Information Security

Informationssicherheit in Deutschland, Österreich und der Schweiz 2015

Eine Studie zur Informationssicherheit in deutschen, österreichischen und Schweizer Unternehmen und Organisationen

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

eingereicht von

Philipp Reisinger, BSc

is131510

im Rahmen des

Studienganges Information Security an der Fachhochschule St. Pölten

Betreuung

Betreuer/in: FH-Prof. Dr. Simon Tjoa

St. Pölten, 6. August 2015 _____ _____

(Unterschrift Verfasser/in) (Unterschrift Betreuer/in)

Fachhochschule St. Pölten GmbH, Matthias Corvinus-Straße 15, A-3100 St. Pölten,T: +43 (2742) 313 228, F: +43 (2742) 313 228-339, E:office@fhstp.ac.at, I:www.fhstp.ac.at

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.

- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Der Studierende räumt der FH St. Pölten das Recht ein, die Diplomarbeit für Lehre- und Forschungstätigkeiten zu verwenden und damit zu werben (z.B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei der Absolvent als Urheber zu nennen ist. Jegliche kommerzielle Verwertung/Nutzung bedarf einer weiteren Vereinbarung zwischen dem Studierenden/Absolventen und der FH St. Pölten.

St. Pölten, 6. August 2015

_____

(Unterschrift Verfasser/in)

Kurzfassung

In dieser Diplomarbeit werden die Durchführung und die Ergebnisse meiner Studie zum Thema Informationssicherheit, welche in Unternehmen in Deutschland, Österreich und der Schweiz vorgenommen wurde, beschrieben. Im Rahmen der Studie wurde versucht, die aktuelle Ist-Situation bezüglich der Informationssicherheit zu erheben und zu bestimmen, inwiefern die Informationssicherheit in den verschiedenen Ländern ein Thema ist bzw. sich im Bewusstsein der Unternehmen befindet.

Zusätzlich zu einigen allgemeinen Fragen zur Informationssicherheit selbst, Vorfällen und verschiedenen „Trendthemen“ wie Cloud Computing und Outsourcing, APTs, der Verwendung von Open Source Software oder der Bedeutung der NSA Enthüllungen wurde erhoben, welche technischen und organisatorischen Maßnahmen bzw. Vorkehrungen in Unternehmen im Informationssicherheits-Bereich getroffen werden und zukünftig geplant sind.

Neben der Umfrage selbst, deren Erstellung und Durchführung, wird auch ein Überblick über die wichtigsten weltweiten und nationalen Informationssicherheits-Studien gegeben.

Aufgrund der Ergebnisse der durchgeführten Umfrage lässt sich festhalten, dass das Thema der Informationssicherheit für die meisten der teilnehmenden Unternehmen von großer bis sehr großer Bedeutung ist. Außerdem zeigt sich, dass sich eine große Mehrheit der Wichtigkeit von korrekten Daten und Informationen sowie der Abhängigkeit von der eigenen IT bewusst ist.

Bezüglich technischer und organisatorischer Maßnahmen kann zusammengefasst werden, dass grundlegende Maßnahmen wie Firewalls, Virenschutz, Backupsoftware, Spamschutz sowie Medien- und Datenvernichtung oder Patch- und Updatemanagement beinahe durchgängig vorhanden sind, wobei sich aber in Bezug auf weitreichende oder speziellere Maßnahmen ein gespaltenes Bild mit teilweise schnell sinkendem Implementierungsgrad zeigt (in Abhängigkeit von Faktoren wie der Unternehmensgröße, dem allgemeinen Bewusstsein für Informationssicherheit, dem Stellenwert bzw. der Notwendigkeit dieser im Unternehmenskontext sowie der Nutzung von Standards). Verschiedene komplexe und/oder aufwändige Maßnahmen wie DLP, SIEM, der Betrieb eines IKS inklusive IT-Kontrollen oder ein firmeneigenes CERT sind nur bei einer Minderheit der Unternehmen umgesetzt.

Die Auswertung und Ergebnisse der Studie werden im Kapitel 4 ausführlich beschrieben und in Kapitel 5.1 zusammengefasst. Alle Detailergebnisse der Fragen sowie der gesamte Fragebogen selbst sind im Anhang A ersichtlich.

Anmerkung: Aufgrund diverser Faktoren und Einschränkungen bei der Verteilung und Durchführung der Umfrage ist eine gewisse Verzerrung der Ergebnisse (Über-/Unterrepräsentation von Unternehmen gewisser Größe/Branche bzw. IT-Affinität & Sicherheitsbewusstsein etc.) möglich und wahrscheinlich (siehe Kapitel 4.5).

Es ist davon auszugehen, dass die meisten Teilnehmerinnen und Teilnehmer dieser Umfrage ein höheres Bewusstsein und Interesse für das Thema der Informationssicherheit aufweisen und hierin besser aufgestellt sind als ein „typisches durchschnittliches Unternehmen“ dies ist.

Daher erhebt diese Studie keinen Anspruch auf Repräsentativität und die Gesamtsituation der Informationssicherheit in Deutschland, Österreich und der Schweiz könnte, verglichen mit den in dieser Studie angeführten Ergebnissen und Schlüssen „anders“ bzw. „schlechter“ sein, als hier nahegelegt wird. Die aktuelle Informationssicherheitssituation soll im Folgenden jedoch zumindest in Bezug auf die teilnehmenden Unternehmen beschrieben werden.

Abstract

The following diploma thesis describes the creation and the results of my study on information security in companies in Germany, Austria and Switzerland. This study examines the current information security situation in these countries and tries to research whether information security is an important topic for the participants and what their commitment, awareness and activities concerning this topic look like.
Additionally to some general information security questions, incidents and various trend topics like cloud computing and outsourcing, APTs, the usage of open source software as well as the consequences and importance of the NSA revelations it was also examined which technical and organizational information security measures and controls are implemented and which measures are planned for the future.
Beside the description of my study this diploma thesis also contains a short overview of the most important worldwide and national information security studies.
The results suggest that for most of the participating companies information security is a topic of high to very high importance. They also show that a majority of the respondents is aware of the importance of correct data and information and their dependency on their own IT.
Regarding technical and organizational information security measures it is concluded that basic measures like firewalls, virus protection, backupsoftware, spam protection as well as media- and data disposal patch- or update management are implemented almost comprehensively. However, concerning more sophisticated or elaborate measures there are huge differences and a sometimes rapid decrease in implementation (which depends on factors like company size, general information security awareness, the status and need within the company context as well as the usage of standards) can be observed. Some complex and/or expensive measures like DLP, SIEM, operation of an internal control system or a company owned CERT are only implemented by a minority of the companies.
The analysis and the results of my study are described in chapter 4 while chapter 5.1 contains a short summary. All detailed results as well as the whole questionnaire are available in the appendix A.

Comment: Due to various factors and restrictions during the distribution and execution of this survey a certain bias of the results (over-/underrepresentation of companies of specific size/branch and/or IT-affinity & security awareness etc.) is possible and likely (see chapter 4.5). It must be assumed that most of the participants exhibit a higher awareness and interest in the topic of information security and are better equipped than a "'typical average company"' would be.
That is why this survey does not raise a claim to be representative and the overall situation of information security in Germany, Austria and Switzerland could be, compared to the results and conclusions of this study, "'different"' and/or "'worse"'. However in the following the current information security situation can at least be described in respect to the participating companies.

Danksagung

Zuallererst und am meisten möchte ich mich bei allen Teilnehmerinnen und Teilnehmern der Umfrage bedanken. Nur durch ihre Unterstützung und Geduld ist diese Diplomarbeit überhaupt erst möglich geworden und ich hoffe sehr, dass die Ergebnisse dieser Arbeit für sie interessant und von Nutzen sind.

Ich möchte mich bei allen Unternehmen, Organisationen und Personen bedanken, die mich bei der Erstellung, Abstimmung, Durchführung und Verteilung meiner Umfrage unterstützt haben. Hier gilt mein Dank insbesondere dem BSI und <kes>, der FH St. Pölten, Computerwelt, dem ADV, dem IKT-Sicherheitsportal, der WKÖ IT-Security Experts Group, ISACA Österreich, Cyber Security Austria sowie der ISSS und der SGRP. Auch gilt mein Dank den vielen weiteren hier namentlich nicht genannten engagierten Personen, die wertvolle Beiträge zu dieser Arbeit geleistet haben. Auch möchte ich mich bei meinem Arbeitgeber, der SBA Research sowie meinen Kolleginnen und Kollegen bedanken, welche ebenfalls bei der Durchführung und Verteilung meiner Umfrage eine große Hilfe waren.

Bei meinem Betreuer Herrn FH-Prof. Mag. Dr. Simon Tjoa, der - nicht nur bei diesem Werk, sondern auch während dem gesamten Studium - immer für meine Fragen zur Verfügung gestanden ist, wertvolle Tipps und Anregungen bei der Erstellung dieser Arbeit geliefert und mich auch bei der Durchführung der Umfrage tatkräftig unterstützt hat, möchte ich mich ebenfalls bedanken.

Schlussendlich möchte im mich natürlich bei meinen Eltern, meiner Familie und bei meiner Freundin, die mich während meinem Studium immer unterstützt und es erst ermöglicht haben bedanken. Auch sie haben bei der Erschaffung dieser Arbeit einen wertvollen Beitrag geleistet.

Inhaltsverzeichnis

1. Einleitung

1.1. Bedeutung Informationssicherheit

Im heutigen digitalen Zeitalter sind bereits beinahe alle Menschen - zumindest in der westlichen Welt - in ihrem alltäglichen Leben und ihrer Existenz auf IT-Systeme und Computer angewiesen. Die Durchdringung des Lebens jedes einzelnen Menschen durch IT und technische Systeme schreitet in hoher Geschwindigkeit voran, wodurch auch das Thema der Vertrauenswürdigkeit und Sicherheit dieser Systeme weltweit an Bedeutung gewinnt. Auch für ganze Staaten hat die Informations- bzw. Cybersicherheit in den letzten Jahren rasant an Bedeutung gewonnen, was an dem wachsenden Bewusstsein für Themen wie die Abhängigkeit von IT in diversen Sektoren und Lebensbereichen (Stichwort kritische Infrastruktur, Internet der Dinge, Industrie 4.0, Smart-Technology etc.) bis hin zu den weltweiten Diskussionen zu Themen wie „(Wirtschafts)Spionage und Überwachung“, „Cybercrime“ und „Cyberwarfare“ sichtbar wird.

Da in der heutigen Zeit bereits auch beinahe alle Unternehmen und Organisationen in ihren Geschäftsprozessen und -tätigkeiten stark von korrekt funktionierenden IT-Systemen und einer stabilen IT-Landschaft abhängig sind und diese täglich nutzen, ist die Informationssicherheit auch für diese ein Thema von großer Wichtigkeit und stetig steigender Bedeutung. Ein Geschäftsbetrieb ohne jegliche Nutzung oder Abhängigkeit von Informations- und Kommunikationstechnik ist für die meisten Unternehmen heute kaum mehr vorstellbar. Aufgrund dieser Abhängigkeit können Ausfälle oder Manipulationen von IT-Systemen dazu führen, dass betroffene Unternehmen ihre Kerntätigkeiten nicht mehr ausführen können, wodurch binnen kurzer Zeit hohe oder existenzbedrohende Schäden entstehen [1, S. 1f].

Auch Informationen und Daten spielen in der heutigen Zeit eine wichtige Rolle und stellen eine zentrale Basis der Geschäftstätigkeiten und des täglichen Betriebs von Unternehmen dar. Der Schutz von Informationen jeglicher Art, insbesondere von personenbezogenen Daten, internen Geschäftsdaten, EMails, Verträgen, Buchhaltungs/Finanz- oder Projektdaten etc., ist von essentieller Bedeutung, da deren Diebstahl, Verlust, Verfälschung oder Nicht-Verfügbarkeit bzw. deren Weitergabe etwa an Mitbewerber oder unautorisierte Dritte - schwere finanzielle, wirtschaftliche und rechtliche Konsequenzen haben und sich mitunter auch negativ auf das Image eines Unternehmens auswirken können [1, S. 1f].

Unternehmen, ihre IT-Systeme sowie vertrauliche Firmendaten sind einer Vielzahl von unterschiedlichen Bedrohungen ausgesetzt, zu denen unter anderem Gefahren wie Schadsoftware, Hacking, (Wirt-

schafts)Spionage, gezielte Angriffe, Phishing, Systemausfälle, technische Fehler etc. zählen. Das weitläufige Feld der Informationssicherheit beschäftigt sich eben damit, den Schutz der Informationen und IT-Systemen eines Unternehmens vor derlei Risiken zu gewährleisten und einen stabilen und reibungslosen Betrieb zu ermöglichen [1, S. 1f].
Die Bedeutung der Informationssicherheit zeigt sich mittlerweile auch auf rechtlicher Ebene (Stichwort Compliance). Die Entwicklung geht immer mehr dahin, dass mittels verschiedener Gesetze und Regelungen für Vorstände und Geschäftsführer im Rahmen ihrer Sorgfaltspflicht eine persönliche Haftung für Versäumnisse und mangelnde Risikovorsorge in Bezug auf Datensicherheitsmaßnahmen vorgesehen ist [2, o. S.].

1.2. Motivation für das Thema

Da ich bereits 2013 im Rahmen meiner Bachelorarbeit eine Studie zum Thema Informationssicherheit in Österreich durchgeführt habe (siehe [1, o. S.]), wollte ich die Chance nutzen, auf dieser Ausgangsbasis eine größere, aktuellere und aussagekräftigere Untersuchung durchzuführen.
Bereits bei meinem Berufspraktikum im Sommer 2012 bei der Firma Security Research wurde ich zum ersten Mal mit dem Thema Studien im Bereich der Informationssicherheit konfrontiert. Während meinen Recherchen stellte ich fest, dass spezifisch für Österreich nur relativ wenige Studien vorhanden bzw. frei verfügbar sind. Auch während meiner folgenden Anstellung bei SBA Research wurde ich immer wieder mit diesem Thema konfrontiert und musste feststellen, dass sich an dieser Situation in Bezug auf Österreich kaum etwas geändert hat.
Der Mangel an Studien zur Informationssicherheit stellt eine große Lücke dar, da dieses Thema aufgrund der steigenden Nutzung und Abhängigkeit von IT und Daten bzw. Informationen von hoher Bedeutung ist. Auch können die Resultate solcher Studien, sowie Zahlen und Fakten zur derzeitigen Informationssicherheitssituation für Unternehmen eine wertvolle Hilfe sein, um die eigene Sicherheitslage richtig einzuschätzen.
Ein weiterer Hintergedanke bei der Erstellung dieser Diplomarbeit was es, eine nicht übermäßig „technische bzw. themen- oder fachspezifische“ Arbeit zu schreiben, von der ich hoffe, dass sie auch außerhalb der FH eine gewisse Verbreitung und Interesse findet und Unternehmen dazu bringt und dabei unterstützt, sich mit dem unbestreitbar sehr wichtigen Thema der Informationssicherheit auseinanderzusetzen.
Die Ergebnisse dieser Studie sollen als Diskussionsbasis dienen und Bewusstsein bzw. Interesse für das Thema der Informationssicherheit schaffen. Außerdem könnte diese Arbeit auch als Basis oder Grundlage für Folgestudien in diesem Bereich genutzt werden, da genaue und aktuelle Informationen zur Informationssicherheitssituation in Unternehmen (auf denen aufbauend Unternehmen etwa Maßnahmen oder Strategien ableiten können), trotz der hohen Bedeutung dieses Themas, sehr oft Mangelware sind.

1.3. Forschungsleitende Fragestellungen

Im Rahmen meiner Studie zur Informationssicherheit in deutschen, Schweizer und österreichischen Unternehmen und Organisationen soll ein Überblick über dieses Thema gegeben und folgende Fragen behandelt werden:

- Wie ist das Bewusstsein in deutschen, Schweizer und österreichischen Unternehmen und Organisationen in Bezug zur Informationssicherheit, was ist deren Stellenwert und wie lässt sich die derzeitige Situation beschreiben?
- Welche technischen und organisatorischen Maßnahmen werden von Unternehmen und Organisationen im Bezug zur Informationssicherheit getroffen?
- Gibt es länderabhängig große Unterschiede bezüglich Stellenwert und Aufstellung in Bezug zur Informationssicherheit zwischen Unternehmen in Österreich, Deutschland und der Schweiz?

Diese Fragen bilden die Grundlage der durchgeführten Arbeit und des erstellten Fragebogens. Sie werden in Kapitel 4.4 behandelt.

1.4. Hypothesen

Zu Beginn der Arbeit wurden nach einer Literaturrecherche sowie aufbauend auf meiner vorigen Studie folgende Hypothesen aufgestellt, die im Rahmen dieser Studie verifiziert werden sollen. Manche Hypothesen wurden auch ausgehend von in der Informationssicherheits-Branche weit verbreiteten Annahmen bzw. Feststellungen formuliert.

I Ein Großteil der Unternehmen ist stark von der eigenen IT abhängig und sich dessen bewusst [1, S. 42]. Generell geben große Unternehmen häufiger an, stark von der eigenen IT abhängig zu sein.

II In einem Großteil der Unternehmen gab es Vorfälle im Bereich der Informationssicherheit [1, S. 33]. Unternehmen, die von Vorfällen betroffen waren, setzen häufiger und mehr technische und organisatorische Maßnahmen ein. Die Betroffenheit von Vorfällen ist unabhängig von der Unternehmensgröße.

III Malware, Hacking, Datenverluste, Fahrlässigkeit von Mitarbeitern und physischer Diebstahl werden von Unternehmen als Hauptrisiken/Bedrohung in Bezug zur Informationssicherheit angesehen [1, S. 31].

IV Malware, Hacking und physischer Diebstahl gehören zu den häufigsten Vorfallsarten, von denen Unternehmen betroffen sind [3]. Diese Vorfallsarten werden unabhängig von Unternehmensgröße und Land am häufigsten genannt.

V Ein Großteil der Unternahmen war von aktuellen Sicherheitslücken wie Heartbleed oder Shell Shock betroffen [4], wobei dies jedoch große Unternehmen häufiger angeben.

VI Die wichtigsten Beweggründe für IT-/Informationssicherheit sind gesetzliche Vorgaben und Compliance, die Vermeidung von Datenverlusten oder Verfälschungen sowie die Sicherstellung der Stabilität des Betriebes. Gesetzliche Vorgaben und Compliance werden öfter von großen Unternehmen als Grund für Informationssicherheit genannt [1, S. 26ff].

VII Ein Großteil der Unternahmen setzt Open Source Software ein. Die meisten vertrauen Open Source Software und unternehmen keine weiteren Schritte, um die Fehlerfreiheit/Qualität/Korrektheit/ Zuverlässigkeit der Open Source Software zu überprüfen.

VIII Nach dem NSA Skandal gibt es größeres Interesse für IT Made in Austria/Germany/Switzerland/ Europe [5, S. 32]. Dies gilt insbesondere für Unternehmen aus Deutschland. Für kleine Firmen ist dieses Thema nicht sehr bedeutend.

IX Der NSA Skandal führt zu größerer Vorsicht bei der Nutzung von Cloud Services und zu einer verstärkten Nutzung bzw. Nachfrage von heimischen/europäischen Anbietern [6, S. 29ff].

X Insbesondere in kleinen Unternehmen ist die Nutzung von Standards/Empfehlungen im Bereich der Informationssicherheit nicht sehr weit verbreitet.

XI Cyber Versicherungen sind (noch) nicht sehr verbreitet [7, S. 62]. Hauptsächlich interessieren sich große Unternehmen, die sich der eigenen Abhängigkeit von der IT bewusst sind und deren technische und organisatorische Sicherheitsmaßnahmen bereits gut aufgestellt sind, hierfür.

XII APT sind zwar ein Thema, aber nicht die „vorrangige“ Vorfallsart. Nur wenige Unternehmen geben an, im letzten Jahr Ziel eines APT gewesen zu sein [8, S. 5] [9, S. 11].

XIII Grundlegende wichtige technische Sicherheitsmaßnahmen (wie Firewalls, Virenschutz, VPNs oder Backupsoftware) sind beinahe durchgängig vorhanden, während sich aber in Bezug auf weiterreichende oder speziellere Systeme (Vulnerability Management Tools, DLP, IDS/IPS, WAF etc.) ein gespaltenes Bild zeigt [1, S. 39f].

XIV In Bezug auf organisatorische Maßnahmen werden insbesondere die Themen Spam & Antivirus, Backup und Wiederherstellung, Identitäts- und Zugriffsmanagement sowie die physische Sicherheit oft behandelt. Aufwändige und umfangreiche Maßnahmen wie der Betrieb eines ISMS, eines IKS oder eines firmeneigenen CERTs werden hauptsächlich von großen Unternehmen umgesetzt [1, S. 41ff].

XV Die technische Aufstellung der Unternehmen ist oft besser als die organisatorische [7, S. 74]. Viele organisatorische Maßnahmen werden erst in großen Unternehmen eingesetzt.

XVI KMU sind insbesondere in Bezug auf organisatorisch Sicherheitsmaßnahmen schlechter aufgestellt als große Unternehmen [10, S. 6ff].

Auf die Hypothesen wird in Kapitel 4.3 eingegangen.

1.5. Definition Informationssicherheit

Da der Begriff der Informationssicherheit in dieser Studie von hoher Bedeutung ist und oft verwendet wird, soll er hier definiert und beschrieben werden.
Laut Begriffsdefinition des ISO 27000 Standard, welcher (zumindest in Europa) im Bereich der Informationssicherheit einer der am weitest verbreiteten Standards zum Thema Implementierung und Betrieb eines Informationssicherheitsmanagementsystems (ISMS) ist, beschäftigt sich die Informationssicherheit mit der „Aufrechterhaltung der *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* von Informationen“ [11, S. 4], wobei neben diesen Grundeigenschaften ebenfalls „andere Eigenschaften wie Authentizität, Zurechenbarkeit, Nicht-Abstreitbarkeit und Verlässlichkeit“ [11, S. 4] berücksichtigt werden können.
Unter *Vertraulichkeit* wird verstanden, dass Informationen nicht für unautorisierte Individuen, Prozesse oder Entitäten zugänglich gemacht oder veröffentlicht werden [11, S. 2].
Unter **Integrität** wird die Genauigkeit bzw. Richtigkeit sowie Exaktheit und Vollständigkeit von Informationen verstanden. Das bedeutet, dass Informationen, Applikationen oder Systeme nicht unberechtigt verändert oder modifiziert werden können beziehungsweise jegliche Veränderung bei deren Benutzung erkannt werden kann und nachvollziehbar ist [11, S. 5].
Verfügbarkeit bedeutet, dass Informationen, Applikationen und Systeme im Bedarfsfall für eine autorisierte Entität uneingeschränkt zur Verfügung stehen müssen [11, S. 2].
Informationen sind laut ISO 27002:2008 Vermögenswerte, welche wertvoll für eine Organisation sind und daher in geeigneter Weise geschützt werden müssen. Dies wird dadurch erklärt, dass insbesondere durch die steigende Vernetzung und umfassenden Nutzung der IT im alltäglichen Geschäftsbetrieb die Abhängigkeit von diesen Ressourcen stetig steigt [12, S. 8]. Weiters wird in ISO 27002:2008 erläutert, dass „Informationen [...] in vielen verschiedenen Formen vorliegen [können, d. Verf]. Sie können auf Papier gedruckt oder geschrieben, elektronisch gespeichert, per Post oder auf elektronischem Wege übermittelt, in Filmen gezeigt oder in Gesprächen mündlich weitergegeben werden“ [12, S. 8]. „Unabhängig davon, in welcher Form die Informationen vorliegen und welche Hilfsmittel zu ihrer gemeinsamen Nutzung oder Speicherung angewendet werden“ [12, S. 8], sollen sie immer angemessen geschützt sein, um „einen kontinuierlichen Geschäftsbetrieb sicherzustellen [und, d. Verf.] Geschäftsrisiken auf ein [angemessenes, d. Verf] Mindestmaß zu reduzieren“ [12, S. 8] [1, S. 2f].

Im ISO 27002:2008 Standard wird beschrieben, dass „Informationssicherheit [...] durch die Implementierung einer Reihe geeigneter [technischer und organisatorischer, d. Verf] Maßnahmen erreicht“ [12, S. 8] bzw. ermöglicht werden kann, wobei zu diesen etwa „Politiken [bzw. Richtlinien, d. Verf.] und Anweisungen, Prozesse, Verfahren, Organisationsstrukturen sowie Hard- und Softwarefunktionen gehören“ [12, S. 8]. Außerdem müssen diese Maßnahmen „festgelegt, umgesetzt, überwacht, überprüft und bei Bedarf verbessert werden, um sicherzustellen, dass die jeweiligen Sicherheits- und Geschäftsziele der Organisation erreicht“ [12, S. 8] werden können [1, S. 2f]. Dies ist die Hauptaufgabe, welche im Rahmen des Betriebs eines Informationssicherheitsmanagementsystems (ISMS) zu erfüllen ist.
Die Informationssicherheit umfasst viele unterschiedliche Bereiche und Themengebiete. Neben diversen technischen Aspekte sind auch organisatorische Aspekte wie etwa die personelle Sicherheit, die physische und umgebungsbezogene Sicherheit, das Informationssicherheits-Risikomanagement, das Management der Zusammenarbeit mit externen Dienstleistern und Lieferanten sowie die Notfallplanung (bzw. das betriebliche Kontinuitätsmanagement) sowie die Einhaltung von gesetzlichen und vertraglichen Verpflichtungen (Compliance) von großer Bedeutung [1, S. 2f]. Auch bei vorrangig technisch anmutenden Themen sind immer gewisse organisatorische Gegebenheiten zu berücksichtigen. So scheint etwa die Netzwerksicherheit zwar ein technisches Thema zu sein, doch müssen auch hier organisatorische Aspekte wie Pflichten und Verantwortlichkeiten, Dokumentationsanforderungen und Vorgehensweisen, Intervalle von Prüfaktivitäten, Richtlinien etc. geklärt werden.

