Zusammenfassend lassen sich die Antworten als Delta in einigen Punkten verdichten.

So wird es eine **vollständige Cloudifizierung** im Gegensatz zur heutigen nur teilweisen Nutzung von Cloud-Diensten geben. Bereits heute ist es laut den Befragten keine Frage von „ob in die Cloud", sondern lediglich „wann".

Der vergleichsweise mittelmäßige IT-Sicherheitslevel von heute wird ein annähernd optimales Maß erreichen. Bei allen Betrachtungen spielt nicht nur die eigene IT, sondern die gesamte Lieferkette eine Rolle.

Artificial Intelligence wird aus der Nische austreten und sowohl im Angriff als auch Verteidigung, also in der Breite beidseitig eingesetzt werden.

Software und Hardware wird die heutige Robustheit deutlich übertreffen. Dabei werden Sicherheitsprodukte ein hohes Maß an Transparenz erreichen und für den Nutzer unsichtbar.

Die Geschäftsmodelle von Angreifern werden sich professionalisieren und auf KRITIS ausgerichtet werden.

4 Und nun? (Der Versuch eines Fazits)

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 IT-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 Lizensierungsmodelle nicht mehr zeitgemäß. Auch die durch die Hersteller propagierte Herkunft aus Deutschland spielt für die Anwender nur eine untergeordnete Rolle.

Innovationen sind für die Großanwender ebenfalls ein sehr zentrales Thema. Durch bestehende (zahlreiche) Prozesse und die Struktur einer großen Organisation, besteht 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 erhoffen 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.

Vielleicht gelingt es global gesehen auf diese Weise – neben der Erreichung eines angemessenen Sicherheitsniveaus, in vielen Bereichen der IT-Sicherheit, nicht länger als Follower aufzutreten, sondern in naher Zukunft die Rolle des Leaders zu übernehmen.

Eine enge Zusammenarbeit zwischen Hersteller und Anwender im Bereich der IT-Sicherheit ist dringend notwendig, um passende IT-Sicherheitslösungen für eine angemessen IT-Sicherheitslevel nutzen zu können.

Literatur

[1] N. Pohlmann, R. Riedel: „Strafverfolgung darf die IT-Sicherheit im Internet nicht schwächen", DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 1/2018

[2] 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: 20.01.2018

[3] 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: 20.01.2018

[4] TeleTrusT – Bundesverband IT-Sicherheit e.V. Strategiepapier „IT-Sicherheitsstrategie für Deutschland", URL: https://www.teletrust.de/fileadmin/docs/IT-Sicherheitsstrategien/2015-Barchnicki-IT-Sicherheits-Wirkungsklassen_09-03-2015.pdf, Stand: 09.03.2015, Zuletzt abgerufen: 20.01.2018