1.5.1. Unterschied IT-Security, Informationssicherheit und Cybersecurity

Wie in der obigen Beschreibung und Definition deutlich wird, kann der Begriff der Informationssicherheit als sehr weitreichend und umfassender verstanden werden. Im Gegensatz hierzu ist der Begriff der IT-Sicherheit meist eher technischer Natur. Grundsätzlich werden beiden Begriffe jedoch relativ oft synonym verwendet und eine genaue Abgrenzung ist mitunter kaum möglich. Der unterschiedliche Umfang bzw. Geltungsbereich der beiden Begriffe wird in Abbildung 1.1 ersichtlich.
Ein weiterer Begriff, der in der letzten Zeit immer mehr an Popularität gewinnt, ist „Cybersecurity“, wobei sich diese wiederum sehr stark mit dem Begriff der Informationssicherheit überschneidet. Von vielen wird „Cybersecurity“ als Teilbereich der Informationssicherheit gesehen, der sich hauptsächlich mit der Sicherheit im Bezug auf Internet-bezogene Themen befasst, [14, o. S.] [15, o. S.] und bei der die gleichen bzw. ähnliche Themenbereiche im Fokus liegen. Grundsätzlich werden auch diese beide Begriffe relativ oft synonym verwendet. In Abbildung 1.2 wird die Überlappung der Begriffe dargestellt.

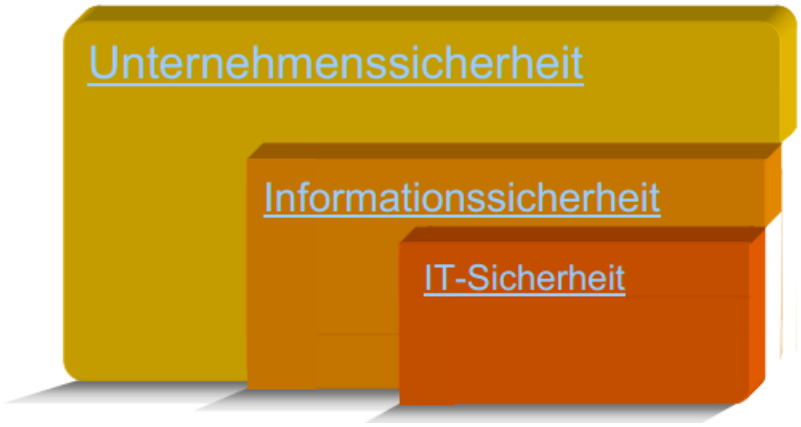

Abbildung 1.1.: Unterschied IT- und Informationssicherheit [13, S. 7]

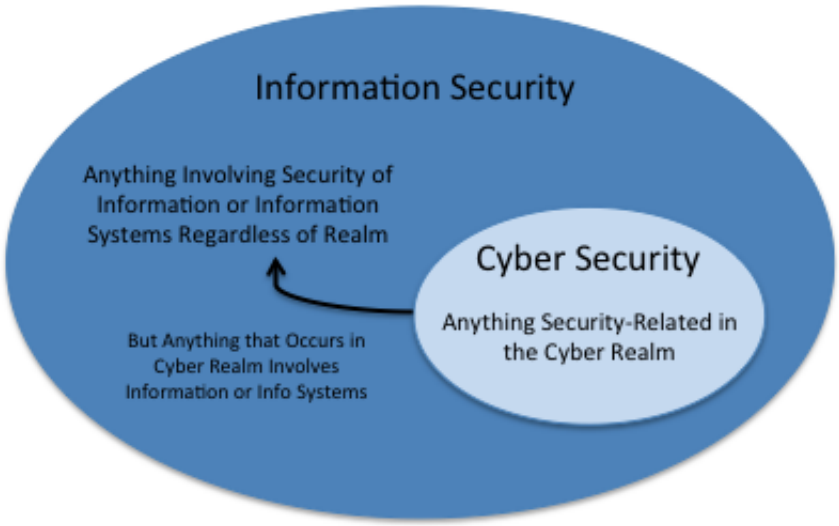

Abbildung 1.2.: Unterschied Cyber- und Informationssicherheit [15, o. S.]

1.6. Aufbau dieser Arbeit

In dem auf die Einleitung folgenden Kapitel 2 wird ein kurzer Überblick über wichtige weltweite und nationale Studien, die sich mit dem Thema Informationssicherheit befassen, gegeben. Außerdem wird vertiefend auf einige deutsche und österreichische Studien in diesem Gebiet eingegangen.

Im Kapitel 3 wird auf die Methodik dieser Studie eingegangen. Außerdem werden der Aufbau und die Themengebiete der eigenen Studie, die Entwicklung und die Inhalte des Fragebogens sowie die Durchführung der Umfrage selbst beschrieben. Außerdem werden zu einigen Themen des Fragebogens vertiefende Informationen geliefert.

Im Kapitel 4 folgt die Darstellung, Auswertung und Interpretation der Ergebnisse der Umfrage. Hierbei wird auf das Teilnehmerfeld und die einzelnen Fragen & Themengebiete eingegangen und es werden die in der Einleitung vorgestellten Hypothesen behandelt. Außerdem wird auf Faktoren, welche sich auf die Aussagekraft dieser Studie (und Studien im Allgemeinen) auswirken und diese beschränken können, aufmerksam gemacht.

Im abschließenden Kapitel 5 befindet sich die Schlussfolgerung mit einer Zusammenfassung der wichtigsten Ergebnisse und es werden Empfehlungen für mögliche weiterführende Studien gegeben. Außerdem werden kurz einige eigene Erfahrungen bezüglich der Erstellung und Durchführung der Studie sowie Rückmeldungen von Teilnehmerinnen und Teilnehmern vorgestellt.

Im Anhang A sind der gesamte Fragebogen der Umfrage inklusive aller Fragen und Begleittexte (A.1) sowie alle Detailergebnisse der einzelnen Fragen (A.3) ersichtlich.

2. Übersicht Informationssicherheits-Studien

Im folgenden Kapitel wird ein Überblick über einige weltweite und nationale Studien gegeben, die das Thema der Informationssicherheit in Unternehmen behandeln. Der Schwerpunkt hierbei wird auf Studien aus Deutschland und Österreich gelegt.

2.1. Weltweite Studien

Weltweit gibt es mehrere Studien, die sich mit dem Thema der Informationssicherheit in Unternehmen beschäftigen. Einige der bekanntesten aktuellen Studien sind:

- Information Week: Strategic Security Survey 2014 [16, S. 1ff]

Die Strategic Security Survey 2014 von Information Week [16, S. 1ff] wurde in über 500 nordamerikanischen Unternehmen durchgeführt und behandelt diverse Themen (Sicherheitsvorfälle, direkt gezielte Angriffe, Sicherheitsausgaben, nützlichste/wirksamste Sicherheitsmaßnahmen, eingesetzte Sicherheitsprodukte, Gefahren, Cloud Computing Risiken etc.) gut und ausführlich. Es gibt viele Statistiken und einen ausführlichen Begleittext.

- Ernst & Young: Global Information Security Survey 2014 [17, S. 1ff]

In der Global Information Security Survey 2014 von Ernst & Young [17, S. 1ff] gibt es zu Beginn einige Fragen zu Themen wie Gefahren und Schwachstellen, die von ungefähr 1800 Teilnehmern in über 60 Ländern beantwortet wurden. Im folgenden Kapitel werden drei Stufen mit Schritten, welche die Verbesserung des Reifegrads des Unternehmens in Bezug auf Cybersecurity zum Ziel haben, behandelt und immer wieder diverse Ergebnisse der Befragung eingebaut. Es werden nicht so viele Themen wie in der Strategic Security Survey behandelt und die Aufbereitung ist nicht ganz so übersichtlich.

- Kaspersky: IT Security Risks Survey 2014 [9, S. 1ff]

Bei der IT Security Risks Survey 2014 von Kaspersky [9, S. 1ff] wurden 3900 Unternehmen in 27 Ländern befragt. Zu Beginn werden Hauptaufgaben der Sicherheitsabteilung abgefragt, während danach auf das Thema Sicherheitsmaßnahmen sowie ausführlich auf externe und interne Bedrohungen eingegangen wird. Auch die Kosten von Sicherheitsvorfällen werden kurz behandelt, wobei viele andere wichtige Themen ausgelassen werden.

- PWC,CIO Magazine, CSO Magazine: Global State of Information Security Survey 2015 [18, S. 1ff]

Die von PWC durchgeführte Global State of Information Security Survey 2015 [18, S. 1ff] ist eine äußerst umfangreiche Studie in knapp 9.700 Unternehmen auf allen Kontinenten. Besonders bemerkenswert ist, dass die Daten nach Region, Industrie und Unternehmensgröße im Internet [19, S. 1ff] aufbereitet sind und gefiltert werden können. Behandelte Themen sind unter anderem Häufigkeit, Quellen, Kosten und Auswirkungen von Sicherheitsvorfällen, Sicherheitsausgaben und Entwicklung dieser sowie Sicherheitsmaßnahmen in Bezug auf Prävention, Erkennung, Reaktion und Schutz.
Das Computer Security Institute (CSI), das regelmäßig eine umfangreiche Studie veröffentlichte ([20, S. 1ff]), existiert anscheinend nicht mehr und auch Deloitte, welches regelmäßig Informationssicherheits Studien veröffentlichte, hat seit 2013 ([21, S. 1ff]) keine globale Studie mehr durchgeführt.
Es gibt auch diverse regelmäßig erscheinende Reports von Antiviren-Herstellern wie etwa Symantec (Internet Security Threat Report) und McAffee Labs (Threats Report) oder anderen Firmen wie FireEye (Threat Report und M-Trends), IBM (X-Force Threat Intelligence) oder Trustwave (Global Security Report). In diesen werden interessante Teilaspekte der Informationssicherheit wie etwa aktuelle Malware, Gefahren im Internet, Datenlecks und Vorfälle in Firmen etc. angesprochen, doch das Thema der Informationssicherheit wird nicht ganzheitlich behandelt, da diese Reports einen etwas anderen, meist engeren Fokus haben.
Zwei Studien, die sich intensiv mit dem Thema Datenlecks und Vorfälle beschäftigen, sind die regelmäßig von dem unabhängigen Forschungsinstitut Ponemon veröffentlichte Studie 2015 Cost of Data Breach Study [22, S. 1ff] sowie der von dem US-amerikanischen Telekommunikationsunternehmen Verizon erstellte, sehr umfangreiche 2015 Data Breach Investigation Report [23, S. 1ff].
Da der Fokus dieser Arbeit die Informationssicherheit in Deutschland, Österreich und der Schweiz ist, werden die weltweiten Studien hier nicht näher beschrieben.

2.2. Studien in Österreich

Es gibt nur wenige Studien zum Thema Informationssicherheit in Unternehmen, welche spezifisch auf den Standort Österreich beschränkt sind. Folgende drei, mittlerweile etwas alte Studien sind in meiner Bachelorarbeit beschrieben [1, S. 12-16]. Zusammenfassend lässt sich allerdings festhalten, dass diese Studien nur mehr eine begrenzte Aussagekraft für den Standort Österreich besitzen und außerdem die letzten beiden nicht frei verfügbar sind.

- L.I. Kurki Diplomarbeit: Informationssicherheit in österreichischen klein- und mittelständischen Unternehmen, [24, S. 1ff]

- Technische Universität Wien und Universität Wien: DAMON - Monitoring zur Datensicherheit in Österreich, [25, S. 1ff]
- ASF: IT-Security in Österreich, [26, S. 1ff]

Es konnte abgesehen von der im Rahmen meiner Bachelorarbeit durchgeführten Studie nur eine weitere Informationssicherheits-Studie für Österreich gefunden werden.

2.2.1. Informationssicherheit in Österreich - Eine Studie zur Informationssicherheit in österreichischen Unternehmen 2013

Diese Studie wurde von mir im Rahmen meiner Bachelorarbeit durchgeführt. In einer Online-Umfrage mit 19 fachspezifischen Fragen wurden 47 Teilnehmerinnen und Teilnehmer zur Informationssicherheitssituation in ihrem Unternehmen befragt. Die behandelten Themen waren die Ausgangsbasis für die in dieser Arbeit durchgeführte Umfrage.
Die Hauptergebnisse waren, dass „sich das Thema Informationssicherheit grundsätzlich durchaus im Blick der meisten Unternehmen befindet und sich eine große Mehrheit der Befragten der Wichtigkeit von korrekten Daten und Informationen sowie der Abhängigkeit von der eigenen IT bewusst ist“ [1, S. 3] und „bezüglich technischer und organisatorischer Maßnahmen zusammengefasst werden kann, dass grundlegende Maßnahmen wie Firewalls, Virenschutz, Backup- und Wiederherstellungsprozeduren sowie Patch- und Update- oder Identitäts- und Zugriffsmanagement beinahe durchgängig vorhanden sind, wobei sich aber in Bezug auf weitreichende oder speziellere Systeme und Maßnahmen, sowie deren Qualität, ein differenzierteres Bild zeigt“ [1, S. 3].
Der Hauptkritikpunkt an dieser Studie war die relativ geringe Anzahl an Beantwortungen, wodurch die Aussagekraft stark vermindert wurde.

2.2.2. Cyber Security Fitness Index Austria

Die Studie „Cyber Security Fitness Index Austria“ wurde 2014 durch das Kuratorium Sicheres Österreich (KSÖ) und einige Partner erstellt. In ihr wurde versucht ein Kennzahlensystem zu entwickeln, um „die unternehmerische Cybersicherheitsvorsorge österreichischer Betreiber der kritischen Infrastruktur zu bewerten“ [27, S. 4]. Die Vorgehensweise basiert auf dem Ansatz der Balanced Scorecard (BSC) über den die Aufstellung der Unternehmen in 4 selbst definierten Dimensionen (Business Value, Security Process, Security Ambition und Resilience) beschrieben werden soll. Für diese Dimensionen wurden über knapp 100 „Indikatoren“ (basierend auf der Beantwortung diverser Fragen) Index Werte berechnet. In den 4 Dimensionen wurden jeweils passende Fragen zu Themen wie IS-Richtlinien, ISMS, Change und

Patch Management, Notfallplanung, Vorfälle, Verfügbarkeit, sichere Softwareentwicklung, Audits und Sicherheitsanalysen etc. gestellt [27, S. 25f].

Für den Cyber Security Fitness Index Austria wurden 30 österreichische Unternehmen aus dem Bereich kritische Infrastruktur (IKT-Sektor, Energieversorgung, Transportsektor, Bankensektor, Gesundheitssektor) befragt. Die Befragung erfolgte in persönlichen Interviews mit den jeweils für die Informationssicherheit verantwortlichen Personen [27, S. 4].

Als Ergebnis wird festgehalten, dass die „unternehmerische Cybersicherheitsvorsorge in den untersuchten kritischen Infrastruktursektoren generell einen hohen Reifegrad erreicht hat“ [27, S. 5] und die für die vier Dimensionen aggregierten Einzelwerte sehr nahe beieinander liegen. Nichtsdestotrotz wird auch Handlungsbedarf aufgezeigt, der „insbesondere bei prozess- und organisationsübergreifenden Vernetzungsaspekten [...] sowie der Ermittlung der Abhängigkeiten zwischen kritischen Prozessen bzw. Services; der Vermittlung der Inhalte der unternehmerischen Cybersicherheitsvorsorge vor allem gegenüber Vertragspartnern und dem Senior Management; dem regelmässigen Test von Notfallplänen in Übungen sowie der Entwicklung geeigneter Führungskenngrössen, die qualifizierte Aussagen über den Nutzen und die Kosten der Maßnahmen im Bereich der Cybersicherheitsvorsorge erlauben“ [27, S. 5] besteht.

Zum Cyber Security Fitness Index Austria ist anzumerken, dass lediglich eine kurze Zusammenfassung der wichtigsten Ergebnisse frei verfügbar ist und er eine sehr starke Fokussierung auf die Ermittlung der Index Werte legt. Bei den meisten Fragen sind Skalen von 1-5 hinterlegt, über die die Unternehmen angeben sollen, wie sehr gewisse Aussagen zutreffen. Diese Werte wurden dann aggregiert und zu einem Index Wert zusammengerechnet (zuerst für die 4 Dimensionen und dann zu einem Gesamt Index). Es ist anzumerken, dass diese Frageart (Bewertung auf Skala 1-5) zu einer gewissen Unschärfe führen kann, da z.B. bei der Frage nach Qualität oder Häufigkeit einer Maßnahme unterschiedliche Personen unter „sehr gut“ bzw. „sehr häufig“ etwas Verschiedenes verstehen (dies kann nur bedingt durch den Interviewer/die Interviewerin ausgeglichen werden). Unter Berücksichtigung der Absicht einen Index Wert zu errechnen ist diese Art der Fragestellung jedoch notwendig.

Im Vergleich zu anderen Informationssicherheits-Studien ist es sehr auffällig, dass in der gesamten Auswertung nur über die Berechnung von Index Werten vorgegangen wird und es keine prozentuellen Auswertungen, wie viele % der Unternehmen gewisse Maßnahmen ergriffen haben oder bestimmte Fragen wie beantwortet haben, gibt (etwa: X% der Unternehmen antworteten eine gewisse Maßnahme implementiert zu haben oder von Vorfällen betroffen gewesen zu sein). Außerdem wird lediglich der IKT Sektor abgedeckt, wodurch die Aussagekraft für „normale“ Unternehmen nur sehr begrenzt ist.

KMU Cyber Security Monitor

Im Rahmen des Cyber Security Fitness Index Austria wurde ein Fragebogen für einen KMU Cyber Security Monitor erarbeitet. Hierbei wurden auf Basis telefonischer Interviews insgesamt 478 KMU in Österreich zu IT-Nutzung und Cybersicherheit befragt, wobei diverse Fragen zu Gefahren, Sicherheitsmaßnahmen, im Unternehmensalltag genutzten elektronischen Diensten etc. gestellt wurden [27, S. 6].
Bezüglich Gefahren wird beschrieben, dass „SPAM, Schadsoftware und Phishing [...] von der überwiegenden Mehrheit der Antwortenden als größte Gefahr interpretiert [werden, d. Verf.]“ [27, S. 40f]. Es wird erklärt, dass sich diese Aussage mit der effektiven Gefährdung (bzw. tatsächliche Vorfällen) der Unternehmen deckt, da die meisten Befragten angaben, von SPAM-Mails (81%) bzw. Schadsoftware (65 %) betroffen gewesen zu sein, wobei Phishing nur für eine Minderheit (30 %) ein Problem darstellte [27, S. 6,S. 40f]. Richtigerweise wird aber darauf hingewiesen, dass Opfern gewisse verdeckte Angriffe (wie Datendiebstahl oder Manipulationen) „oftmals gar nicht bewusst sind und sie beispielsweise erst durch Dritte darauf hingewiesen werden,, [27, S. 6,S. 40f], wodurch die Zahlen zu Gefährdungen und Vorfällen vorsichtig zu interpretieren sind.
Zu Sicherheitsmaßnahmen wird erklärt, dass die „überwiegende Mehrheit der Befragten auf bewährte Mittel der Cybersicherheit wie Virenschutz, Spamfilter und Firewall setzt. Hinzu kommen regelmäßige Softwareaktualisierungen, Patches sowie Passwortschutz“ [27, S. 41]. Andere Maßnahmen, etwa in Bezug auf die Netzwerküberwachung und -sicherheit (IDS, IPS, URL-Filtering, Penetration Testing, VPNs etc.) spielten bei den befragten Unternehmen jedoch kaum eine Rolle.
Der KMU Cyber Security Monitor wird nur als kleiner Teil im Abschlussbericht zum Cyber Security Fitness Index Austria behandelt und ist nicht frei verfügbar. Der Fragebogen des KMU Cyber Security Monitor ist allerdings im Anhang enthalten und es fällt auf, dass in der relativ kurz gehaltenen Auswertung (knapp 7 Seiten) nicht alle der gestellten Fragen behandelt wurden.

2.3. Studien in Deutschland

Im Vergleich zu Österreich konnten in Deutschland mehrere aktuelle Studien zum Thema Informationssicherheit gefunden werden.

2.3.1. Cyber-Sicherheits-Umfrage 2014

Die Cyber-Sicherheits-Umfrage 2014 wurde vom BSI durchgeführt. In ihr wurden 257 deutsche Unternehmen mit Schwerpunkt auf das Thema Cyber-Angriffe befragt [8, S. 1ff]. Weiters wurden Fragen zu Sicherheitsbudget und umgesetzten Sicherheitsmaßnahmen sowie zum Einsatz und der Verbreitung von verschiedenen Betriebssystemen gestellt.

Eine knappe Mehrheit von 56% der Befragten gab an, in den letzten drei Jahren bereits Ziel von Cyber-Angriffen gewesen zu sein, wobei diese in wenigstens einem Drittel der Fälle der Angriff erfolgreich waren [8, S. 3f]. Die am häufigsten genannten Angriffe waren gezielte und ungezielte Malware-Infektionen sowie DDOS Angriffe auf den Internetauftritt [8, S. 5]. 38,5% der Befragten gaben an überhaupt (beliebiger Zeitraum) schon einmal von einem erfolgreichen Cyber-Angriff betroffen gewesen zu sein [8, S. 6].

Als häufigste Sicherheitsmaßnahmen werden die Absicherung von Netzübergängen (Sicherheitsgateways, Firewall usw.), zentrale und dezentrale Abwehr von Schadprogrammen (Scan am Client + Server sowie Sicherheitsgateway und Mail), Segmentierung von Netzen sowie Minimierung von Netzübergängen und Patchmanagement genannt [8, S. 16].

Interessant beim Einsatz von Betriebssystemen war, dass lediglich 35% der Organisationen angaben, Windows XP gar nicht einzusetzen. Zusätzlich zu 24,1% keine Angabe gaben 31,5% an, in einem „geringen“ Umfang (bis zu 25% der Systeme) noch auf Windows XP zu setzen [8, S. 18].

Die Ergebnisse der BSI Cyber-Sicherheits-Umfrage sind frei verfügbar. Das Dokument ist jedoch sehr schlicht gehalten und es gibt kaum erklärenden Begleittexte oder Grafiken. In Bezug auf Angriffe und Vorfälle werden sehr gute Informationen geliefert. Im Vergleich zu umfangreichen Informationssicherheits-Studien werden allerdings nur relativ wenige Themen behandelt.

2.3.2. Bitkom-Umfrage 2015

In einer Studie des Digitalverbands BITKOM wurden Geschäftsführer und Sicherheitsverantwortliche von 1.074 Unternehmen repräsentativ befragt. Eines der wichtigsten Ergebnisse ist, dass gut die Hälfte (51 Prozent) aller Unternehmen in Deutschland in den vergangenen zwei Jahren von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl betroffen gewesen ist, wobei weitere 28 Prozent vermuteten, dass es auch bei ihnen zu einem solchen Vorfall gekommen sein könnte [28, o. S.].

Es wird beschrieben, dass „das am häufigsten auftretende Delikt der Diebstahl von IT- und Kommunikationsgeräten ist: In 28 Prozent der befragten Unternehmen sind in den letzten zwei Jahren zum Beispiel Computer, Smartphones oder Tablets gestohlen worden. Fast ein Fünftel (19 Prozent) registrierten Fälle von Social Engineering. [..] 17 Prozent der befragten Unternehmen berichten vom Diebstahl sensibler elektronischer Dokumente bzw. Daten und 16 Prozent von Sabotage ihrer IT-Systeme oder Betriebsabläufe. Bei 8 Prozent der Unternehmen ist die elektronische Kommunikation ausgespäht worden“ [28, o. S.].

Zu Tätern wird festgehalten, dass „nach den Ergebnissen der Umfrage vor allem aktuelle oder ehemalige Mitarbeiter als Täter in Erscheinung treten. Gut die Hälfte (52 Prozent) der betroffenen Unternehmen

gibt diesen Personenkreis an. [...] Die zweite große Tätergruppe mit 39 Prozent umfasst das unternehmerische Umfeld, bestehend aus Wettbewerbern, Lieferanten, Dienstleistern und Kunden. 17 Prozent nennen Hobby-Hacker als Täter. 11 Prozent sind Opfer organisierter Bandenkriminalität geworden und 3 Prozent standen im Visier ausländischer Geheimdienste. Bei 18 Prozent ist der Täterkreis unbekannt“ [28, o. S.].

Ein Artikel mit den Ergebnissen der BITKOM-Umfrage ist frei verfügbar. Außerdem werden in einem Dokument Grafiken und Statistiken zur Verfügung gestellt. In Bezug auf Angriffe und Vorfälle werden sehr gute Informationen geliefert. Im Vergleich zu umfangreichen Informationssicherheits-Studien werden allerdings ebenfalls nur relativ wenige Themen behandelt.

2.3.3. IT-Sicherheit und Datenschutz 2015

Bei der von der NIFIS (Nationale Initiative für Informations- und Internet-Sicherheit) durchgeführten Studie wurden 100 deutsche Fach- und Führungskräfte persönlich befragt [29, S. 1ff].

In dieser Studie wird nicht detailliert auf die Sicherheitssituation in Unternehmen selbst eingegangen, sondern es wird die Meinung zu Themen wie den Trends im Bereich Informations- und IT-Sicherheit 2015, Entwicklung der Ausgaben für IT-Sicherheit, Mehrwert, IT-Risiken und Sicherheitsaspekte beim Cloud Computing, der Schutz vor Spähattacken, Richtlinien und BYOD abgefragt.

Eines der Ergebnisse ist, dass „der Bedarf an IT-Sicherheitstechnologie auch in den nächsten Jahren weiter stark wachsen [wird. So, d. Verf.] [...] geht fast die Hälfte der Unternehmen (45 Prozent) von einer Verdopplung der Ausgaben für IT-Sicherheit und Datenschutz bis 2020 aus. In der Vorgängerstudie für das Jahr 2014 waren es noch 34 Prozent“ [29, S. 7].

Eine Zusammenfassung der wichtigsten Ergebnisse ist frei verfügbar. Da in den Fragen aber nicht detailliert auf die Sicherheitssituation in Unternehmen selbst eingegangen wird (getroffene Maßnahmen, Stellenwert der Informationssicherheit, Vorfälle etc.), sind die Ergebnisse nur bedingt nutzbar.

2.3.4. Studie: Industriespionage 2014

Die Studie: Industriespionage 2014 wurde von Corporate Trust durchgeführt [7, S. 1ff]. In ihr wurden 530 Unternehmen in Deutschland und Österreich befragt. Der Schwerpunkt dieser Studie sind Spionageangriffe (Industriespionage). Da diese jedoch oft auf die IT abzielen, werden in der Umfrage auch diverse Informationssicherheitsthemen behandelt.

Zum Thema Spionage wird festgehalten, dass „jedes zweite Unternehmen in den vergangenen beiden Jahren einen Spionageangriff oder Verdachtsfall zu beklagen [hatte, d. Verf.]. Konkret waren 26,9 Prozent in Deutschland und 27 Prozent in Österreich von einem konkreten Vorfall betroffen. Weitere 27,4 Prozent (Deutschland) bzw. 19,5 Prozent (Österreich) hatten zumindest einen Verdachtsfall“ [7, S. 8].

Zu Angriffsform wird beschrieben, dass „sich die Täter aktuell immer mehr auf elektronische Angriffe zu fokussieren scheinen. 49,6 Prozent der Unternehmen in Deutschland und 41,8 Prozent der österreichischen Firmen gaben an, dass Hackerangriffe auf EDV-Systeme und Geräte die häufigste Form der Spionage war. An zweiter Stelle lag [...] das Abhören bzw. Abfangen von elektronischer Kommunikation. In Deutschland konnte bei 41,1 Prozent der Fälle ein solcher Datenzugriff festgestellt werden, in Österreich bei 40,0 Prozent. Social Engineering belegt in der Statistik in Deutschland nur noch den dritten Platz (38,4 Prozent der Fälle), in Österreich gar nur den fünften Platz (18,2 Prozent der Fälle)“ [7, S. 9, S. 25].

Weiters wird auf die Schäden durch Industriespionage, Täter und deren Herkunft sowie die Verbreitung und der Wert von Cyber Versicherungen eingegangen. Eine große Frage behandelt auch das Thema der im IKT-Bereich getroffenen Sicherheitsvorkehrungen, um sich gegen Spionage/Informationsabfluss zu schützen. Hier sind Standard-Sicherheitsmaßnahmen wie die „Absicherung des internen Firmennetzwerks gegen Angriffe von Außen (z. B. durch Firewall etc.)“ oder „Passwortschutz auf allen Geräten“ am verbreitetsten, während Themen wie „Verschlüsselter E-Mail-Verkehr“, „Sicherheitszertifizierung“ oder „DLP“ nur kaum Beachtung finden [7, S. 45]. Darauf folgend werden auch im Personal- und baulichen Bereich getroffene Maßnahmen beschrieben [7, S. 53ff].

In Bezug auf zukünftige Maßnahmen wir beschrieben, dass „nach wie vor [...] technische Maßnahmen als am wichtigsten erachtet [werden, d. Verf.]. Bezüglich der Frage, welche Vorkehrungen die Unternehmen in Zukunft treffen wollen, um auf die Risiken durch Industriespionage vorbereitet zu sein, waren in Deutschland 52,7 Prozent und in Österreich 48,3 Prozent der genannten Maßnahmen technischer Natur“ [7, S. 75ff]. Bei den technischen Maßnahmen wurden die „Sicherung der Netzwerkinfrastruktur (Firewalls, IDS, IDP etc.)„ sowie „strengere Regelungen bei den Zugriffs- und Zutrittsberechtigungen“ als die wichtigsten Themen angesehen.

Die Studie ist frei verfügbar. Das Dokument enthält ausführliche Begleittexte und Grafiken. Es muss jedoch festgehalten werden, dass Informationssicherheitsthemen nicht im Hauptfokus dieser Studie liegt.

2.3.5. Security-Bilanz Deutschland

Die Studie Security Bilanz Deutschland ist ein Gemeinschaftsprojekt von Techconsult und des Heise Zeitschriften Verlags mit diversen Unternehmen und Organisationen wie etwa dem BSI, BITKOM oder der TeleTrust. Sie wurde Anfang 2014 durchgeführt und an ihr nahmen 503 Unternehmen teil. Es ist vorgesehen, die Studie jährlich zu wiederholen und seit Ende Juli 2015 ist eine neue Version verfügbar [30, S. 3, S. 27].

Das „Ziel des Projektes ist, die Themen IT-Sicherheit und Informationssicherheit im Mittelstand umfassend zu betrachten. Zentrales Anliegen war dabei, mittelständische Unternehmen dabei zu unterstützen, die eigene IT- und Informationssicherheit zu verbessern“ [30, S. 3f]. Die Studie „liefert ein umfassendes Gesamtbild, wie der deutsche Mittelstand hinsichtlich IT- und Informationssicherheit aufgestellt ist“ [30, S. 3f].

Das Besondere an dieser Studie ist, dass die Studienergebnisse als Basis für einen Online-Self-Check (Heise Security Consulter) genutzt werden, der Unternehmen bei der Standortbestimmung hinsichtlich ihrer IT-Sicherheit unterstützen soll [30, S. 4f].

Der Fragebogen umfasste ca. 40 Fragen, wobei unter anderem folgende Themen:“

- Relevanz, Anforderungen und Umsetzung von IT- und Informationssicherheit in verschiedenen Unternehmensbereichen
- Maßnahmen, Regelungen und Strategien zur IT- und Informationssicherheit, untergliedert in vier Ebenen:
  - Technische Ebene
  - Organisatorische Ebene
  - Rechtliche Ebene
  - Strategische Ebene
- Bedrohungslage, Ausfälle und Handlungsbedarf im letzten Jahr

behandelt werden“ [30, S. 6].

Interessant an der Befragung zu Maßnahmen ist, dass diese in Form eines „Relevanz-Umsetzungs-Schema“ erhoben werden, wobei untersucht wird, „welche Maßnahmen und Lösungen [...] für die Unternehmen wichtig sind und wie zufrieden die Unternehmen mit deren Umsetzung sind“ [30, S. 5]. Dies scheint eine sehr vernünftige Vorgehensweise zu sein, da unterschiedliche Maßnahmen für unterschiedliche Unternehmen mehr oder weniger Sinn machen können und somit eine genauere Berechnung des Index Werts ermöglicht wird. Außerdem könnte ebenfalls untersucht werden, welche Maßnahmen von Unternehmen insgesamt öfter/seltener als relevant angesehen werden. Auch die Frage nach der Zufriedenheit mit der Umsetzung ist sehr gut, da somit erkannt werden kann, in welchen Bereichen und Maßnahmen Unternehmen noch Defizite sehen.

In dem Bericht wird nun für unterschiedliche Branchen ein Sicherheitsindex berechnet. Es wird beschrieben, dass „der Indexwert für das Sicherheitspotenzial [...] im Gesamtdurchschnitt 57 von 100 Punkten [erreicht, d. Verf.]. Dieses Niveau zeigt deutlich, dass der Mittelstand noch weit von einer vollständigen

Beherrschung der relevanten Sicherheitsaspekte entfernt ist. Weiterhin offenbart sich, dass es deutliche Unterschiede zwischen den Branchen gibt. So führt die Industrie mit 60 Indexpunkten knapp vor den Banken und Versicherungen mit 59 Punkten das Feld an. Die Dienstleister liegen mit 57 Punkten genau im Durchschnitt. Öffentliche Verwaltungen und Non-Profits liegen mit 54 Punkten drei Zähler unter dem Schnitt, das Schlusslicht bildet der Handel mit nur 52 Punkten“ [30, S. 7].

Es wird auch versucht einen Gefährdungsindex zu bilden, der über die von Unternehmen wahrgenommene Bedrohung, sowie Unzufriedenheit oder Zufriedenheit mit der Umsetzung des eigenen Schutzes berechnet werden soll [30, S. 8f].

Es folgt eine genaue Analyse der verschiedenen Ebenen, in der detailliert auf die Ergebnisse eingegangen wird und in der sich deutlich zeigt, „dass die Performance auf technischer und rechtlicher Ebene deutlich besser ausfällt, als auf organisatorischer oder strategischer Ebene“ [30, S. 11ff].

In einem zweiten Bericht zu der Studie wird umfassend auf die Maßnahmenumsetzung eingegangen, wobei nicht mehr die Indices selbst im Fokus stehen [10, S. 1ff]. In drei Kapiteln („Bedrohungsszenarien - (subjektive) Relevanz und Einschätzung des aktuellen Schutzes“, „Umsetzung von IT- und Informationssicherheit in Geschäftsbereichen“, „Umsetzung von IT- und Informationssicherheit nach Handlungsfeldern“) folgt eine genaue Aufarbeitung von wahrgenommenen Bedrohungen, der Qualität und dem Grad der Umsetzung von IT- und Informationssicherheit in einzelnen Geschäftsbereichen (Marketing, IT, Personalwesen, Vertrieb etc.) sowie der Umsetzung von IT- und Informationssicherheit auf technischer, rechtlicher, strategischer und organisatorischer Ebene.

In der Managment Summary werden die wichtigsten Ergebnisse beschrieben. Es wird festgehalten, dass “keines der genannten Bedrohungsszenarien von mehr als 40 Prozent aller befragten Unternehmen als relevant erachtet wird“ [10, S. 5f] und „dies nicht nur der deutliche Beleg eines gering ausgeprägtes Problembewusstseins ist, sondern es vielmehr eine völlige Fehleinschätzung der aktuellen Bedrohungslage, sowie der Reichweite möglicher Konsequenzen erfolgreicher Cyber-Angriffe [dokumentiert, d. Verf.]“ [10, S. 5f].

Weiters wird erklärt, dass „in den Unternehmen [...] ein Umsetzungsgefälle zwischen strategischen und operativ tätigen Arbeitsbereichen [besteht, d. Verf.]“ [10, S. 5f], und „rund 60 Prozent der befragten Unternehmen [...] in den Marketingabteilungen die größten Defizite [ausmachten, d. Verf.]“ [10, S. 15] wobei mit geringem Abstand weitere operativ tätige Abteilungen (Verkauf, Einkauf) folgten. Auch die Umsetzung von Schutzmaßnahmen in den strategisch tätigen Geschäftsbereichen der Geschäftsleitung, IT-Organisation und Finanzen/Controlling wurde nur leicht besser beurteilt [10, S. 15].

Bezüglich der Umsetzung von IT- und Informationssicherheit auf technischer, rechtlicher, strategischer und organisatorischer Ebene wird beschrieben: „

- Die Umsetzung einfacher technischen Lösungen, wie Anti-Viren und Anti-Malware Tools weist bereits deutliche Defizite auf. Rund 60% der befragten Unternehmen muss somit ein ungenügender Basisschutz attestiert werden.
- Anspruchsvollere technische Lösungen, wie Maßnahmen und Lösungen zur Datenverschlüsselung oder sicheren Kollaboration, werden vom Großteil der mittelständischen Unternehmen gar nicht, oder unzureichend umgesetzt. Mehr als die Hälfte der befragten Unternehmen haben massiven Nachholbedarf bei der Umsetzung von Verschlüsselungslösungen.
- Sehr anspruchsvolle Lösungen, wie Unified Threat Managament, Intrusion Detection oder Data-Loss-Prevention sind bei der Mehrzahl der Unternehmen gar nicht oder unzureichend umgesetzt.
- Organisatorische Maßnahmen, wie die Klassifizierung von Daten und Prozessen, die Schulung von Mitarbeitern sowie der Einsatz von Richtlinien und die Simulation von Ernstfallszenarien findet im überwiegenden Teil der befragten Unternehmen keine erfolgreichen Einsatz.
- Die rechtliche Absicherung, in Form der Definition von Zuständigkeiten und der Haftungsfragen im Ernstfall, aber auch der Einsatz von Geheimhaltungsvereinbarungen weist in mindestens der Hälfte der Unternehmen massive Defizite auf.
- Strategische Maßnahmen, wie die Festlegung einer unternehmensweiten IT-Security-Strategie oder die Abstimmung von Personal- und Budgetplanung auf den IT-Security-Bereich wird bei rund 60% der befragten Unternehmen nicht hinreichend umgesetzt“ [10, S. 5f].

Diese Studie ist äußerst umfassend und die verschiedenen Bereiche der Informationssicherheit werden sehr gut abgedeckt. Eine Zusammenfassung der wichtigsten Ergebnisse ist frei verfügbar. Nach einer kostenlosen Registrierung ist auch der vollständige Bericht (zwei Teile) erhältlich. Außerdem soll abermals auf den für Unternehmen kostenlos zur Verfügung stehenden Online-Self-Check (Heise Security Consulter) hingewiesen werden, der auf dieser Studie basierend die gleichen Themengebiete und Fragen abdeckt und Unternehmen bei der Bestimmung des eigenen Sicherheitsniveaus unterstützen kann.

2.3.6. <kes>/Microsoft-Sicherheitsstudie 2014

Die <kes>/Microsoft-Sicherheitsstudie wird bereits seit über 20 Jahren von den beiden Hauptverantwortlichen Unternehmen <kes>, einer Fachzeitschrift für Informationssicherheit, und dem Softwarehersteller Microsoft durchgeführt. Es handelt sich hierbei um eine sehr umfangreiche Studie zur Lage der Informationssicherheit im deutschsprachigen Raum mit starkem Fokus auf Deutschland.

Die aktuellste Studie wurde im Jahr 2014 durchgeführt, wobei lediglich eine Zusammenfassung der Ergebnisse frei verfügbar ist (sowie eine Präsentation zur Vorstellung der Ergebnisse bei einer Konferenz [31, o. S.]). Einige der älteren Versionen sind frei im Internet abrufbar.

Die Studie weist einen äußerst umfangreichen Fragebogen auf, der 2014 von 133 teilnehmenden Unternehmen beantwortet wurde. Es wird explizit erwähnt, dass die Studie keinen Anspruch auf Repräsentativität erhebt und die Teilnehmerinnen und Teilnehmer „tendenziell als besonders sicherheitssensitiv gelten müssen, wodurch es außerhalb der erfassten Stichprobe eher noch deutlich schlechter um die Informations-Sicherheit stehen dürfte“ [32, o. S.].

Die in der Zusammenfassung aufgeführten wichtigsten Ergebnisse sind [32, o. S.]:„

- 74 % der Studienteilnehmer gaben an, dass sie in den letzten zwei Jahren generell von Malware-Vorfällen betroffen waren, wobei 31 % tatsächliche nennenswerte Schäden hatten.
- Bei den Infektionswegen in die Unternehmen hinein liegt die E-Mail weiterhin an der Spitze, gefolgt von WWW-Inhalten, die eine Infektion über aktive Inhalte oder 'Drive-by'-Attacken bewirken.
- Erneut war mehr als die Hälfte der Befragten mutmaßlich Opfer von Vertraulichkeitsbrüchen - als wichtigste Ursache trat die neue Kategorie 'Datenlecks/Probleme bei Partnern' auf, gefolgt vom Verlust und Diebstahl von Speichermedien sowie mobilen Systemen.
- Die schlechteste Sicherheitseinschätzung erhalten erneut mobile Endgeräte (Smartphones, Tablets & Co.) sowie Speichermedien.
- industrielle IT-Systeme liegen auf dem Niveau von Telearbeitsplätzen.
- Über 80% der Teilnehmer besitzen eine schriftliche Strategie zur Informations-Sicherheit - die Bereitschaft, Konzepte und Maßnahmen schriftlich zu fixieren, nimmt erneut zu.
- Die organisatorische Umsetzung von Policies in die Praxis nennt erneut fast ein Viertel nicht oder gerade einmal ausreichend im Mittel ergibt sich eine 'befriedigende' Umsetzung.
- Verstöße gegen Gesetze, Vorschriften und Verträge bleiben wichtigstes Kriterium zur Risikobewertung - etwa ein Viertel verzichtet weiterhin auf eine Risikoklassifizierung von Anwendungen und Systemen.
- ISO 2700x erhält erstmals höhere praktische Bedeutung zuerkannt als IT-Grundschutz - das deutsche Telemediengesetz erlangt höhere Aufmerksamkeit, der Umsetzungsgrad entsprechender Maßnahmen bleibt jedoch auf dem früheren Niveau.
- Es fehlt wieder häufiger an Geld/Budget, um die Informations-Sicherheit zu verbessern - häufigstes Hindernis bleibt jedoch mangelndes Bewusstsein bei Mitarbeitern.“ [32, o. S.].

Generell ist zur festzuhalten, dass diese Studie äußerst umfassend ist und die verschiedenen Bereiche der Informationssicherheit sehr gut abgedeckt werden. Da die gesamte Studie leider nicht frei verfügbar ist, kann hier nicht näher auf sie eingegangen werden. Eine Beschreibung der wichtigsten Ergebnisse der 2012 durchgeführten <kes>/Microsoft-Sicherheitsstudie findet sich in [1, S. 9f].

2.4. Zusammenfassung

In Abbildung 2.1 wird ein Überblick über wichtige Grundinformationen zu allen Studien, welche in diesem Kapitel angesprochen wurden, gegeben. Es ist ersichtlich von wem die Studie herausgegeben wurde, ob diese regelmäßig durchgeführt wird (und es daher auch Vergleichsdaten zu vergangenen Jahren gibt), welche Erhebungsmethode verwendet wurde und ob die Methodik bzw. Vorgehensweise in der jeweiligen Studie beschrieben ist. Außerdem ist auch die Anzahl der teilnehmenden Unternehmen, deren Herkunft (Land) und Größe sowie die Verfügbarkeit (frei oder nicht) der Studie aufgeführt.
Es ist sofort zu erkennen, dass die weltweiten Studien, welche von bekannten großen Organisationen durchgeführt werden, relativ hohe Teilnehmerzahlen haben und auch mitunter sehr große Unternehmen abdecken. Die durchschnittlichen Studien in Österreich und Deutschland haben kaum mehr als wenige hundert Teilnehmerinnen und Teilnehmer. Weiters ist auch erkennbar, dass die vier vorgestellten globalen Studien schon mehrmals durchgeführt wurden, während dies bei nur wenigen der vorgestellten deutschen und österreichischen Studien der Fall ist. Der Großteil der Studien ist frei verfügbar und alle weisen zumindest eine rudimentäre Methodenbeschreibung auf. Als Erhebungsmethode werden am häufigsten Online Befragungen und (telefonische) Interviews genutzt.
Zusammenfassend kann festgehalten werden, dass insbesondere für Österreich kaum (aktuelle und umfassende) Studien verfügbar sind. In Deutschland sind durchaus einige Studien und Umfragen verfügbar, wobei in Bezug auf Umfang und Themenabdeckung hier besonders die Security-Bilanz Deutschland und die <kes>/Microsoft-Sicherheitsstudie hervorgehoben werden können. Die BSI Cyber-Sicherheits-Umfrage und die Bitkom-Umfrage 2015 liefern in Bezug auf die Teilgebiete Angriffe und Vorfälle ebenfalls gute Informationen.
Bezüglich der weltweiten Studien stellt sich die Frage, inwiefern diese für Deutschland und Österreich aussagekräftig sind und ob daher von ihnen ausgehend Rückschlüsse auf die derzeitige Situation der Informationssicherheit in Deutschland, Österreich und der Schweiz zulässig sind.
Meiner Meinung nach können hierzu folgende Punkte festgehalten werden (wie auch in [1, S. 15]):

- Die Studien sind auf sehr große Unternehmen (in Bezug auf Mitarbeiter und verfügbares Budget) bezogen bzw. ausgerichtet
- Die Studien beziehen sich auf andere geographische Regionen mit anderen rechtlichen und gesellschaftlichen Rahmenbedingungen (etwa auch in Bezug auf Datenschutz & -sicherheit)
- Die Themenabdeckung ist meist nicht so hoch wie etwa bei der Security-Bilanz Deutschland und der <kes>/Microsoft-Sicherheitsstudie

- Diese großen Studien besitzen daher eine eher beschränkte Aussagekraft für Deutschland, Österreich und die Schweiz

Diese Gründe sprechen dafür, dass durchaus der Bedarf an einer aktuellen Studie zur Informationssicherheitssituation (insbesondere in österreichischen Unternehmen) gegeben ist. Im Folgenden soll nun versucht werden diesen Bedarf, zumindest ansatzweise, abzudecken und einen Beitrag zur Beschreibung der derzeitigen Informationssicherheitssituation in Deutschland, Österreich und der Schweiz zu leisten.

Studie	Herausgeber	Jahr	regelmäßig durchgeführt?	Erhebungsmethode	Methodenbeschreibung	Regionen/Länder	Anzahl Teilnehmer	Unternehmensgröße	frei verfügbar
IT Security Risks Survey 2014	Kaspersky	2014	regelmäßig, 4te Version	Befragung	Ja, p 4f	weltweit, 27	3.900	< 250 - > 50.000	Ja
Global State of Information Security Survey 2015	PWC	2015	regelmäßig	Online Befragung	Ja, p 35	weltweit, 154	9.700	keine Angaben	Ja
2014 Strategic Security Survey	Information Week	2014	regelmäßig, 17te Version	Online Befragung	Ja, p 5, 41ff	Nordamerika	536	< 100 - > 10.000	Ja
EY Global Information Security Survey 2014	Ernst & Young	2014	regelmäßig, 17te Version	Interviews & Online Befragung	Ja, p 34f	weltweit,60	1.825	< 1000 - > 50.000	Ja
Studie: Industriespionage 2014	Corporate Trust	2014	regelmäßig, 3te Version (2007, 2012, 2014)	Offline & Online Fragebogen & telefonischen Interviews	Ja, p10	Deutschland, Österreich	530	Kleinunternehmen, Mittelstand, Konzerne	Ja
Ergebnisse der Cyber-Sicherheits-Umfrage 2014	BSI	2014	einmalig (bisher)	Online Befragung	Ja, p 2	Deutschland	257	< 10 - > 10.000	Ja
kes/Microsoft-Sicherheitsstudie 2014	SecuMedia	2014	regelmäßig (alle 2 Jahre)	Offline & Online Fragebogen	Ja,	Deutschland; (Schweiz, Österreich)	133	< 100 - < 100.000	Nein
Bitkom-Umfrage 2015	BITKOM	2015	einmalig (bisher)	telefonischen Interviews	Ja	Deutschland	1.074	> 10 - > 500	Ja
IT-Sicherheit und Datenschutz 2015	NIFIS	2015	einmalig (bisher)	Interviews	Ja	Deutschland	100	keine Angaben	Ja
Security-Bilanz Deutschland 2014	Techconsult	2014	einmalig, geplant jährlich	Online Befragung	Ja, p 27ff	Deutschland	503	> 20 - < 2.000	Ja
Informationssicherheit in Österreich - Eine Studie zur Informationssicherheit in österreichischen Unternehmen 2013	Philipp Reisinger	2013	einmalig, Nachfolger 2015	Online Befragung	Ja, p 17f	Österreich	47	> 1-9 - > 250	Ja
Cyber Security Fitness Index Austria 2015	KSÖ	2015	einmalig (bisher)	Interviews	Ja, p 15ff, p25f	Österreich	30	keine Angaben	Nein
KMU Cyber Security Monitor 2015	KSÖ	2015	einmalig (bisher)	telefonischen Interviews	Ja, p 38	Österreich	457	> 1-9 - > 250	Nein

	Weltweit
	Deutschland
	Österreich

Abbildung 2.1.: Übersicht Studien Informationssicherheit

3. Methodik, Fragebogendesign & Verteilung

Im folgenden Kapitel wird auf die Methodik dieser Studie eingegangen. Außerdem werden der Aufbau und die Themengebiete der eigenen Studie, die Entwicklung und die Inhalte des Fragebogens sowie die Durchführung der Umfrage selbst beschrieben. Zu wichtigen Themengebieten des Fragebogens werden einige vertiefende Informationen geliefert

3.1. Methodik

Bei der Erstellung dieser Studie wurde nach der in der Abbildung 3.1 dargestellten Vorgehensweise verfahren. Die einzelnen Schritte sollen hier nun näher beschrieben werden.

Abbildung 3.1.: Vorgehensweise Studie

Zu Beginn der Arbeit wurde eine umfangreiche Literaturrecherche durchgeführt, wobei einige der untersuchten Arbeiten bereits in Kapitel 2 beschrieben sind. Es sollten andere Informationssicherheits-Studien gefunden werden, welche dann in Hinblick auf deren Methodik (Art der Durchführung, Fragebogenumfang etc.) sowie auf die behandelten und abgedeckten Themenfelder untersucht wurden. Außerdem sollten auch Ideen zum Fragendesign (offen/geschlossen, Art der Fragestellung etc.) und anhand der Ergebnisse der Studien Ideen für mögliche Hypothesen für die eigene Studie ermittelt werden.
Nach den Literaturrecherche wurde die forschungsleitende Fragestellung und die Hypothesen festgelegt. Die Hypothesen basieren auf den Ergebnissen meiner letzten Studie sowie auf Ergebnissen diversen andere Informationssicherheits-Studien und Berichte. Manche Hypothesen behandeln auch in der Informationssicherheits-Branche weit verbreitete Annahmen bzw. Feststellungen (z.B. die technische Aufstellung der Unternehmen ist oft besser als die organisatorische, insbesondere in kleinen Unternehmen ist die Nutzung von Standards/Empfehlungen im Bereich der Informationssicherheit nicht sehr weit verbreitet).
Nach dem Erstentwurf der Hypothesen wurden diese mit einigen Expertinnen und Experten besprochen und darauffolgend mit meinem Betreuer abgestimmt und finalisiert. Hierbei kam es noch zu diversen kleineren Anpassungen und Optimierungen.

Aufbauend auf den Hypothesen, den in anderen Informationssicherheits-Studien behandelten Themen sowie auf meiner vorigen Studie wurden die Themengebiete der Umfrage festgelegt und ein erster Entwurf des Fragebogens erstellt. Dieser wurde in 5 große Bereiche unterteilt, in welchen in 21 Fragen diverse Informationssicherheits-bezogene Themen möglichst umfassend behandelt werden sollen. Die behandelten Themengebiete werden im Kapitel 3.2.1 genauer beschrieben. Grundsätzlich wurde bei der Fragengestaltung versucht eher einen groben bzw. breiten Überblick über alle für Unternehmen relevanten Informationssicherheits-Themen abzufragen, wobei es Teilnehmerinnen und Teilnehmern mit grundlegendem IT- und Informationssicherheitswissen möglich sein sollte, die Fragen zu beantworten.
Dieser Entwurf des Fragebogens wurde nach einer internen Abstimmung mit Arbeitskolleginnen und -kollegen und meinem Betreuer mehreren Experten vorgelegt und mit diesen besprochen. Nach deren Rückmeldungen und der Einarbeitung einiger Verbesserungsvorschläge wurde die finale Version des Fragebogens erstellt. Es wurde entschieden keinen gesonderten Test-Durchlauf (mit einigen ausgewählten Unternehmen) bezüglich Verständlichkeit und Beantwortbarkeit des Fragebogens durchzuführen, da der Fragebogen in vielen Bereichen Ähnlichkeiten zu dem meiner vorigen Studie aufweist. Da diese Studie viele positive Rückmeldungen erhielt und von den Unternehmen gut angenommen wurde [1, S. 46f], wurde ein eigener Test-Durchlauf nicht als notwendig erachtet.
Bezüglich der tatsächlichen Durchführung der Studie wurde entschieden, die Umfrage online durchzuführen. Es wurde abermals das Online-Umfragetool der Website surveymonkey.com genutzt, welches sich bereits bei meiner vorigen Umfrage bewährt hatte und sich durch hohe Praktikabilität und Benutzerfreundlichkeit auszeichnete. Durch die online-Durchführung war die Verteilung der Umfrage an Unternehmen sehr einfach und es gab die Möglichkeit zu einer leichten und übersichtlichen Auswertung (und Export) der Antworten. Die Beantwortung der Umfrage war über einen Link möglich und allgemein öffentlich zugänglich. Die Umfrage war in einem Zeitraum von ungefähr 3 Monaten zwischen Ende Februar und Ende Mai 2015 geöffnet. Aus logistischen und organisatorischen Gründen konnte die Umfrage nicht mit individuellen und eventuell passwortgeschützten Links an die Unternehmen verteilt werden, da mir keine umfangreiche Datenbank an Unternehmen zur Verfügung stand und daher bei der Verteilung dankenswerterweise diverse Organisationen und Personen mitwirkten (siehe Kapitel 3.3). Grundsätzlich können individualisierte bzw. passwortgeschützte Links zur Umfrage (als Zugangsbeschränkung) interessant sein um sicherzustellen, dass die Umfrage nicht vorsätzlich manipuliert werden kann.
Bei der Auswertung der Umfrage wurden primär die Ergebnisse der einzelnen Fragen gesamt und länderspezifisch untersucht und außerdem diverse Frage untereinander verglichen. Im weiteren Verlauf wurde versucht die Hypothesen zu verifizieren. Die Ergebnisse der Auswertung sind in Kapitel 4 ersichtlich. Vor der eigentlichen Auswertung wurden die erhobenen Daten überprüft und aufbereitet. Hierbei wur-

den offensichtlich unvollständige Beantwortungen (nur wenige Fragen beantwortet) aus dem Datensatz entfernt (ungefähr 20-30) und bei Beantwortungen, die vor der Angabe von Land und Unternehmensgröße abgebrochen wurden bei diesen als Antwort „keine Angabe“ hinterlegt, sofern diese einigermaßen vollständig waren und die Antworten daher in der Umfrage verwendet werden konnten. Im Rahmen der Auswertung wurde die Ergebnisse auch in Rücksprache mit einem Experten evaluiert und bei einer Vorab-Vorstellung auf der FH St. Pölten diskutiert.

3.2. Fragebogendesign

3.2.1. Themengebiete

Die Studie selbst wurde in 5 Themenbereiche aufgeteilt, in welchen über verschiedenste Fragen folgende Informationssicherheits bezogene Themen behandelt werden. Diese Themenbereiche werden nun im Folgenden näher beschrieben.

- Wichtigkeit der Informationssicherheit, Abhängigkeit von IT & Informationen bzw. Daten
- Gründe und Motivation für Informationssicherheit, Bedrohungen, Nutzung von Standards
- Aktuelle Situation im Unternehmen - Informationssicherheits-Policy, Richtlinien, Evaluierung der Informationssicherheit, Beratung, Vorfälle
- „Trendthemen“ - mobile Geräte, Cloud & Outsourcing, Mitarbeiter-Awareness, Open Source Software, APTs, NSA-Enthüllungen
- Technische und organisatorische Aufstellung der Unternehmen

Der erste Bereich erhält drei Einstiegsfragen, in denen versucht wird die Wichtigkeit und den Stellenwert des Themas der Informationssicherheit für das Unternehmen selbst zu erfragen. Es wird erfragt, wie das Unternehmen seine eigene Abhängigkeit von der IT sieht und inwiefern sich der Ausfall von IT-Kernsystemen auf das Kerngeschäft des Unternehmens auswirken würde. Weiters wird auch erfragt, als wie wichtig das Unternehmen seine Daten sieht und als wie schwerwiegend es die Auswirkungen bei einem Verlust, Nichtverfügbarkeit oder Verfälschung bzw. bei deren Weitergabe (an Mitbewerber oder unautorisierte Dritte) ansieht. Außerdem wird um eine Einschätzung bezüglich des Stellenwerts der Informationssicherheit im Unternehmen selbst gebeten, wobei hierzu nach der Integration und Berücksichtigung von Informationssicherheitsvorgaben und -maßnahmen in unternehmerische Tätigkeiten gefragt wird.

Im zweiten Bereich wird nach den Gründen bzw. der Motivation des Unternehmens gefragt, sich mit dem Thema der Informationssicherheit zu beschäftigen. Außerdem wird erfragt, ob das Unternehmen hierzu auf branchenübliche Standards oder Empfehlungen zurückgreift. Weiters wird behandelt, welchen Gefahren bzw. Bedrohungen sich das Unternehmen in Bezug zur Informationssicherheit ausgesetzt fühlt und was die Hauptprobleme bzw. hemmenden Faktoren bei der Aufrechterhaltung und Verbesserung der Informationssicherheit im Unternehmen sind.
Im dritten Bereich werden Fragen zur aktuellen (insbesondere organisatorischen) Situation im Unternehmen gestellt. Es wird gefragt, ob es in dem Unternehmen für die IT/Informationssicherheit verantwortliche Personen gibt und ob bzw. welche Richtlinien und Vorgaben es in diesem Bereich vorhanden sind. Weiters wird erfragt, ob das Unternehmen im vergangenen Jahr externe Beratung zu Informationssicherheits-Themen in Anspruch genommen hat und ob es im letzten Jahr Vorfälle im Bereich der Informationssicherheit gab. Bei den Vorfällen wird erfragt, welcher Art diese waren. Obwohl in diverser Studien auch nach Häufigkeit und Schwere der Vorfälle gefragt wird, wurde hierauf bewusst nicht eingegangen, da diese Frage schon sehr detailliert wäre und Unternehmen hierzu nicht unbedingt die Daten vorliegen haben bzw. nicht darauf antworten wollen. Außerdem wird erhoben, ob die Unternehmen ihre Informationssicherheitssituation regelmäßig, etwa in Form von Audits, Penetration Tests und Vulnerability Scans evaluieren und überprüfen.
Im vierten Bereich wird auf einige aktuelle „Trendthemen“ eingegangen. Hierbei wird nach der Nutzung von mobilen Geräte (und BYOD) sowie der Nutzung von Cloud Dienstleistungen bzw. Outsourcing von IT gefragt sowie, ob dabei spezielle Sicherheitsmaßnahmen ergriffen werden. Weiters wird erhoben, ob die Unternehmen im Bereich der Mitarbeiter-Awareness-Aktivitäten aktiv sind und falls ja, in welcher Form diese erfolgen. Eine Frage behandelt den Einsatz von Open Source Software und ob Maßnahmen getroffen werden, um diese auf Fehlerfreiheit/Korrektheit und Qualität zu überprüfen. In Bezug auf Open Source Software wird ebenfalls erfragt, ob die Unternehmen von schwerwiegenden Sicherheitslücken wie Heartbleed oder Shellshock betroffen waren. Die beiden letzten Fragen untersuchen, ob die Unternehmen im vergangenen Jahr Ziel eines komplexen, fortgeschrittenen, direkt auf sie gezielten ITAngriffs (APTAdvanced Persistent Threat) waren sowie ob die NSAEnthüllungen bezüglich Überwachung und Spionage sowie der gezielten Manipulation von (amerikanischen) Soft und HardwareProdukten für sie ein Thema waren und falls ja, ob darauffolgend spezielle Sicherheitsmaßnahmen ergriffen wurden.
Im finalen fünften Bereich wird in zwei umfangreichen Matrix-Fragen die derzeitige technische und organisatorische Aufstellung des Unternehmens untersucht. Hierbei wird erfragt, welche technischen (Tools, Systeme, Vorkehrungen) oder organisatorischen Maßnahmen (Prozesse, Richtlinien, Aktivitäten) derzeit im Unternehmen eingeführt bzw. implementiert sind und ob bzw. welche in Zukunft geplant sind.

3.2.2. Hintergrund Themengebiete

In diesem Abschnitt sollen nun kurz zusätzliche Informationen zu den Themen Heartbleed & Shellshock, Open Source Software, den NSA-Enthüllungen und APTs gegeben werden.
Heartbleed & Shellshock waren im Jahr 2014 zwei schwerwiegende und äußerst weitreichende Schwachstellen in stark verbreiteter Open Source Software, welche auch medial viel Aufmerksamkeit erhielten. Bei Heartbleed handelte es sich um eine Lücke in der Open Source Bibliothek OpenSSL (freie Software für Transport Layer Security & https) „welche das Auslesen potentiell hoch sensibler Informationen, die sonst nur verschlüsselt oder gar nicht übertragen werden würden erlaubte. Darunter fallen je nach Anwendungsfall und Applikation verschiedene Daten. Bei HTTPS-Webanwendungen beispielsweise können dadurch private oder sensible Daten von Benutzerinnen und Benutzern ausgelesen werden. Neben dem Zugriff auf sensible Daten kann ein Angreifender auch Sitzungsinformationen von angemeldeten Benutzerinnen und Benutzern oder private Schlüssel des Servers erbeuten“ [4, S. 1f].
Als Gegenmaßnahmen musste eine Aktualisierung von OpenSSL auf Version 1.0.1g durchgeführt sowie (aufgrund der Tatsache, dass die Lücke 27 Monate unentdeckt in der Software war und Angriffe inklusive einer möglichen Kompromittierung des privaten Schlüssels nicht wirklich nachvollziehbar/erkennbar waren [33, o. S.]) alle SSL-Zertifikate erneuert werden. Nach dem Bekanntwerden wurden bei einem Scan aller österreichischen IP-Adressen (ca. 12 Millionen) 121.420 IP-Adressen identifiziert, die auf eine HTTPS-Anfrage antworten (wobei auf jeder Adresse eine oder eine Vielzahl von Webseiten betrieben werden können). Von diesen knapp 120.000 Systemen waren dabei 7.014 (6%) potentiell verwundbar. Knapp einen Monat später waren in Österreich immer noch 1.300 Systeme potentiell verwundbar [34, o. S.]. Auch weltweit war die Situation ähnlich, wodurch Heartbleed sehr viel Aufmerksamkeit erhielt. Der bekannte Sicherheitsforscher Bruce Schneier bezeichnete die Sicherheitslücke als katastrophal. Auf einer Skala von 1-10 sei es eine 11 [34, o. S.].
Im September 2014 wurde mit der Sicherheitslücke Shellshock eine weitere schwerwiegende Schwachstelle in Open Source Software bekannt. Sie „befindet sich in der Kommandozeilensoftware bash, die praktisch in allen Linux-Systemen als Standard-Shell eingesetzt wird. Durch einen Fehler beim Parsen von Umgebungsvariablen wird das Ausführen von beliebigen Befehlen möglich“ [35, S. 2], wobei sich die Schwachstelle sogar „unter bestimmten Umständen auch von einem externen Angreifer ausnutzen“ [35, S. 2] lässt. Es gibt einige Beispiele für Fälle, in denen die Lücke tatsächlich für Angriffe ausgenutzt wurde [36, o. S.]. Aufgrund der hohen Verbreitung von Systemen mit vorinstallierter bash Shell war auch diese Sicherheitslücke äußerst kritisch. Interessant ist, dass die Lücke alle bash Versionen seit dem Jahr 1994 betraf und sie in all diesen Jahren nicht entdeckt wurde (obwohl der Quellcode der Open Source Software jederzeit überprüft werden hätte können) [36, o. S.]. Zur Behebung mussten abermals Updates in allen betroffenen Systemen eingespielt werden.

Generell ist bei Open-Source-Software zwar jederzeit eine Überprüfung möglich, da der gesamte Quellcode offen und frei verfügbar ist, doch die Tatsache, dass Sicherheitslücken oft jahrelang unentdeckt bleiben zeigt auf (oder legt zumindest den Schluss nahe), dass diese Möglichkeit kaum genutzt wird. Dies kann damit zusammen hängen, dass nur wenige Menschen die Expertise und Zeit haben solche Code Reviews tatsächlich durchzuführen. Ein Projekt, welches sich eben mit dem Scan von Open Source Software beschäftigt ist der Coverity Scan [37, o. S.]. Die Heartbleed & Shellshock Sicherheitslücken befanden sich in Open Source Software, welche sehr weit verbreitet in Unternehmen eingesetzt wird. Darum wird in dem Fragebogen untersucht, ob Unternehmen von den vorgestellten Sicherheitslücken betroffen waren und ob sie Maßnahmen treffen, um eingesetzte Open Source Software auf Fehlerfreiheit/Korrektheit und Qualität zu überprüfen.

Die von Edward Snowden 2013 angestoßenen Enthüllungen der Tätigkeiten und Programme der NSA und des GCHQ, lassen Rückschlüsse auf den Umfang der Überwachung und gezielten (Wirtschafts)-Spionage im Internet sowie der Manipulation und Beeinflussung von IT-Technologien zu.

Ein bekanntes Beispiel für die gezielte Manipulation von IT-Technologien ist die des NIST Standards für Zufallszahlengeneratoren [38, o. S.]. Auch diverse andere Aktivitäten, welche im Rahmen der NSA-Enthüllungen aufgedeckt wurden [39, o. S.] [40, o. S.] [41, S. 100ff] [42, S. 102f] oder etwa das „Bullrun“ Programm der NSA, welches die gezielte Schwächung von IT-Sicherheitsprodukten zum Ziel hat [43, o. S.] [44, o. S.] [45, o. S.], sind weitere gute Beispiele für die bewusste Manipulation von IT-Produkten.

Auch „in einem Programm namens 'Sentry Raven' arbeitet die NSA mit bestimmten US-Konzernen zusammen, Kryptographie-Systeme aus den USA für die Überwachung nutzbar zu machen. Zwar werden keine Namen genannt, aber diese Enthüllung erinnert daran, dass RSA Geld erhalten hat, um ein Verschlüsselungsprogramm zu schwächen“ [46, o. S.] [47, o. S.]. Dieses Programm kann als ein Indiz dafür gesehen werden, dass Verschlüsselungssystemen aus den USA nur begrenzt vertraut werden sollte [48, o. S.]. Ein Beispiel für lange unbekannte Kooperationen zwischen der NSA mit ausländischen Unternehmen ist „Sentry Owl“. Hier arbeitet die NSA „mit bestimmten ausländischen Partnern und ausländischen Unternehmen daran, Geräte und Produkte für die Überwachung nutzbar zu machen. Es sind zwar keine Unternehmensnamen und Umfang der Kooperation bekannt, aber trotzdem lasst dieses Kooperation auch einen Wechsel auf vermeintlich sichere Technik aus anderen Staaten, etwa aus Deutschland, in einem anderen Licht erscheinen“ [46, o. S.] [49, o. S.].

Im April 2015 wurde bekannt, dass der deutsche BND jahrelang dem US-Geheimdienst NSA geholfen hat, europäische Unternehmen und auch Politiker auszuspionieren. So wurde etwa „gezielt nach Informationen etwa über den Rüstungskonzern EADS, Eurocopter oder französische Behörden“ [50, o. S.] gesucht (Stichwort Selektorenliste).

Grundsätzlich werfen die NSA Enthüllungen die Frage auf, inwiefern dieses Thema (Überwachung, Spionage, Manipulation von IT-Technologien) für Unternehmen interessant/relevant ist und ob bzw. welche Maßnahmen von ihnen getroffen werden.

In den vergangenen Jahren erlange der Begriff des APTs (Advanced Persistent Threat oder zu Deutsch „fortgeschrittene, andauernde Bedrohung“) große Bedeutung (insbesondere auch in den Marketing- Abteilungen diverser Hersteller von Sicherheitsprodukten). Bei einem APT handelt es sich um „zielgerichtete Cyber-Angriffe durch fortgeschrittene, gut organisierte und professionell ausgestattete Angreifer“ [51, S. 13f] wobei „APTs sowohl in ihrer Vorbereitung als auch in ihrer Durchführung meist sehr komplex sind und typischerweise in mehreren Phasen vollzogen werden. Das Ziel eines APT ist es, möglichst lange unentdeckt zu bleiben, um über einen längeren Zeitraum sensible Informationen auszuspähen oder anderweitig Schaden anzurichten“ [51, S. 13f].

Es gibt einige bekannte Beispiele für APTs - bzw. für Angriffe, welche als APTs bezeichnet werden - wie etwa Operation Aurora [52, o. S.], den Angriff auf RSA 2011 [53, o. S.] oder den Angriff auf ein deutsches Stahlwerk [54, o. S.], doch zu ihrer tatsächliche Häufigkeit und ihrer Relevanz für Unternehmen gibt es nur wenige Daten. So gaben von den 257 Teilnehmern der BSI Cyber-Sicherheits-Umfrage 2014 nur 18 Unternehmen an, in den Jahren 2012-2014 einem APT artigen Angriff ausgesetzt gewesen zu sein [8, S. 5]. Auch in der Kaspersky Global IT Security Risk Survey 2014 gaben lediglich 12 % der Unternehmen an im vergangenen Jahr, von einer fortgeschrittenen und gezielten Attacke betroffen gewesen zu sein. Trotz der häufigen Verwendung des Begriffes gibt es allgemein nur wenige Umfragen, die das Auftreten von APTs in Unternehmen behandeln.

3.2.3. Aufbau Fragebogen

Der Aufbau des Fragebogens ähnelt sehr stark den oben beschriebenen Themenbereichen. Zusätzlich wurden jedoch noch eine Einleitung, diverse Hilfstexte und Fragen zur Demografie eingebaut. Bei der Erstellung des Fragebogens waren die bei der letzten Umfrage gemachten Erfahrungen eine große Hilfe. Auch die Seite fragebogen.de [55, o. S.] wurde genutzt, da auf ihr viele nützliche Informationen zum Aufbau von Fragebögen und der Entwicklung von qualitätsvollen Fragen enthalten sind. Eine weitere Seite mit sehr guten Tipps zur Erstellung von Fragebögen stammt von der Wirtschaftspsychologischen Gesellschaft [56, o. S.]

In der Einleitung am Beginn der Umfrage wird den Unternehmen für ihre Teilnahme gedankt und es wird erklärt, dass es sich um eine wissenschaftliche (nicht kommerzielle) Umfrage in Rahmen einer Diplomarbeit handelt, um die Antwortbereitschaft zu erhöhen [55, o. S.]. Es wird erklärt, dass Unternehmen durch die Teilnahme profitieren können, da verschiedene organisatorische und technische Maßnahmen

angesprochen werden und diese als Anregung verstanden werden können, wie die eigene Informationssicherheitssituation verbessert werden kann. Außerdem wird den Unternehmen in Aussicht gestellt, dass sie durch die Teilnahme präzise Ergebnisse zur aktuellen Situation in der Schweiz, Deutschland und Österreich erhalten. Weiters wird auch auf die Anzahl der Fragen und die Beantwortungsmodalitäten, sowie die ungefähre Dauer für die Beantwortung des Fragebogens eingegangen. Da in dieser Umfrage durchaus sensible Daten zu Sicherheitsvorfällen und der sicherheitstechnischen Aufstellung gesammelt werden, wird den Unternehmen versichert, dass ihre Angaben vertraulich behandelt und lediglich in anonymisierter Form verwendet werden, um ihnen mit gutem Gewissen eine wahrheitsgemäße Beantwortung zu ermöglichen. Außerdem sind auf der ersten Seite auch die Partner und Unterstützer dieser Arbeit dankend erwähnt, um deren Hilfe hervorzuheben und um potentielle Teilnehmerinnen und Teilnehmer von der Seriosität dieser Umfrage zu überzeugen.

Danach folgen auf mehreren Seiten die 21 fachspezifischen Fragen zu den bereits beschriebenen Themengebieten. Die Fragen zur technischen und organisatorischen Aufstellung (zwei große Matrix Fragen) wurden bewusst am Ende der Umfrage platziert, da Matrix Fragen aufwändig zu beantworten und generell suboptimal in Umfragen sind [55, o. S.]. Hierdurch sollte vermieden werden, dass Teilnehmerinnen und Teilnehmer gleich zu Beginn der Umfrage „abgeschreckt“ werden. Vor den Matrix Fragen wird außerdem explizit darauf hingewiesen, dass die Umfrage fast abgeschlossen ist, um die Unternehmen zu einer Beantwortung zu motivieren. Weiters wurden bei den Matrix Fragen und bei diversen anderen Fragen Hilfstexte mit Erklärungen und Beispielen eingebaut, um eine Hilfestellung bei der Beantwortung zu bieten.

Nach den fachspezifischen Fragen werden noch demografische Daten zu Land, Unternehmensgröße, Branche (nach NACE Rev.2 (Statistische Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft)) und Aufgabenbereich der Teilnehmerin/des Teilnehmers im Unternehmen gestellt, wobei insbesondere Unternehmensgröße und Land für die Auswertung und die Verifikation der Hypothesen von Bedeutung sind. Die demografischen Daten wurde am Ende platziert, da deren Beantwortung eher „langweilig“ ist (und sie am Beginn der Umfrage platziert zu einer höheren Abbruchquote führen können). Außerdem wird eine Person, die bereits bis zu diesem Punkt gekommen ist, hier eher nicht mehr die Umfrage abbrechen, da sie bereits einen gewissen Aufwand und Zeit investiert hat [57, S. 18].

Am Ende der Umfrage wird den Unternehmen nochmals für ihre Teilnahme an der Umfrage gedankt und erwähnt, dass sie den Link zur Umfrage gerne weiter verteilen können. Außerdem können sie eine E-Mail-Adresse angeben, an die ihnen nach Abschluss der Umfrage die Ergebnisse zugesandt werden. Natürlich gibt es auch die Möglichkeit für Rückmeldungen, Anregungen und Verbesserungsvorschläge.

3.2.4. Umfang Fragebogen

Wie bereits auch in meiner letzten Arbeit ausführlich beschrieben [1, S. 19f] ist das Finden des „richtigen“ Umfangs des Fragebogen eine große Herausforderung. Schlussendlich muss bei jeder Umfrage immer ein Kompromiss zwischen Umfang, Genauigkeit bzw. Detailtiefe und der für die Ausfüllung benötigten Zeitdauer gefunden werden, da die den Unternehmen zumutbare Zeitdauer äußerste begrenzt ist. Auch in der Experten-Diskussion zu meinem Fragebogen kam mehrmals die Rückmeldung, dass mehr als 20 Fragen in einer Online Umfrage kaum machbar sind. Dies entspricht genau dem Umfang meiner ersten Umfrage, der dieses Mal jedoch leicht überschritten wurde (21 fachspezifische Fragen + Demografie). Trotzdem war bei dieser Umfrage die Abbruchquote (während dem Fragebogen) nicht unverhältnismäßig hoch. Nichtsdestotrotz war die für die Ausfüllung geschätzte Zeitdauer von 15-20 Minuten wahrscheinlich relativ optimistisch, da die teilnehmenden Unternehmen auch Zeit benötigen, die Fragen zu „verstehen“ und diverse Begleittexte zu lesen.

Aufgrund der Zeitbeschränkung konnten in den 21 fachspezifischen Fragen leider nicht in aller Tiefe auf die Themen eingegangen werden und schon in der Auswahl der Themenbereiche musste eine gewisse Fokussierung durchgeführt werden. Es wurden bewusst auch keine allzu spezifischen Detailfragen gestellt, da nicht unbedingt alle teilnehmenden Personen „Informationssicherheits-Spezialisten und Spezialistinnen“ sind und daher über ein unterschiedliches „Fachwissensniveau“ verfügen. Außerdem würden Unternehmen, die weniger Affinität zu dem Thema Informationssicherheit besitzen, diese Detailfragen nicht (sinnvoll) beantworten können und auch keinen Mehrwert aus ihnen ziehen.

Wie bei solchen Umfragen üblich (und nachdem es sich bereits in meiner vorigen Umfrage bewährt hatte) wurde entschieden „Single Choice“, „Multiple Choice“ sowie „Matrix Fragen“ zu nutzen. Es wurde bewusst auf freie/offene Fragen verzichtet, da diese aufwändiger zu beantworten sind und deren Beantwortung (sowie Auswertung) mehr Zeit in Anspruch nimmt. Außerdem ist bei ihnen die Antwortqualität sehr stark von der ausfüllenden Person abhängig und sie wären eher bei einer „geführten/unterstützten“ Beantwortung oder einem Interview angemessen. Bei den geschlossenen Fragen bestand allerdings, soweit erforderlich, die Möglichkeit über ein freies Antwortfeld detailliertere oder zusätzliche Angaben zu machen.

Die Nutzung von geschlossenen Fragen hat viele Vorteile. Es muss jedoch auch darauf hingewiesen werden, dass „deren korrekte und klare Formulierung eine gewisse Herausforderung darstellt, da unter anderem auch sichergestellt werden muss, dass die Teilnehmerin oder der Teilnehmer nicht schon durch die Fragestellung zu einer bestimmten Antwort hingelenkt oder beeinflusst wird“ (Suggestivfragen).

Außerdem muss berücksichtigt werden, dass die Antwortoptionen das gesamte Spektrum an Antwortmöglichkeiten abdecken. Hinweise zur Formulierung von Fragen und Antwortoptionen werden unter anderem auf der Seite fragebogen.de [55, o. S.] oder in [57, S. 16ff] und [56, o. S.] gegeben.
Auch aus Zeitgründen war es möglich Fragen zu überspringen. Bis auf die demografischen Fragen nach Land und Unternehmensgröße wurde keine Beantwortung erzwungen. Dies hatte auch den Grund, dass Teilnehmerinnen und Teilnehmer Fragen die ihnen unklar sind, zu denen sie keine Informationen haben bzw. teilen wollen (oder die ihnen zu umfangreich sind) nicht beantworten müssen (andernfalls könnte es zu einer erhöhten Abbruchquote oder zu inkorrekten/unüberlegten Antworten kommen). Außerdem wurde in der Umfrage ein Balken eingeblendet, um den antwortenden Personen ihren Fortschritt zu visualisieren.

3.2.5. Gesamter Fragebogen

Der gesamte Fragebogen mit allen Fragen, Erklärungen und Begleittexten ist im Anhang in Kapitel A.1 ersichtlich.

3.3. Verteilung der Umfrage

Wie bereits in 3.1 erklärt wurde entschieden, die Umfrage online durchzuführen. Hierzu wurde das Online-Umfragetool auf der Website surveymonkey.com genutzt.
Die Verteilung (und Erreichung einer angemessen großen Anzahl an Beantwortungen) der Umfrage stellte wie auch schon bei meiner vergangenen Studie eine große Herausforderung dar. Für Unternehmen bietet die Teilnahme an Studien oft wenig Mehrwert und kann als Zeit- und Ressourcen-fressend angesehen werden. Aus diesem Grund wurde in der Einleitung der Umfrage und bei der Verteilung explizit auch auf Vorteile bzw. den Mehrwert hingewiesen, welche Unternehmen durch die Teilnahme erzielen können. Wie auch in Kapitel 2.4 beschrieben werden die meisten anderen Informationssicherheitsstudien von großen Organisationen oder Zeitschriften etc. durchgeführt, welche selbst eine gewisse Mitgliederbasis und Reichweite aufweisen, welche ich als Student nicht vorweisen kann.
Dankenswerterweise erhielt ich bei der Verteilung der Umfrage sehr viel Unterstützung von verschiedensten Unternehmen, Organisationen und Personen und konnte ebenfalls auf im Rahmen meiner vergangenen Studie geknüpfte Kontakte zurückgreifen.

Die Umfrage wurde unter anderem über und durch folgende Organisationen und Kontakte verteilt:

- BSI in Rahmen eines Newsletters der Allianz für Cyber-Sicherheit
- <kes> in einem Newsletter
- Professor der Universität Regensburg
- FH St. Pölten an Partner und Kontakte
- Lehrbeauftragte der FH St. Pölten
- StudienkollegInnen im Bachelor und Master Studiengang
- Computerwelt in einem Artikel [58, o. S.] und auf deren Facebook Seite
- ADV in einem Artikel und Newsletter sowie in sozialen Netzen
- IKT Portal - onlinesicherheit.gv.at in einem Artikel [59, o. S.]
- WKÖ IT-Security Experts Group in einem Newsletter
- ISACA Österreich in einem Newsletter
- Cyber Security Austria an diverse Kontakte
- SBA Research in einer Mail an diverse Kontakte
- Information Security Society Switzerland (ISSS) in einem Newsletter
- Sicherheitsgruppe Schweiz (SGRP) in einem Newsletter
- private Kontakte

Ich möchte mich hiermit abermals bei allen Teilnehmerinnen und Teilnehmern sowie allen Unterstützern für deren Hilfe bei der Verteilung der Umfrage herzlich bedanken. Ohne deren Mitwirkung und Unterstützung wäre diese Arbeit nicht möglich gewesen.

4. Auswertung & Interpretation der Ergebnisse

Im folgenden Kapitel erfolgt eine Beschreibung der Auswertung des Fragebogens und eine Interpretation der Ergebnisse. Weiters wird auf die Hypothesen und die forschungsleitenden Fragestellungen eingegangen. Außerdem werden Faktoren, welche zu einer Beschränkungen der Aussagekraft der durchgeführten Umfrage (sowie von Umfragen im Allgemeinen) führen können, diskutiert.

4.1. Rücklaufquote und Teilnehmerfeld

Die Umfrage war in einem Zeitraum von ungefähr 3 Monaten zwischen Ende Februar und Ende Mai 2015 geöffnet. In dieser Zeit wurde sie von insgesamt 229 Unternehmen ausgefüllt. Von diesen nannten 56 Deutschland, 82 Österreich und 65 die Schweiz als ihren Hauptstandort. Die restlichen 26 Unternehmen machten hierzu entweder keine Angabe (19, siehe Anmerkung 4.1) oder nannten ein anderes Land (7). Ein Überblick über die Herkunft der teilnehmenden Unternehmen ist in Abbildung 4.1 ersichtlich.
Es ist anzumerken, dass aufgrund der Tatsache, dass zu den einzelnen Fragen bewusst keine Antworten erzwungen wurden (siehe Kapitel 3.2.4), nicht alle Fragen von allen Teilnehmerinnen und Teilnehmern beantwortet wurden und je Frage die Gesamtanzahl der Beantwortungen (leicht) schwankt. Daher sind die genauen Antwortzahlen je Frage in den jeweiligen Grafiken und in den Detailergebnissen im Anhang A.3 aufgeführt. In der folgenden Auswertung beziehen sich daher alle Prozentangaben immer auf die tatsächliche (schwankende) Antwortanzahl der jeweiligen Frage und nicht auf das gesamte Teilnehmerfeld der 229 Unternehmen.
Im Teilnehmerfeld befanden sich Unternehmen unterschiedlicher Größe. Die genaue Aufteilung nach der Unternehmensgröße ist in Abbildung 4.2 ersichtlich. 21,4% der Unternehmen waren klein Unternehmen mit 1-49 Angestellten. 12% der Unternehmen hatten zwischen 50 und 249 Angestellten, während weitere 12,2 % 250-999 Menschen beschäftigten. 39% der teilnehmenden Unternehmen waren große Unternehmen und hatten mehr als 1000 Angestellte. Die länderspezifische Übersicht der Unternehmensgrößen ist in Abbildung 4.3 ersichtlich. Auffallend ist, dass in Österreich im Vergleich zu Deutschland und Schweiz relativ viele kleine Unternehmen an der Umfrage teilnahmen (36,6%), während in der Schweiz viele Unternehmen mit mehr als 1000 Angestellten (50,8%) antworteten. Deutschland liegt bei der Unternehmensgröße tendenziell im Mittelfeld.

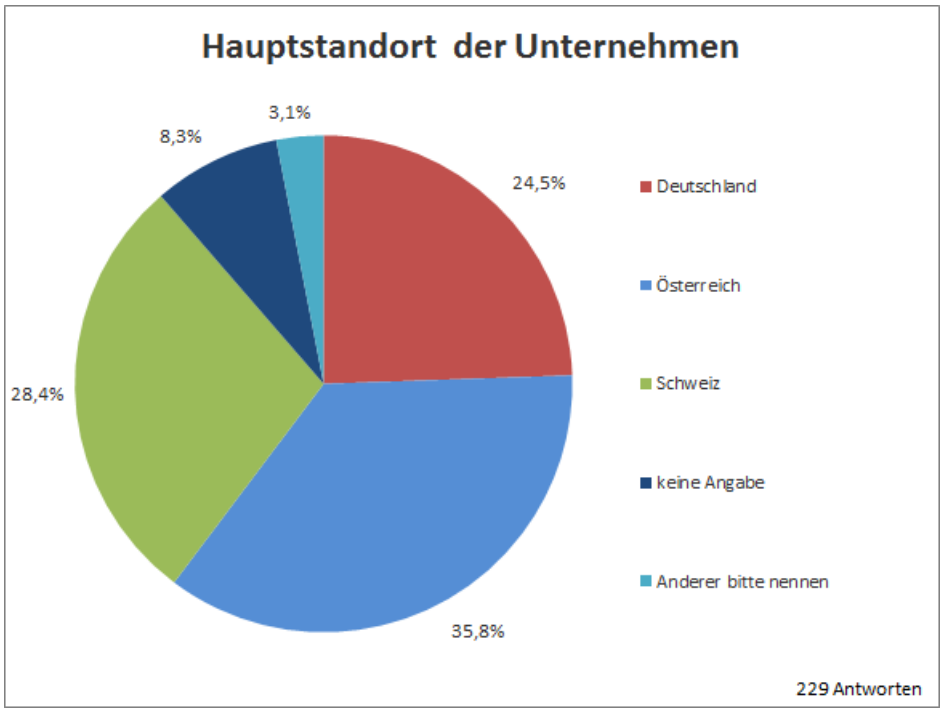

Abbildung 4.1.: Hauptstandort

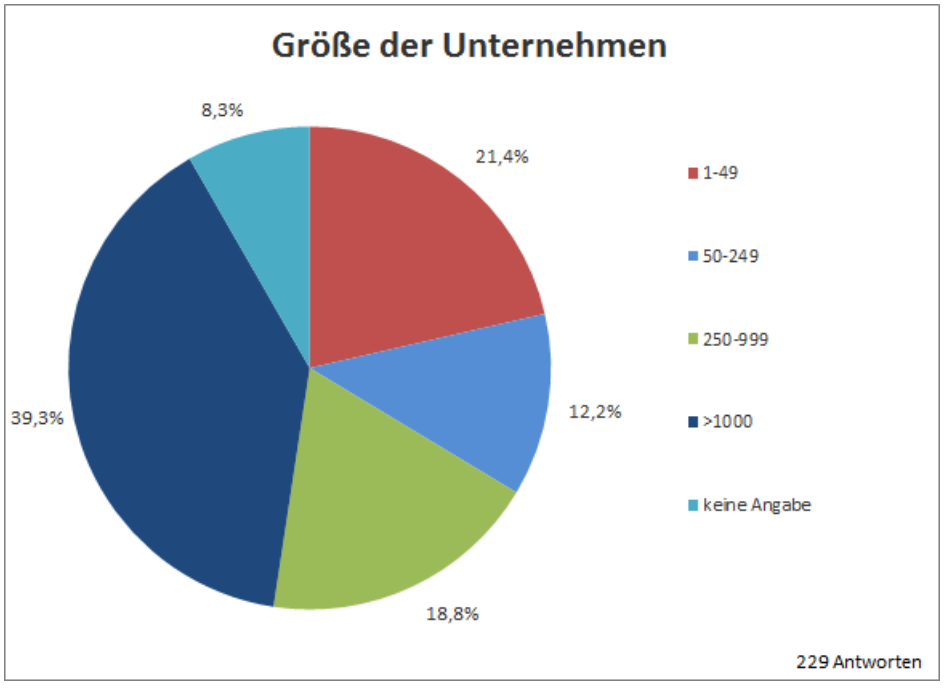

Abbildung 4.2.: Unternehmensgröße

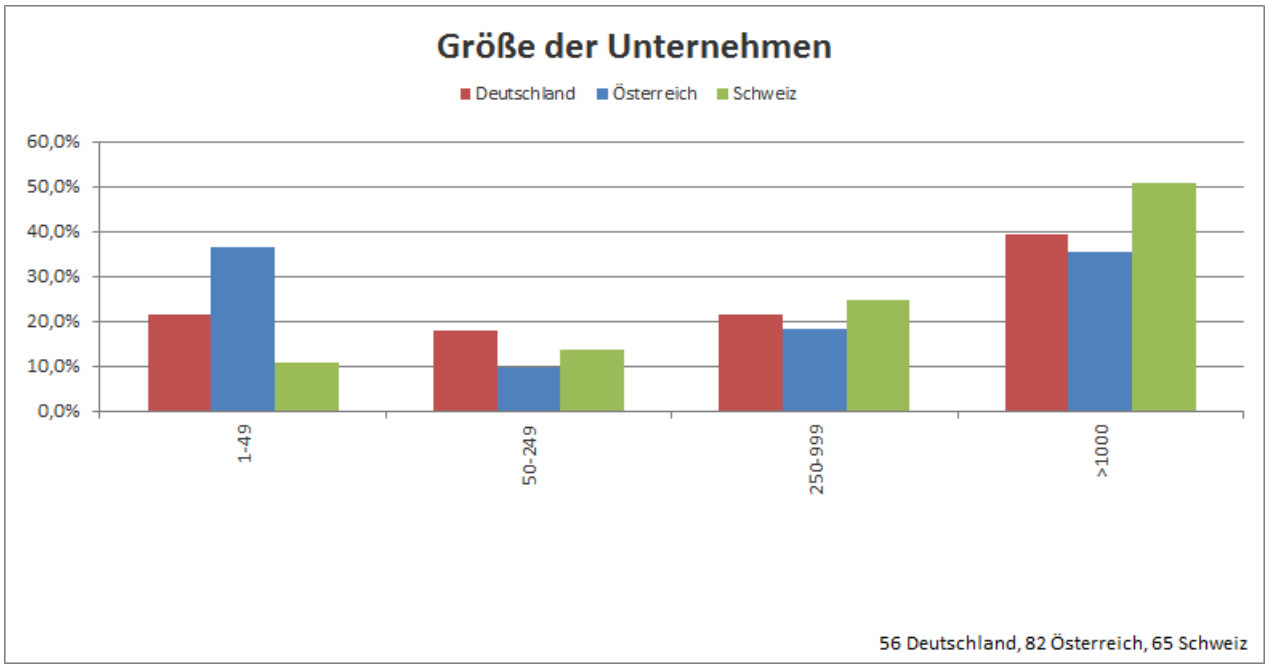

Abbildung 4.3.: Länderspezifisch: Unternehmensgröße

Anmerkung: Bei Beantwortungen, die vor der Angabe von Land und Unternehmensgröße abgebrochen wurden, wurde - wie in Kapitel 3.1 erklärt - als Antwort „keine Angabe“ hinterlegt, sofern diese einigermaßen vollständig waren und die Antworten daher in der Umfrage verwendet werden konnten.

Die teilnehmenden Unternehmen kamen aus den verschiedensten Branchen. Die Aufstellung hierzu ist in der Tabelle A.30 ersichtlich. Die meisten Teilnehmerinnen und Teilnehmer stammten aus den Branchen „Information und Kommunikation“ (28,3%), „Öffentliche Verwaltung, Verteidigung und Sozialversicherung“ (21,2%), „Erbringung von Finanz- und Versicherungsdienstleistungen“ (13,1%), sowie „Erbringung von sonstigen (witschaflichen) Dienstleistungen“ (10,6%), „Herstellung von Waren“ (6,6%) und „Energieversorgung“ (4%).

Die Umfrage wurde von Personen mit unterschiedlichen Aufgabenbereichen bzw. Funktionen innerhalb ihres Unternehmens ausgefüllt. Bei dem Großteil der Teilnehmerinnen und Teilnehmer handelte es sich um „CISOs/Informationssicherheits-Beauftragte“ (29,9%), „IT-Leitung oder Sicherheitsmanagement“ (25,4%) oder die „Geschäftsleitung“ (12,5%). Bei jeweils 6,5% der Unternehmen wurde die Umfrage durch eine Person mit „System-“ oder „Netzwerkadministrationsaufgaben“ ausgefüllt. Die weitere Aufschlüsselung ist in Tabelle A.31 ersichtlich.

Zu der Rücklaufquote der Umfrage selbst (Prozentsatz der angeschriebenen bzw. erreichten Unternehmen, welche dann auch tatsächlich an der Umfrage teilgenommen haben) können leider keine genauen Angaben gemacht werden, da durch die Verteilung über die vielen unterschiedlichen Kanäle keine Aufstellung über alle angeschriebenen Unternehmen verfügbar ist. Außerdem wurden auch Artikel zu der

Studie auf diversen Websites; Netzwerken veröffentlicht und auch hier ist nicht bekannt, wie viele Unternehmen über diesen Kanal erreicht wurden.

4.2. Auswertung der Fragen

Wie bereits in Kapitel 3.2.1 beschrieben wurde die Umfrage in 5 Themenbereiche/Schwerpunkte aufgeteilt, an denen sich nun auch die Auswertung orientieren wird.

- Wichtigkeit der Informationssicherheit, Abhängigkeit von IT & Informationen bzw. Daten
- Gründe und Motivation für Informationssicherheit, Bedrohungen, Nutzung von Standards
- Aktuelle Situation im Unternehmen - Informationssicherheits-Policy, Richtlinien, Evaluierung der Informationssicherheit, Beratung, Vorfälle
- „Trendthemen“ - mobile Geräte, Cloud & Outsourcing, Mitarbeiter-Awareness, Open Source Software, APTs, NSA-Enthüllungen
- Technische und organisatorische Aufstellung der Unternehmen

Anmerkung: Vor Beginn der Auswertung soll noch darauf aufmerksam gemacht werden, dass diese Studie natürlich gewissen Einschränkungen und Faktoren, welche sich auf ihre Aussagekraft und Repräsentativität auswirken können, unterliegt. Diese werden in Kapitel 4.5 näher beschrieben. Insbesondere ist es aufgrund der zur Verteilung genutzten Kanäle, sowie der „Selbst Selektion“ der Teilnehmerinnen und Teilnehmer (Unternehmen entscheiden frei und selbstständig an der Umfrage teilzunehmen) äußerst wahrscheinlich, dass die meisten Teilnehmerinnen und Teilnehmer dieser Umfrage ein höheres Bewusstsein und Interesse für das Thema der Informationssicherheit aufweisen und hierin besser aufgestellt sind als ein „typisches durchschnittliches Unternehmen“ dies ist. Daher ist es möglich und wahrscheinlich, dass die Gesamtsituation der Informationssicherheit in Deutschland, Österreich und der Schweiz, verglichen mit den in dieser Studie aufgeführten Ergebnissen und Schlüssen, „anders“ bzw. „schlechter“ sein könnte, als durch die Ergebnisse hier nahegelegt wird.

4.2.1. Wichtigkeit der Informationssicherheit, Abhängigkeit von IT & Informationen bzw. Daten

Bei der ersten Frage nach der eigenen Abhängigkeit von IT antworteten, wie in Abbildung 4.4 ersichtlich, 57,6% der Unternehmen „sehr stark“ von der eigenen IT abhängig zu sein. Bereits ein Ausfall von

Kernsystemen für wenigen Stunden würde das Kerngeschäft dieser Unternehmen stark negativ beeinträchtigen oder unmöglich machen. Weitere 31,4% gaben an „stark“ von der eigenen IT abhängig zu sein und nach einem Ausfall von einem Tag mit ernsten Problemen für das Kerngeschäft zu rechnen. Lediglich 11% der Unternehmen gaben an „nur in Teilbereichen“ oder nur in „geringem Ausmaß“ von der eigenen IT abhängig zu sein.

Wie in Abbildung 4.5 ersichtlich gab es zwischen den Ländern nur einen großen Unterschied. Interessanterweise gaben 65,9% der österreichischen Unternehmen eine „sehr starke“ Abhängigkeit von der eigenen IT an, während nur 46,4% der deutschen bzw. 50,8% der Schweizer Unternehmen so antworteten. Dementsprechend gaben weniger österreichische Unternehmen eine „starke“ Abhängigkeit an, während bei den beiden anderen Antworten die Ergebnisse wieder sehr ähnlich sind. Mit 7,1% wurde eine geringe Abhängigkeit von der IT in Deutschland häufiger angegeben als in Österreich und der Schweiz wo dies nur 2,4% bzw. 1,5% taten.

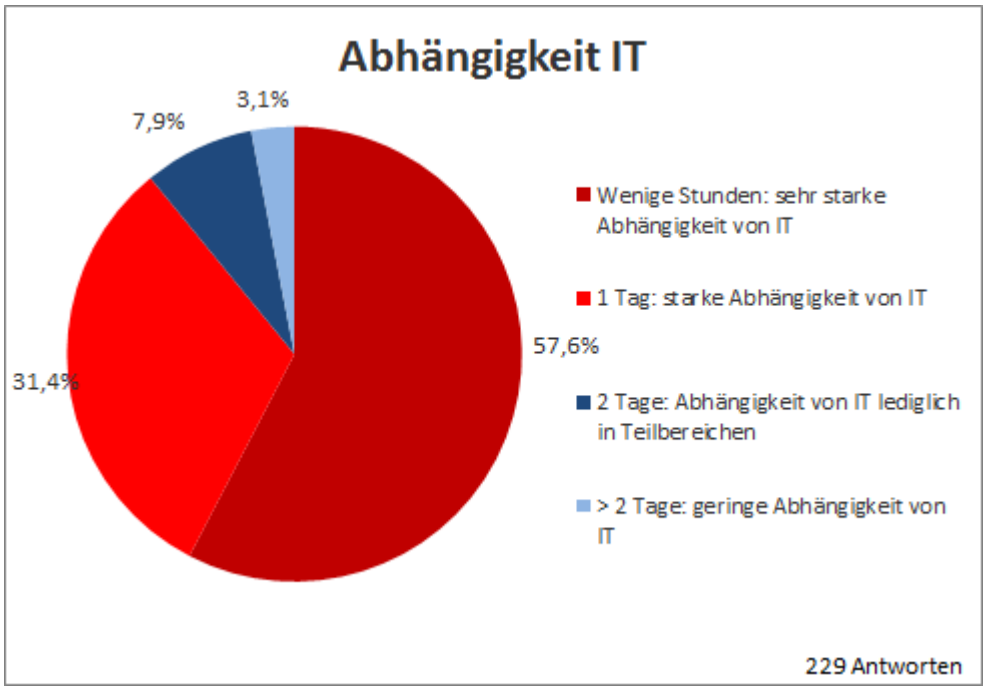

Abbildung 4.4.: Abhängigkeit von IT

In Bezug auf die Wichtigkeit von Daten und Informationen für das Geschäft des Unternehmens und den möglichen Auswirkungen eines Verlustes, Nichtverfügbarkeit oder Verfälschung bzw. deren Weitergabe (etwa an Mitbewerber oder unautorisierte Dritte) auf das Kerngeschäft zeigt sich ein ähnliches Bild wie in Frage 1. So gaben, wie in Abbildung 4.6 ersichtlich, 52,4% der Unternehmen an, dass bei solchen Vorfälle mit „sehr hohen“ Auswirkungen auf das Kerngeschäft zu rechnen ist (schwerwiegenden Imageschäden, Know-How Verluste, Geldverluste, rechtliche Konsequenzen und langfristige Auswirkungen

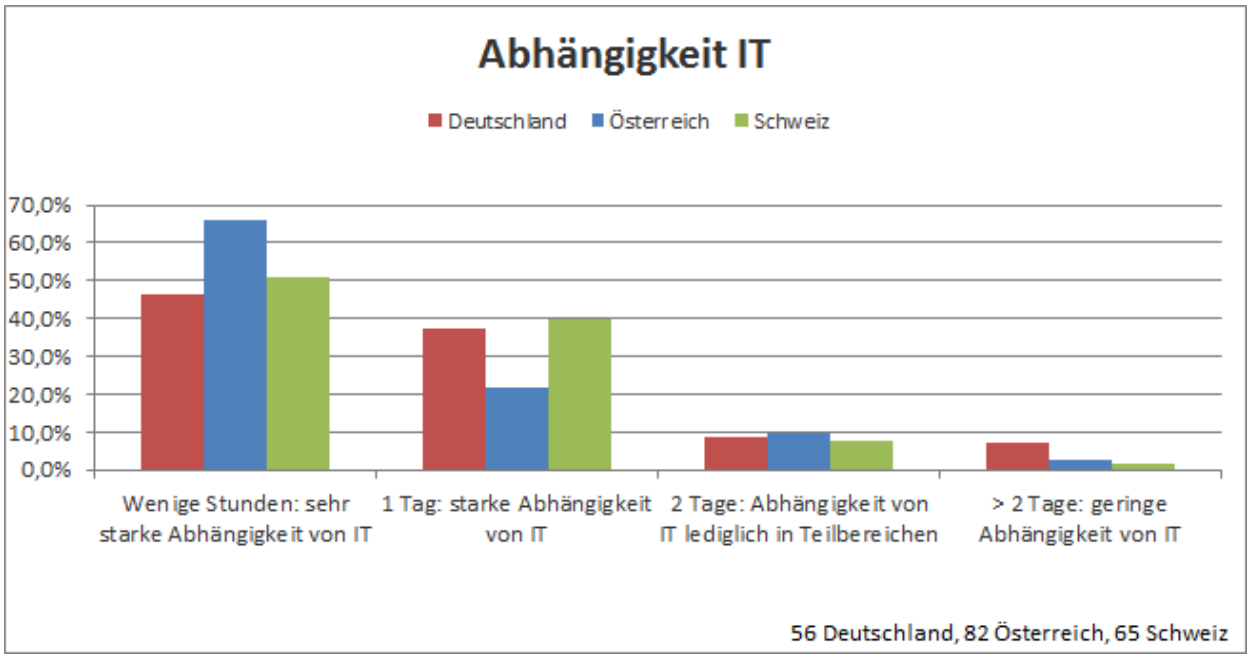

Abbildung 4.5.: Länderspezifisch: Abhängigkeit von IT

auf die Neukunden- bzw. Auftragsgewinnung). Weitere 26% rechneten in so einem Fall mit „hohen“ Konsequenzen auf das Geschäft, während nur 17,6% bzw 4% der Teilnehmerinnen und Teilnehmer „lediglich spürbare“ bzw. „geringe“ Konsequenzen befürchteten.

Die länderspezifische Auswertung in 4.7 weist keine großen Unterschiede auf. Lediglich bei der „mittleren/spürbaren“ Auswirkung gibt es in Österreich prozentuell sichtlich weniger Antworten als in Deutschland und der Schweiz. Dafür rechnen in Österreich 7,3% mit „kaum spürbaren“ Auswirkungen, während dies in Deutschland und der Schweiz lediglich 3,6% bzw. 1,6% der Unternehmen tun.

Bei der Grundsatzfrage nach der Wichtigkeit des Themas der Informationssicherheit in den Unternehmen, deren Ergebnisse in Abbildung 4.8 aufgeführt sind, antworteten 37,6%, dass dieses Thema für sie „sehr wichtig“ sei und in allen wesentlichen Geschäftsprozessen einen definierten, integralen Bestandteil darstellt. Weitere 40,2% sehen die Informationssicherheit als „wichtiges“ Thema, wofür eine dedizierte Rolle verantwortlich ist, während 21,8% die Informationssicherheit als „weniger wichtiges“ Thema empfinden, welches hauptsächlich in der IT angesiedelt ist. Lediglich für 0,4% der Unternehmen (dies ist ein einziges der teilnehmenden Unternehmen) stellt Informationssicherheit ein „unwichtiges oder nebensächliches“ Thema dar, welches keine besondere Berücksichtigung findet.

Zwischen den Ländern gab es, wie in Abbildung 4.9 ersichtlich, lediglich kleine Unterschiede. Der Anteil der Unternehmen, für die die Informationssicherheit ein „sehr wichtiges“ Thema ist ist in Deutschland, Österreich und der Schweiz beinahe gleich. Dafür gaben in Deutschland mehr Unternehmen an, dass es sich bei der Informationssicherheit um ein „wichtiges“ Thema handelt. Dementsprechend ist auch der

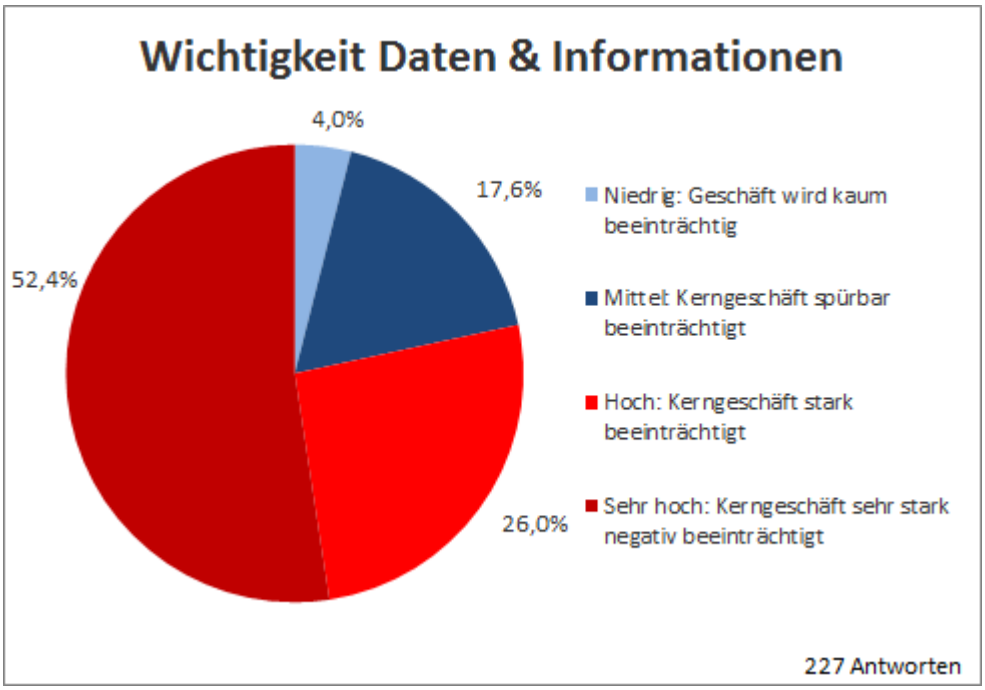

Abbildung 4.6.: Wichtigkeit von Daten und Informationen

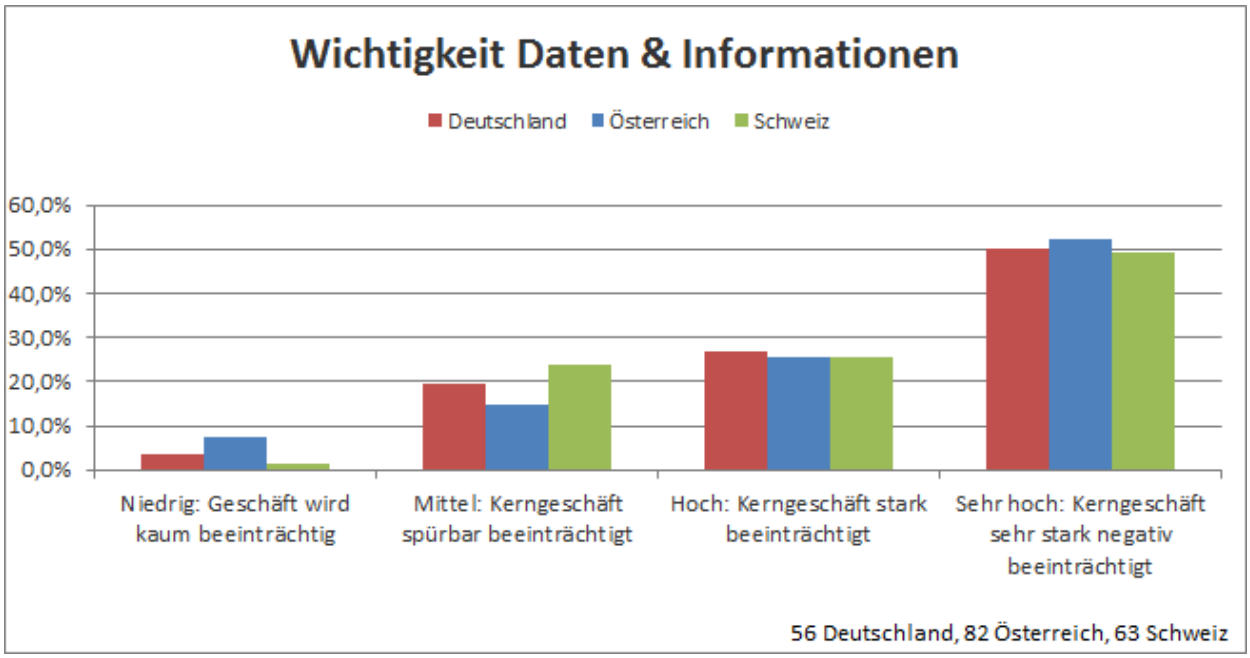

Abbildung 4.7.: Länderspezifisch: Wichtigkeit von Daten und Informationen

Anteil der deutschen Unternehmen, die in der Informationssicherheit lediglich ein IT Thema sehen, mit 17,9% im Ländervergleich am geringsten.

Schon in diesen Antworten wird ein Sachverhalt ersichtlich, der auch in Kapitel 4.5 und in der Anmerkung 4.2 erklärt wird. Es ist äußerst wahrscheinlich, dass die meisten Teilnehmerinnen und Teilnehmer dieser Umfrage ein höheres Bewusstsein und Interesse für das Thema der Informationssicherheit haben und hierin besser aufgestellt sind als ein „typisches durchschnittliches Unternehmen“ dies ist.

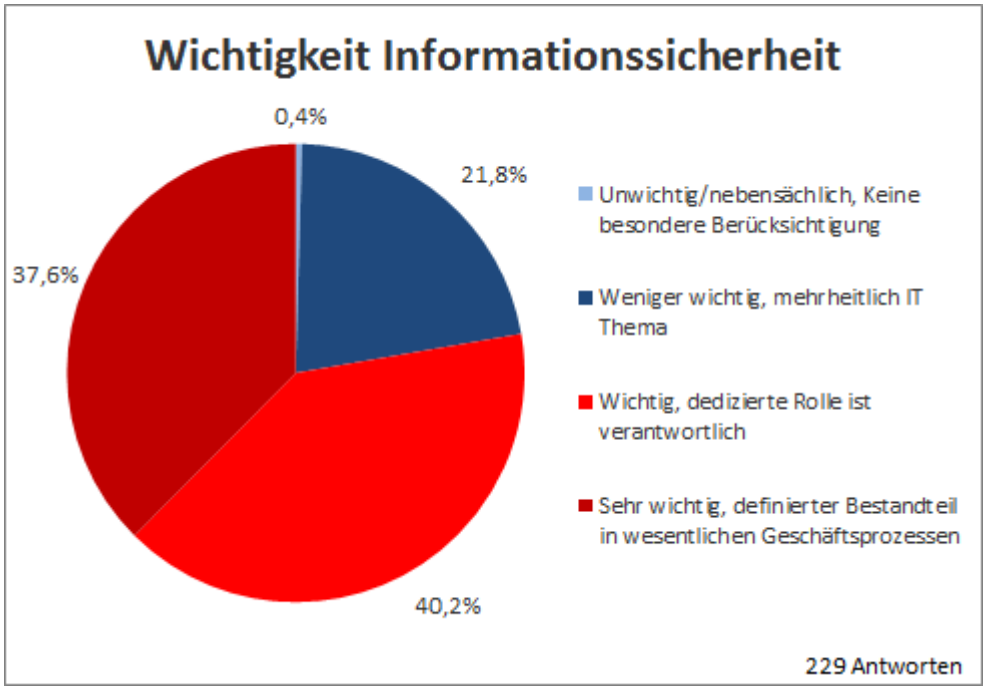

Abbildung 4.8.: Wichtigkeit der Informationssicherheit

4.2.2. Gründe und Motivation für Informationssicherheit, Bedrohungen, Nutzung von Standards

Für Unternehmen gibt es verschiedenste Gründe bzw. Motivation, sich mit dem Thema der Informationssicherheit zu beschäftigen. Am häufigsten werden, wie in Abbildung 4.10 ersichtlich, „Gesetzliche Vorgaben (Datenschutz, EU-Richtlinien)/Compliance“ (80,3%), die „Vermeidung von (Geld/Image)Verlusten durch Sicherheitsvorfälle oder Datenpannen“ (71,5%), die Vorbeugung von „Datenverlusten/Verfälschung“ (68,9%), die „starke Abhängigkeit von eigener IT in gewissen Geschäftsprozessen“ (55,7%) sowie die Sicherstellung der „Stabilität des Betriebs“ (53,5%) genannt. 18,4% bzw. 12,7% nennen „Vorfälle in der Vergangenheit“ bzw. „Vorfälle, über die in Medien berichtet wurde“ als Grund. Das NSA-Überwachungsskandal hingegen wurde lediglich von 3,1% aufgeführt.

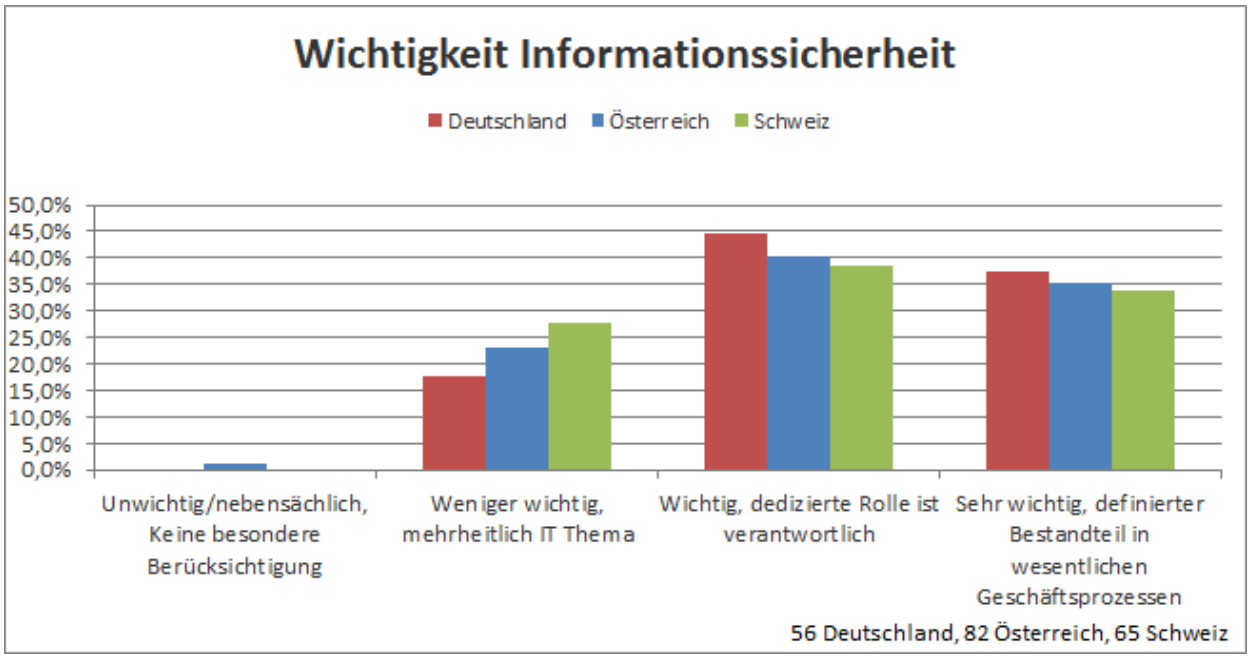

Abbildung 4.9.: Länderspezifisch: Wichtigkeit der Informationssicherheit

Im Ländervergleich in 4.11 sind einige Unterschiede ersichtlich. Insbesondere interessant ist, dass „Forderung von Kunden/Partnern“ in Österreich lediglich von knapp 22% der Unternehmen als Grund genannt wurde, während in Deutschland und der Schweiz jeweils ungefähr 38% diese Antwort gaben. Auch „Gesetzliche Vorgaben/Compliance“ werden in Österreich von lediglich 73% der Unternehmen genannt während in Deutschland bzw. der Schweiz 87,3% bzw 81,5% diese Angabe machen.

Bei der Nutzung von Standards und Empfehlungen im Bereich der Informationssicherheit, welche in Abbildung 4.12 dargestellt wird werden wie zu erwarten „ISO 27001“ (69,1%), „BSI - IT-Grundschutz“ (52,3%), „ITIL“ (49,1%) und „COBIT“ (26,4%) am häufigsten genannt. Der „BSI - Grundschutz kompakt“ (31,8%) sowie die „OWASP Top 10“ (32,7%) werden ebenfalls verbreitet genutzt. Auch die relativ neuen „SANA Critical Security Controls“ werden von 10,9% der Unternehmen genannt. Lediglich 12,7% der Unternehmen geben an, „keine speziellen Standards oder Empfehlungen“ im Bereich der Informationssicherheit zu verwenden.

Bei der Antwort „keine speziellen Standards oder Empfehlungen“ im Bereich der Informationssicherheit zu nutzen, sticht Österreich mit 21% im Vergleich zu Schweiz und Deutschland mit 12,7% und 5,7% hervor. Die weiteren länderspezifischen Unterschiede sind in Abbildung 4.13 ersichtlich. Es ist auffallend, dass in der Schweiz die Nutzung der „ISO 27001“ mit 84,1% im Vergleich zu Österreich und Deutschland mit 60,5% bzw 62,4% besonders hoch ist. Interessanterweise werden „ITIL“ und „COBIT“ in Deutschland im Vergleich zu der Schweiz und Österreich weniger oft genannt.

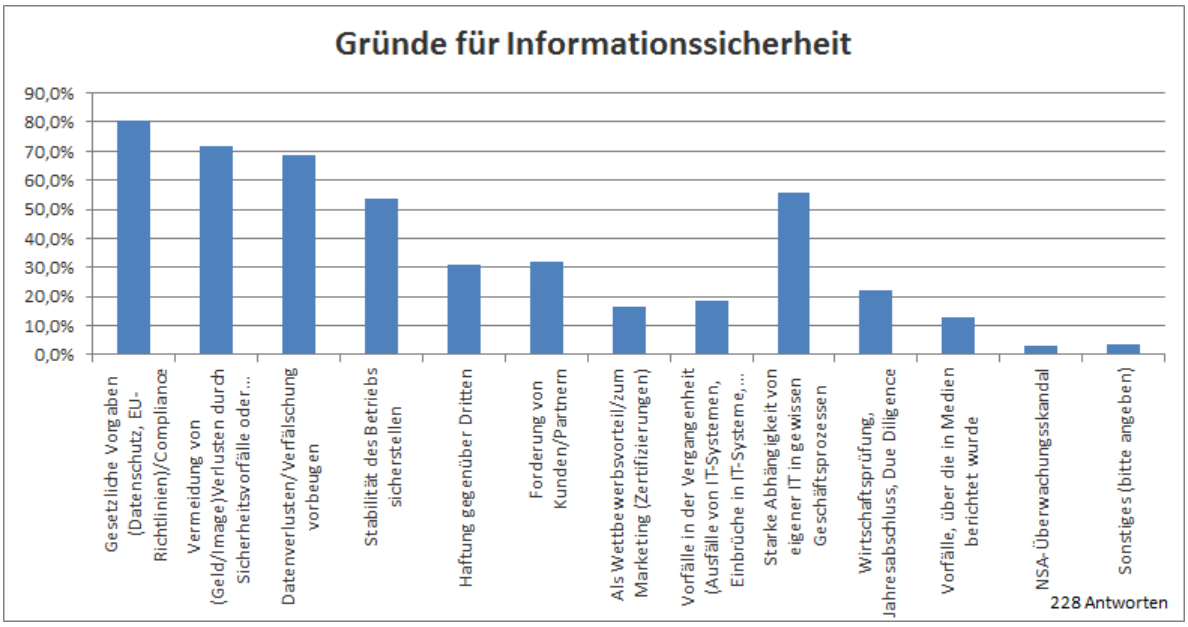

Abbildung 4.10.: Gründe und Motivation für Informationssicherheit

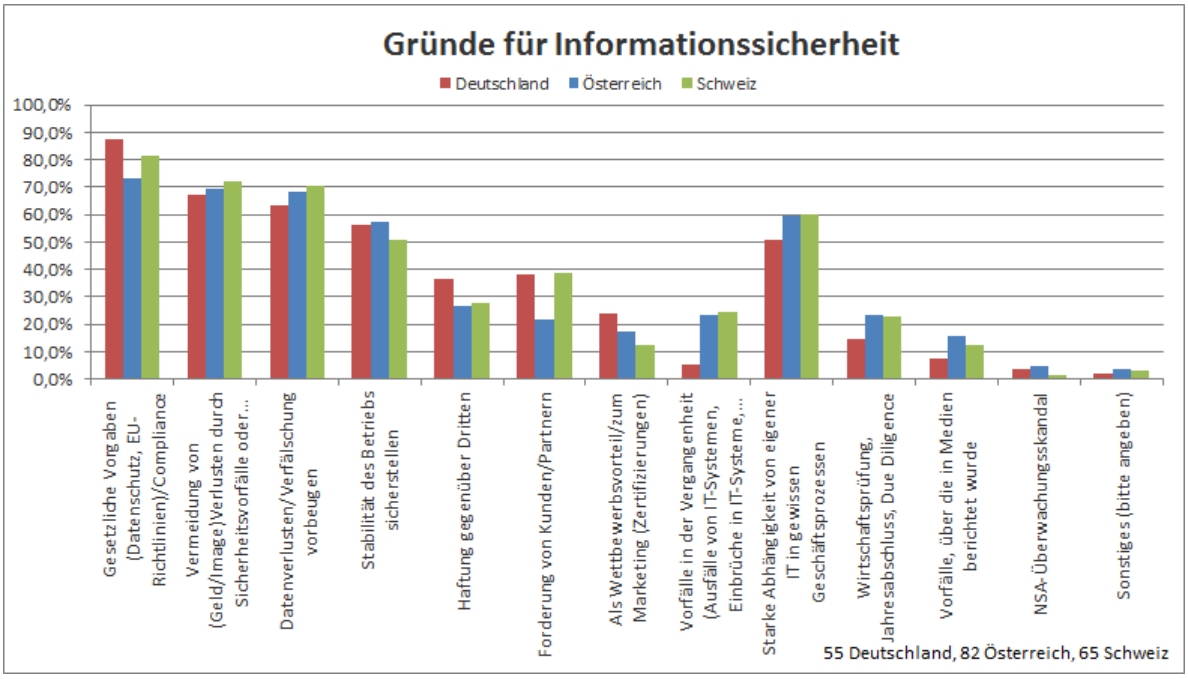

Abbildung 4.11.: Länderspezifisch: Gründe und Motivation für Informationssicherheit

Bei den sonstigen Antworten wurden etwa auch Standards wie „Common Criteria for Information Technology“, „ISF Standard of Good Practice“, die „CSA Cloud Control Matrix“, „ISAE 3402“, das „US Cyber Security Framework“, das „Schweizer Informationssicherheitshandbuch für die Praxis“ sowie die „ÖNORM A7700“ genannt.

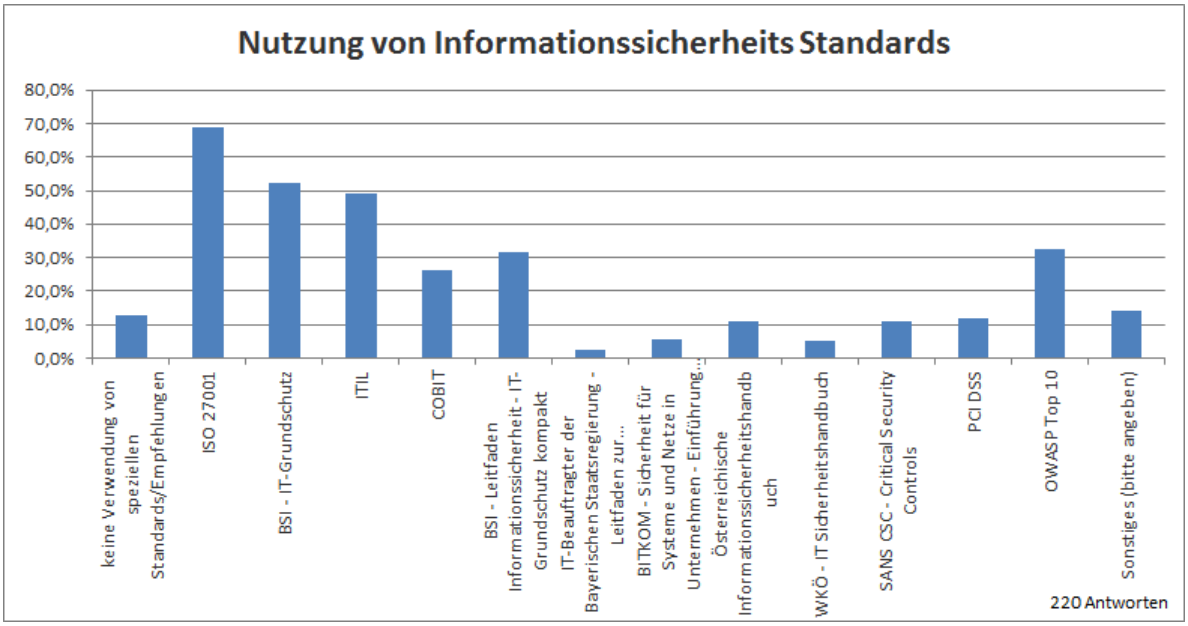

Abbildung 4.12.: Nutzung von Standards & Empfehlungen im Bereich der Informationssicherheit

In Bezug zur Informationssicherheit gibt es verschiedenste Risiken und Bedrohung, denen sich Unternehmen ausgesetzt fühlen. Hierbei am häufigsten genannten werden, wie in Abbildung 4.14 ersichtlich, „Malware (Viren, Trojaner, Spyware etc.)“ (57,3%), „Datendiebstahl (unautorisierte Person erlangt Daten)“ (49,3%), „Fahrlässigkeit eigener Mitarbeiter“ (39,6%), „Datenverluste (Daten gelöscht/verloren, nicht mehr wiederherstellbar)“ (34,4%) sowie „APTs (zielgerichtete, komplexe, fortgeschrittene Angriffe)“ (30,8%) und „Social Engineering“ (30%).

Zwischen den verschiedenen Ländern gibt es auch in dieser Frage, wie in Abbildung 4.15 ersichtlich, einige Unterschiede. Sie sind aber meist nicht sehr groß und Betragen höchstens ca. 10%.

Ein weiteres wichtiges Risiko für die Verfügbarkeit der IT, welches unter den sonstigen genannt wurde, ist der „Ausfall kritischer (interner Versorgungs-)Infrastruktur (Klima, Netzwerk)“.

Als Hauptprobleme bei Aufrechterhaltung & Verbesserung der Informationssicherheit werden in Abbildung 4.16 „fehlendes Budget“ (54,0%), „fehlende Unterstützung und Bewusstsein (z.B. zu Risiken und Gefahren) im (Top)Management“ (54,5%), „fehlendes Bewusstsein der Mitarbeiter“ (66,1%), „fehlende Mitarbeiter-Akzeptanz für Sicherheitsmaßnahmen, die die Usability/Benutzbarkeit einschränken“ (65,2%) sowie „sich schnell ändernde Systemumgebung und Angriffsarten“ (42,0%) genannt.

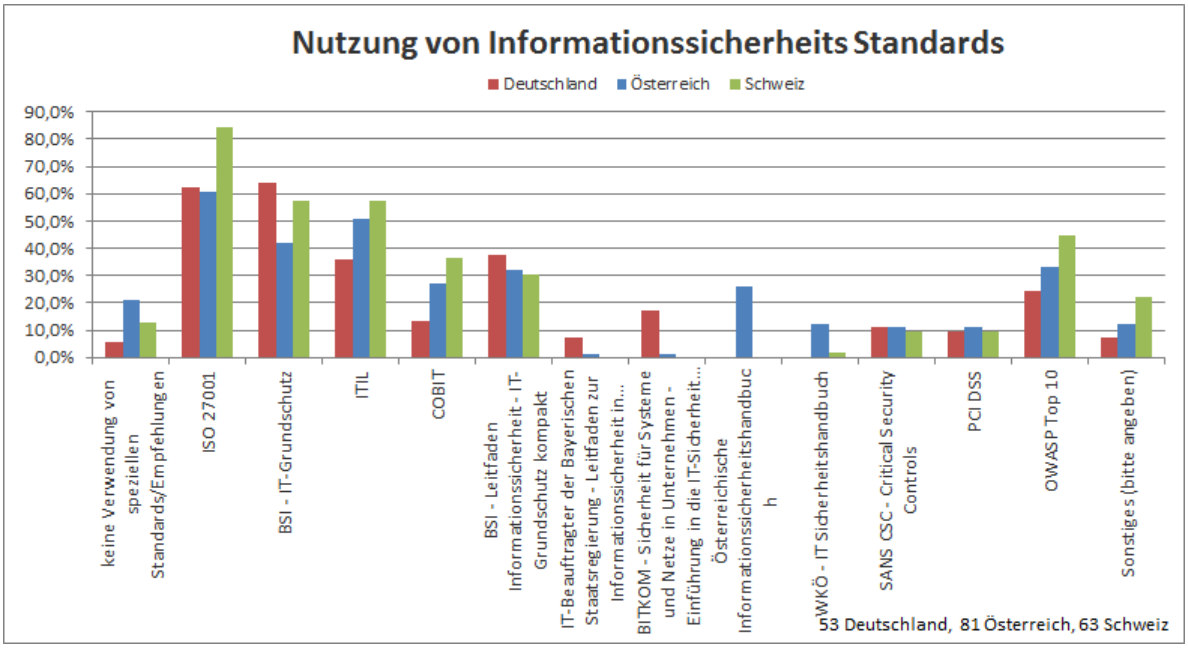

Abbildung 4.13.: Länderspezifisch: Nutzung von Standards & Empfehlungen im Bereich der Informationssicherheit

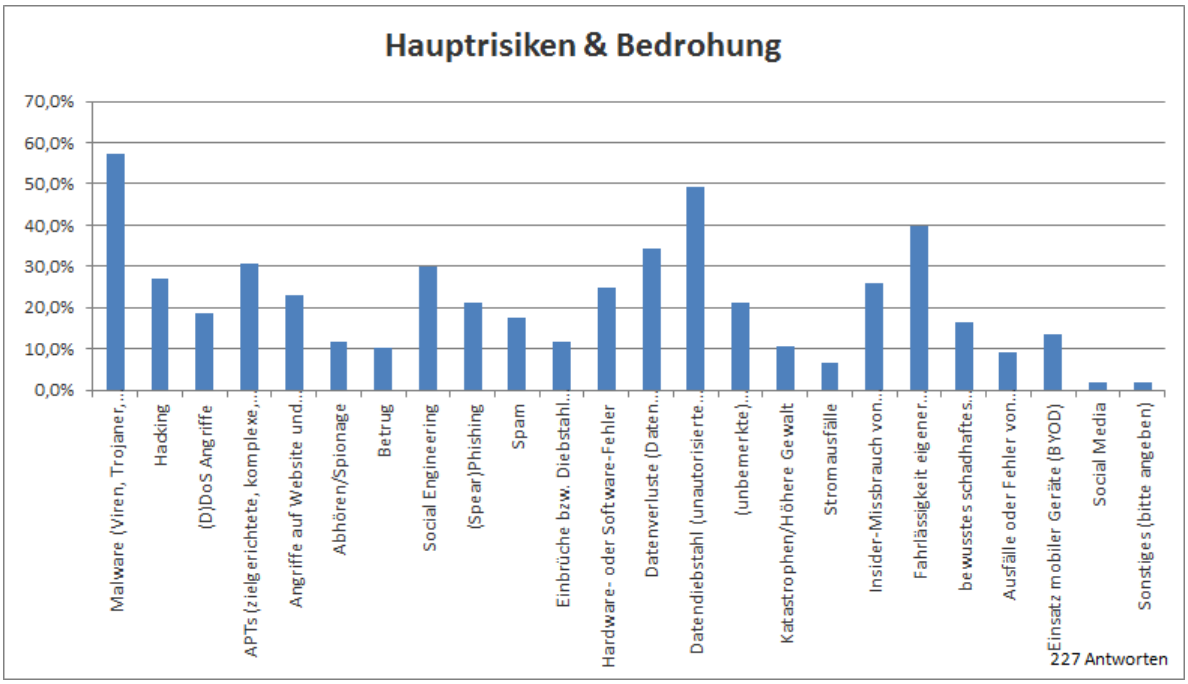

Abbildung 4.14.: Hauptrisiken & Bedrohung in Bezug zur Informationssicherheit

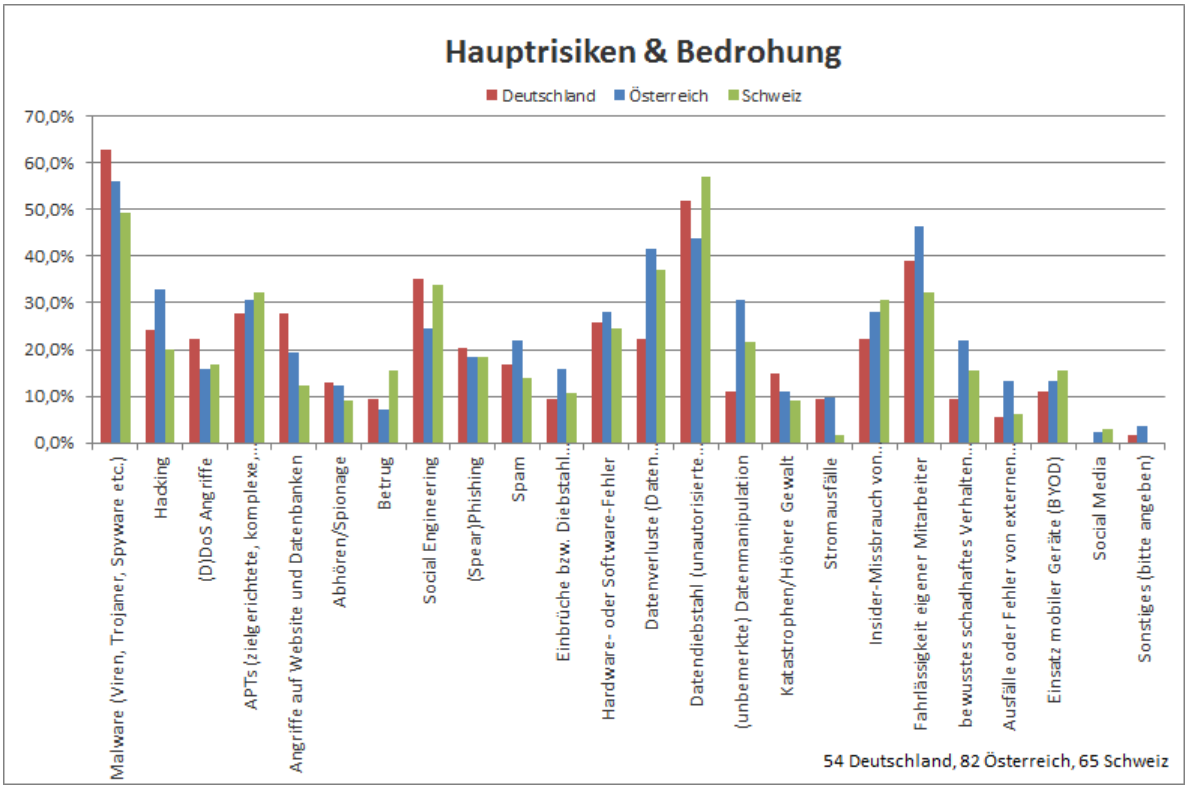

Abbildung 4.15.: Länderspezifisch: Hauptrisiken & Bedrohung in Bezug zur Informationssicherheit

Im Ländervergleich gibt es bei dieser Frage, wie in Abbildung 4.17 zu sehen, zwischen Österreich, Deutschland und der Schweiz kaum Unterschiede.

Unter Sonstiges wurden noch einige weitere interessante Probleme aufgezeigt. Insbesondere wurde die „fehlende Zeit um Maßnahmen umzusetzen oder auszuarbeiten“, „für die Sicherheit immer höher werdende Aufwände (vor allem zeitlichen Ressourcen), „Personalressourcenengpässe“, und der Fakt, dass die „Ressource Mensch zu teuer (wertvoll) ist, um sie für Sicherheit auszugeben“ genannt. Als ein weiteres Hauptproblem wird „die Dynamik der Veränderung, die durch Technologie und neue Arbeitsformen verursacht wird“ genannt (Stichwort mobile Geräte, BYOD, Remote Arbeit, verschwimmende Grenzen des Unternehmensnetzwerkes). Auf technischer Ebene werden die „Redundanzen in technischen Lösungen/ zu hohe Vielfalt an Tools“ sowie „Standards mit zweifelhafter Sicherheit (AES, elliptische Kurven)“ als Problem genannt. Auch der fehlende „Willen sich permanent verbessern zu müssen“ wird sehr treffend als ein bei der Verbesserung der Informationssicherheit hemmender Faktor aufgeführt.

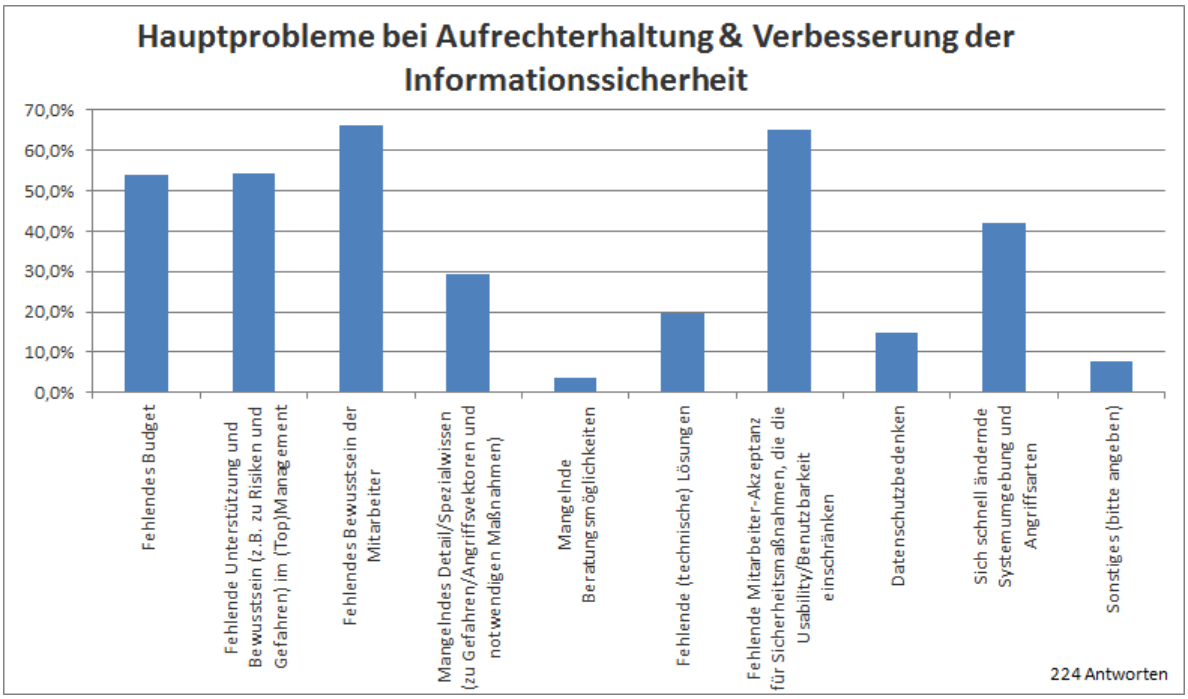

Abbildung 4.16.: Hauptprobleme bei der Aufrechterhaltung & Verbesserung der Informationssicherheit

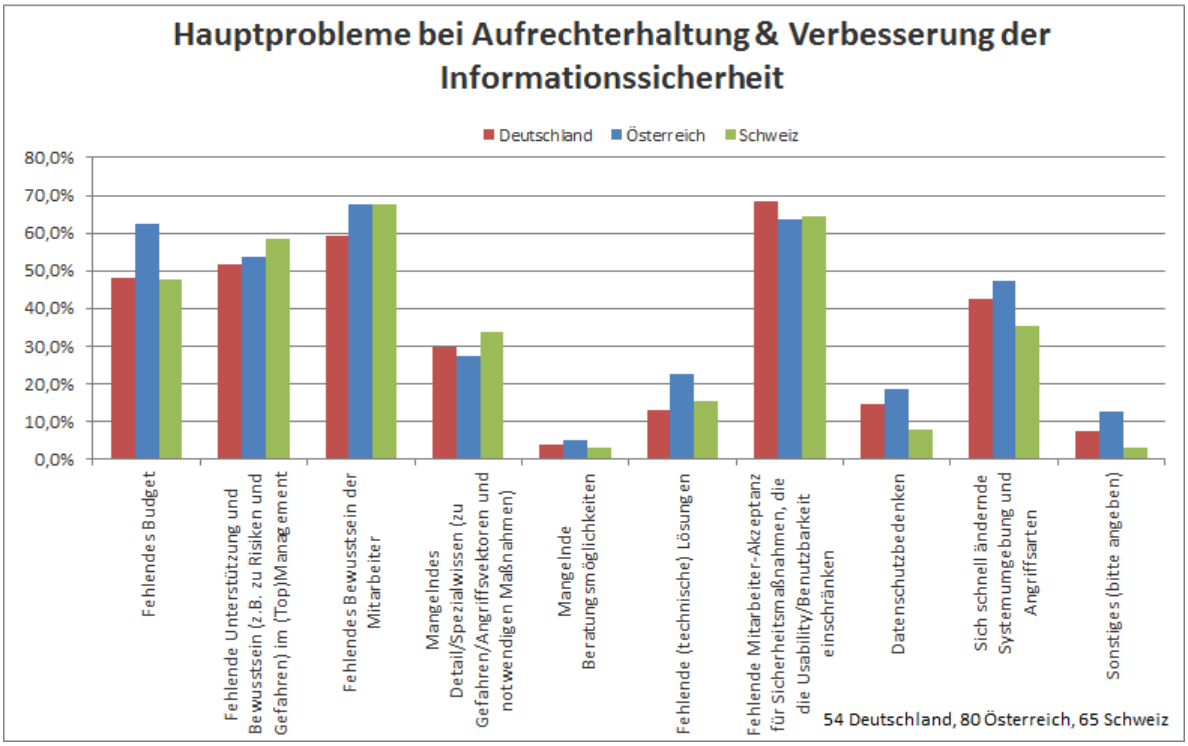

Abbildung 4.17.: Länderspezifisch: Hauptprobleme bei der Aufrechterhaltung & Verbesserung der Informationssicherheit

4.2.3. Aktuelle Situation im Unternehmen - Informationssicherheits-Policy, Richtlinien, Evaluierung der Informationssicherheit, Beratung, Vorfälle

In Frage 8, welche die grundlegende organisatorische Regelung und Verantwortung für die Informationssicherheit untersucht, gaben - wie in Abbildung 4.18 ersichtlich - eine große Mehrheit von 76,2% an, dass es in ihrem Unternehmen einen „Informationssicherheits-Verantwortlichen und eine Informationssicherheits-Policy“ gibt. In 14,3% der Unternehmen gab es zwar eine verantwortliche Person, jedoch ohne unternehmensweite Richtlinie zur Informationssicherheit, während lediglich in 9,4% der Unternehmen weder die Verantwortung, noch eine Richtlinie definiert waren.

Im Ländervergleich in Abbildung 4.19 fallen nur geringe Unterschiede auf. In Österreich ist der Anteil der Unternehmen mit geregelter Verantwortlichkeit und Richtlinie mit 66,7% etwas geringer als der Schweiz und Deutschland, bei denen 80% bzw. 83,6% diese Angabe machten. In Deutschland hatten lediglich 3,6% der Unternehmen weder die Verantwortung, noch eine Richtlinie definiert, während dies in Österreich und der Schweiz bei 11,1% bzw 12,3% der Unternehmen der Fall war.

Auch in dieser Frage wird ersichtlich, dass die meisten Teilnehmerinnen und Teilnehmer dieser Umfrage ein hohes Bewusstsein für das Thema der Informationssicherheit haben und zumindest grundlegende organisatorische Rahmenbedingungen (Verantwortlichkeit und Richtlinie) von einer großen Mehrheit der Unternehmen geregelt werden.

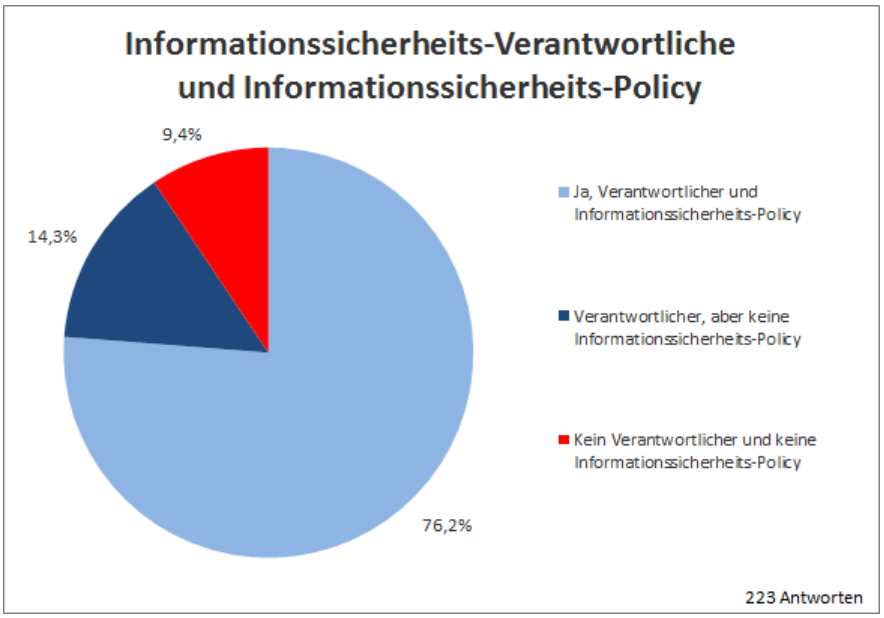

Abbildung 4.18.: Informationssicherheits-Verantwortliche und Informationssicherheits-Policy

In der nächsten Frage, welche in Abbildung 4.20 dargestellt ist, werden in den Unternehmen vorhandene Richtlinien und Vorgaben zur Informationssicherheit behandelt. Nur eine Minderheit von 6,7% der

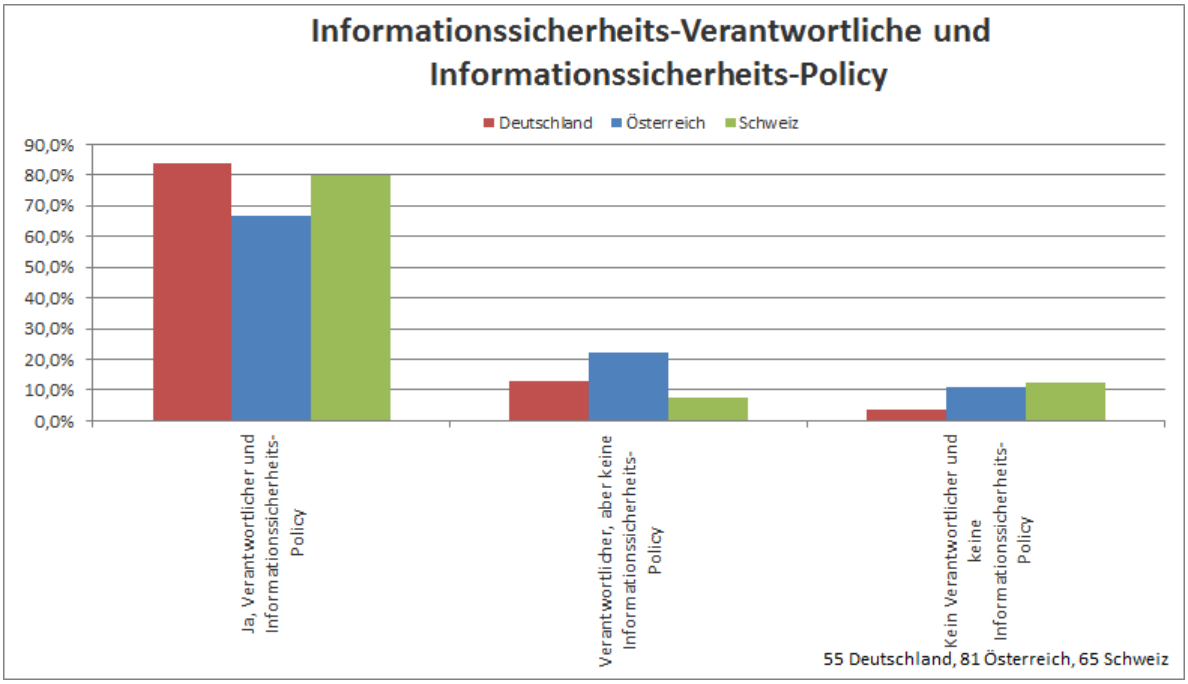

Abbildung 4.19.: Länderspezifisch: Informationssicherheits-Verantwortliche und Informationssicherheits-Policy

Unternehmen gab an, dass es bei ihnen „keine Richtlinien und Vorgaben“ gibt. Am häufigsten wurden „Passwortrichtlinien“ (86,5%) sowie Vorgaben zur „Nutzung Mail, Internet & Social Media“ (84,5%) genannten. Auch Vorgaben zur „Datenvernichtung und Geräteentsorgung“ (71,7%) sowie zur „Nutzung mobiler Geräte (etwa auch BYOD) und Speichermedien“ (68,2%) wurden oft genannt. Es fällt auf, dass der mit 43,9% am seltenste genannte Punkt „Dokumentationsvorgaben/-anforderungen“ ist. Dies kann ein Indikator sein, welcher die oft geäußerte Meinung bestätigt, dass viele Unternehmen technisch relativ gut aufgestellt sind, jedoch in der Organisation (Steuerung, Regelungen, Dokumentation, regelmäßige Überprüfung und Kontrolle der getroffenen Maßnahmen) Schwächen bestehen.

Im Ländervergleich gab es auch in dieser Frage einige Unterschiede, welche in Abbildung 4.21 ersichtlich sind. Besonders auffällig ist, dass in Deutschland lediglich 1,8% der Unternehmen angaben „keine Richtlinien/Vorgaben“ zu besitzen, während dies bei 9,9% bzw 9,2% der Unternehmen aus Österreich und der Schweiz der Fall war. Weiters interessant ist, dass in der Schweiz 64,4% angaben Vorgaben zum wichtigen Thema der „Informationsklassifikation & Verarbeitung“ zu besitzen, während dies nur 54,5% bzw. 45,7% der deutschen und österreichischen Unternehmen taten. Generell sind diverse Richtlinien/Vorgaben in Österreich am wenigsten weit verbreitet.

Bei Sonstiges wurden unter anderem „Inter-Enterprise Services Vereinbarungen“, sowie Richtlinien zum „Schutz vor Schadsoftware“, „sichere Entwicklung und Beschaffung“, „sicheren Betrieb“, „Netzwer-

ke und Firewalls“, „Physische Sicherheit“, „Kryptografie“, „Security Incident Handling und IT-Notfallmanagement“ und von einem anscheinend relativ spezialisierten Unternehmen „Vorgaben für Entwicklung und Betrieb von SCADA-Systemen“ genannt.

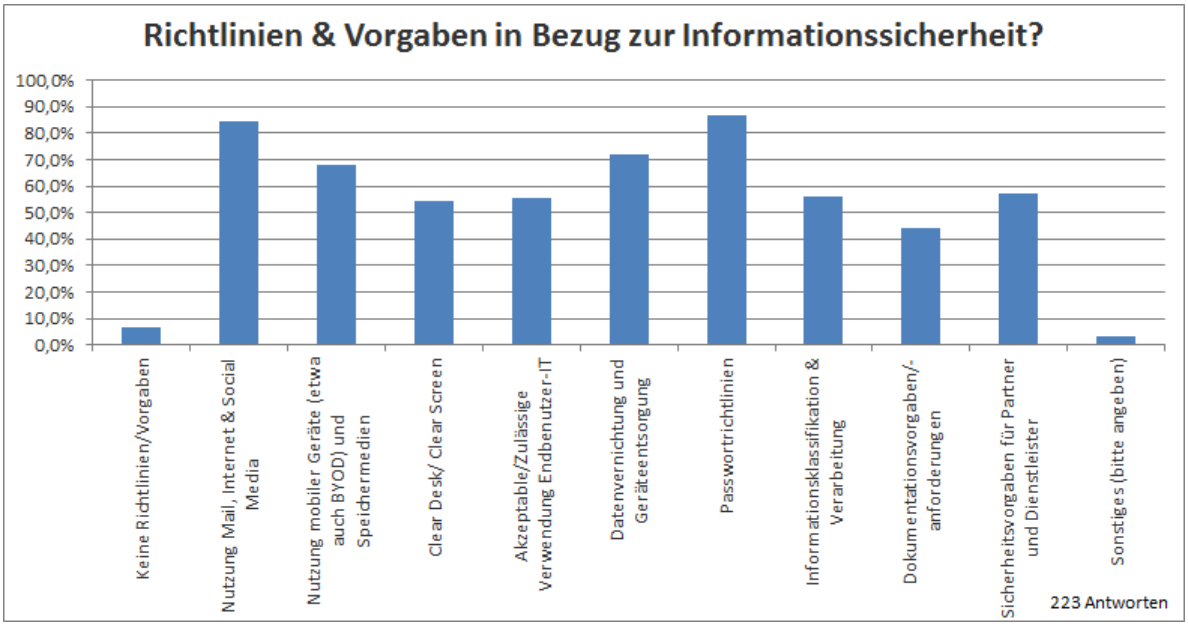

Abbildung 4.20.: Richtlinien & Vorgaben in Bezug zur Informationssicherheit

Bezüglich Aktivitäten zur Überprüfung der Informationssicherheit gaben, wie in Abbildung 4.22 ersichtlich, nur 14,8% an „keine regelmäßigen Überprüfungsaktivitäten“ durchzuführen. Am häufigsten wurde die „Durchführung von internen Audits“ (70,4%) genannt. Andere Aktivitäten wie „externe Audits“, „Penetration Tests“ und „Vulnerability Scans“ wurden relativ einheitlich von ca. 57% der Unternehmen genannt.

Im Ländervergleich in Abbildung 4.23 gibt es einige Unterschiede. In Deutschland gaben nur 10,9% an „keine regelmäßigen Überprüfungsaktivitäten“ durchzuführen, während dies in Österreich und der Schweiz 21% bzw. 15,4% der Unternehmen angaben. Interessanterweise wurde die „Durchführung von Vulnerability Scans“ nur von 40% der deutschen Unternehmen als Überprüfungsaktivität genannt (im Vergleich zu 59,3% Österreich, 61,5% Schweiz). Weiters auffallend ist, dass in der Schweiz die „Durchführung von externen Audits“ von 75,4% der Unternehmen genannt wurde (im Vergleich zu 52,7% Deutschland und 46,9% Österreich). Dies kann unter anderem damit zusammenhängen, dass wie in Abbildung 4.13 ersichtlich die Nutzung des ISO 27001 Standards (mit welchem externe Audits verbunden sind) in der Schweiz sehr weit verbreitet ist.

In Abbildung 4.24 ist zu sehen, dass ein Großteil der Unternehmen auf externe Hilfe bei diversen Informationssicherheits-Themen zurückgreift. Nur eine Minderheit von 28,3% der Unternehmen gab an „keine externe Beratung“ in Anspruch zu nehmen. Mit knapp 59% war der Einsatz von Externen bei

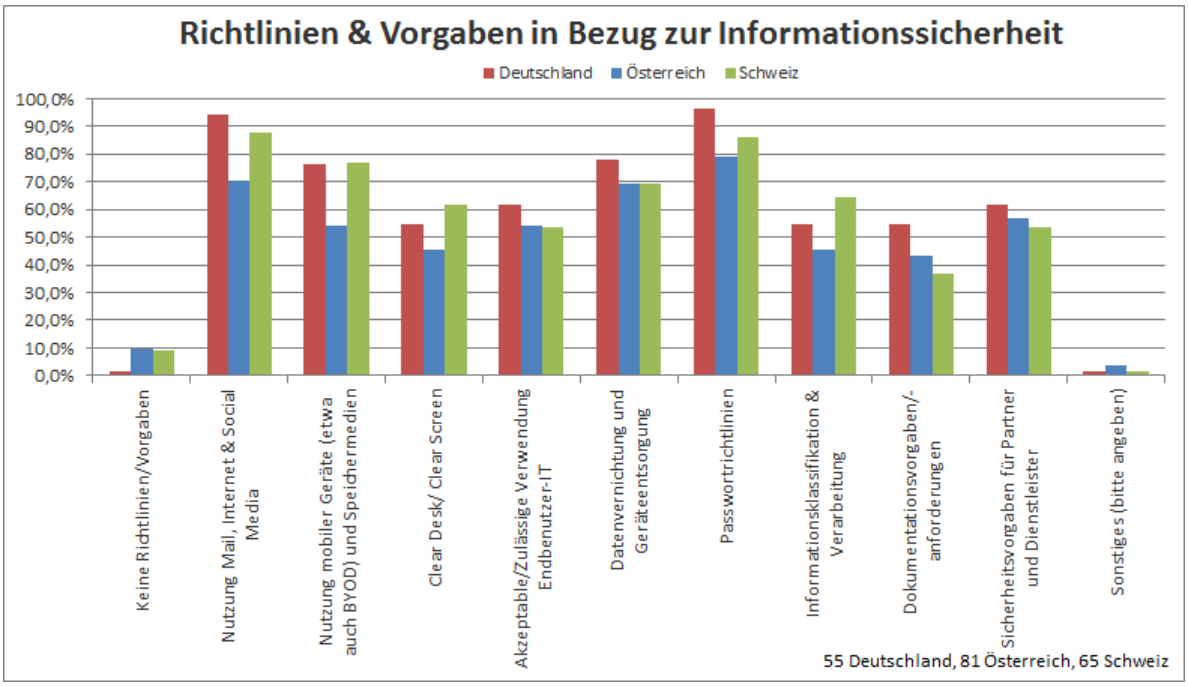

Abbildung 4.21.: Länderspezifisch: Richtlinien & Vorgaben in Bezug zur Informationssicherheit

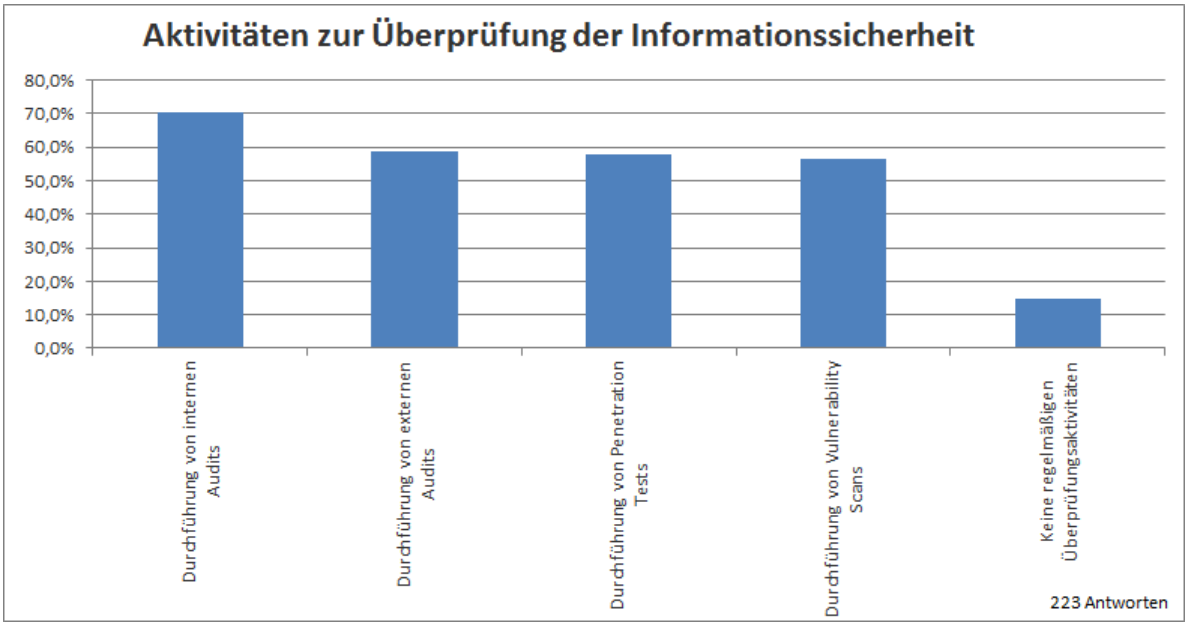

Abbildung 4.22.: Aktivitäten zur Überprüfung der Informationssicherheit

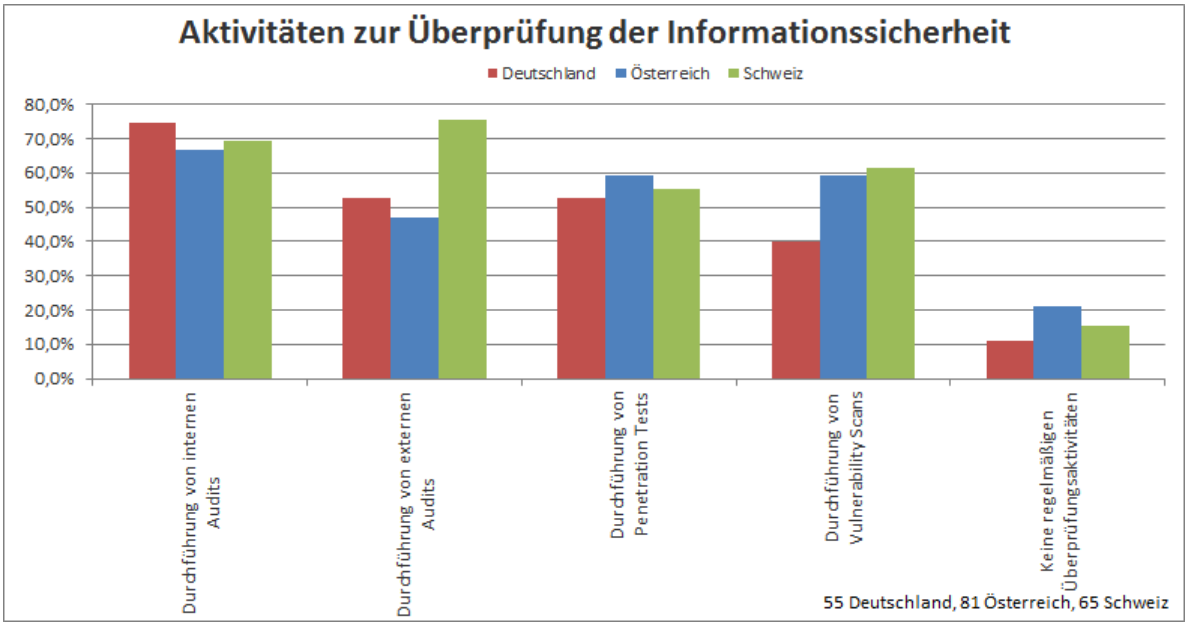

Abbildung 4.23.: Länderspezifisch: Aktivitäten zur Überprüfung der Informationssicherheit

der „Durchführung von Audits und Penetration Tests“ am häufigsten. 25,6% ließen sich bei der „Durchführung von Schulungen“ unterstützen. Auch „Informationssicherheits-Strategie- und Managementberatung“ (21,9%), „Durchführung von Risikoanalysen“ (23,3%), „Beratung bei Produkterwerb und Implementierung“ (21,9%) sowie „Entwicklung von Informationssicherheits-Prozessen und -Maßnahmen sowie Optimierung dieser“ (19,2%) wurden jeweils knapp von einem Fünftel der Teilnehmerinnen und Teilnehmer genannt. Am seltensten wurden die Punkte „Incident Response“ (7,3%) und „Forensik“ (9,1%) erwähnt.

Im Ländervergleich in Abbildung 4.25 ist der auffallendste Unterschied, dass in der Schweiz 70,3% die „Durchführung von Audits, Penetration Tests“ nannten während dies in Deutschland und Österreich nur 51,9% bzw. 53,1% der Unternehmen taten. Diese Angabe deckt sich jedoch mit der vorigen Frage, in der die „Durchführung von externen Audits“ in der Schweiz im Vergleich zu Österreich und Deutschland erheblich häufiger genannt wurde.

In Abbildung 4.26 werden die Antworten der Unternehmen bezüglich tatsächlich aufgetretener Vorfälle im Bereich der Informationssicherheit im vergangenen Jahr dargestellt. Lediglich eine Minderheit von 11,1% gab an, im vergangenen Jahr von keinen Vorfällen betroffen gewesen zu sein. Dies bedeutet, dass beim Großteil von knapp 89% der Unternehmen, im letzten Jahr zumindest ein Vorfall im Bereich der Informationssicherheit aufgetreten war. 53,5% der Unternehmen gaben an, dass sie von „Malware (Viren, Trojaner, Spyware etc.)“ betroffen waren, während als zweit häufigste Vorfallsart „Spam“ von 46,5% genannt wurde. Auch die „Fahrlässigkeit von Mitarbeitern“ (28,6%), „Hardware- oder Software-

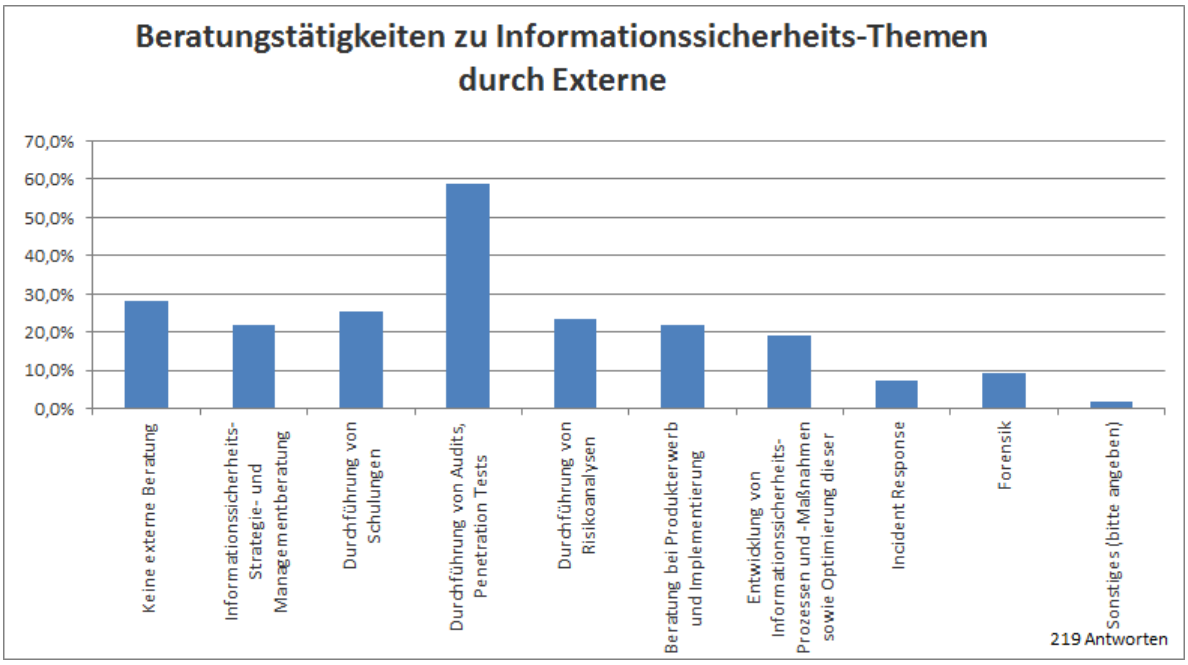

Abbildung 4.24.: Beratungstätigkeiten zu Informationssicherheits-Themen durch Externe

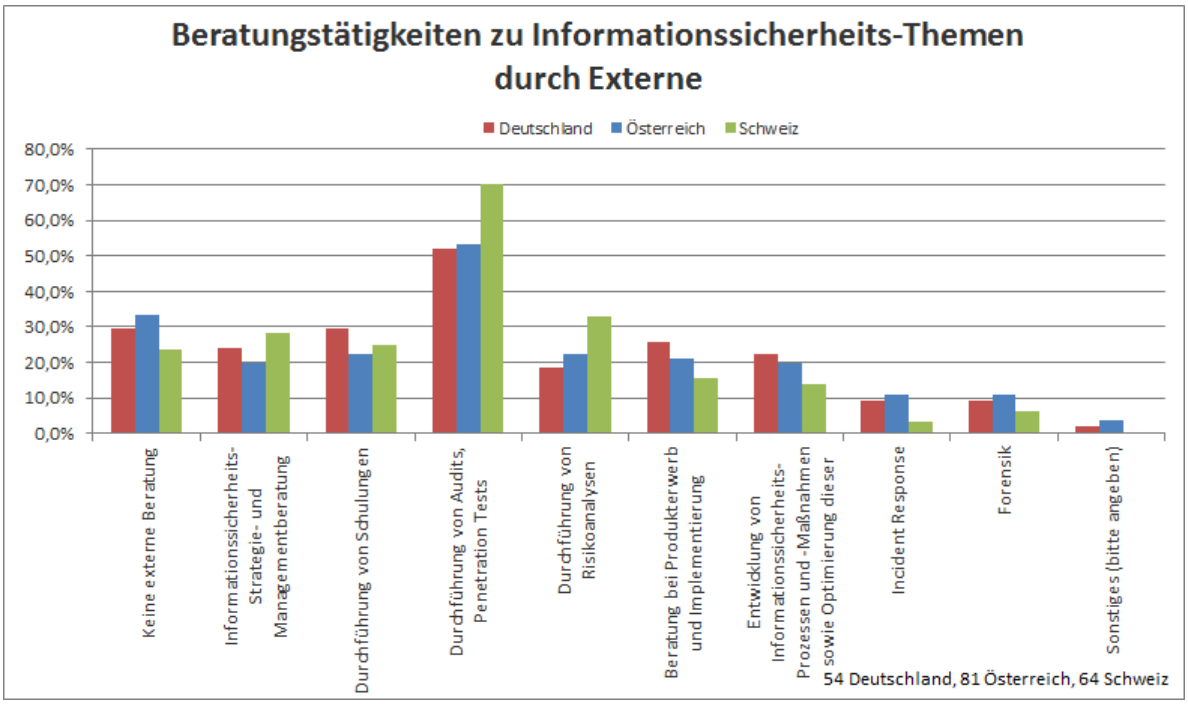

Abbildung 4.25.: Länderspezifisch: Beratungstätigkeiten zu Informationssicherheits-Themen durch Externe

Fehler“ (28,6%), „Stromausfälle“ (25,3%) sowie „(Spear)Phishing“ (21,2%) wurde häufig genannt. Von Hacking oder D(DOS) Angriffen waren anscheinend nur relativ wenige Unternehmen betroffen (9,7% bzw. 15,2%). Nur eine Minderheit von 5,5% der Unternehmen gab an von „APTs (zielgerichtete, komplexe, fortgeschrittene Angriffe)“ betroffen gewesen zu sein (eine nähere Behandlung des Themas APTs befindet sich in Frage 18 in Abbildung 4.38 und 4.39).

Interessanterweise gaben ähnlich wie bei meiner letzten Umfrage (siehe [1, S. 35]) 15,7% der Unternehmen an, von „Datenverlusten (Daten gelöscht/verloren, nicht mehr wiederherstellbar)“ betroffen gewesen zu sein. Angesicht des verbreiteten technischen und organisatorischen Engagements im Backup & Wiederherstellungsbereich (siehe 4.2.5 und 4.2.5, jeweils von knapp 100% als implementiert genannt) ist dies doch ein überraschend hohes Ergebnis, welches dafür spricht, dass der „Reifegrad“ (Qualität der Umsetzung, Effektivität und Effizienz) der implementierten Maßnahmen zwischen den Unternehmen doch mitunter stark schwankt.

Bei den sonstigen Angaben wurde einige Male darauf hingewiesen, dass aufgrund der Vertraulichkeit keine Angaben zu Vorfällen gemacht werden können. Als eine andere Art von „Vorfällen“ wurde die sehr hohe Anzahl an „Vulnerabilities“ in diversen Softwareprodukten genannt (durch notwendige Patches kann die Verfügbarkeit der Software beeinträchtigt werden. Weiters entsteht Zeit- und Koordinationsaufwand).

Im Ländervergleich in Abbildung 4.27 fällt insbesondere auf, dass in der Schweiz sowohl bei „Malware (Viren, Trojaner, Spyware etc.)“ als auch bei „Spam“ jeweils ca. 10% weniger Antworten als in Deutschland und Österreich gab und „(Spear)Phishing“ mit 26,6% im Vergleich zu Deutschland und Österreich mit 13% und 19% ein größeres Problem war.

Bei Gegenüberstellung der Informationssicherheitsvorfälle mit den in Abbildung 4.14 dargestellten wahrgenommenen Risiken & Bedrohungen fällt auf, dass die Einschätzung bei „Malware“ sehr gut übereinstimmt (53,5% Vorfälle, von 57,3% als Risiko wahrgenommen). Die größten Differenzen (höhere Risikoeinschätzung als es Vorfälle gab) lassen sich hier insbesondere bei „Datendiebstahl“ (3,2% Vorfälle, von 49,3% als Risiko wahrgenommen. Insbesondere bei Datendiebstahl stellt sich jedoch die Frage, wie viele Unternehmen einen solchen Vorfall tatsächlich erkennen), APTs (5,5% Vorfälle, von 30,8% als Risiko wahrgenommen) sowie auch bei „Hacking“ (9,7% Vorfälle, von 26,9% als Risiko wahrgenommen), „Datenverlusten“ (15,7% Vorfälle, von 34,4% als Risiko wahrgenommen), „(unbemerkte) Datenmanipulation“ (1,4% Vorfälle, von 21,1% als Risiko wahrgenommen) und „Insider Missbrauch von Rechten/Systemen“ (7,4% Vorfälle, von 26% als Risiko wahrgenommen) erkennen.

„Spam“ und „Stromausfälle“ werden jeweils von viel weniger Unternehmen als Risiko wahrgenommen (wobei reiner Spam im Gegensatz zu Phishing kein großes Schadenspotential hat und darum wahrscheinlich eher nicht als Risiko genannt wurde), als es tatsächlich Vorfälle in diesem Bereich gab (bei Spam 46,5% Vorfälle, von 17,6% als Risiko wahrgenommen, bei Stromausfällen 25,3% Vorfälle, von 6,6% als Risiko wahrgenommen).

Eine Gesamtübersicht über die Differenz der Einschätzung der Risiken und der Nennung von Vorfällen ist in Tabelle 4.1 ersichtlich. Positive Differenzen bedeuten, dass eine bestimmte Kategorie in Frage 6 von mehr Unternehmen als Risiko angesehen wurde, als in Frage 12 Vorfälle in dieser Kategorie gemeldet worden sind. Im Gegenzug beschrieben negative Differenzen, dass diese Kategorie von weniger Unternehmen als Risiko angesehen wurde, als Vorfälle in dieser Kategorie in Frage 12 ausgewiesen wurden.

Vorfälle: Nennung Vorfälle Gesamt, ***Risiko***: Risiko Einschätzung Gesamt, ***Differenz***: Einschätzung Risiken - Nennung Vorfälle

Kategorie	***Vorfälle***	***Risiko***	***Differenz***
Malware (Viren, Trojaner, Spyware etc.)	53,5%	57,3%	3,8%
Hacking	9,7%	26,9%	17,2%
(D)DoS Angriffe	15,2%	18,5%	3,3%
APTs (zielgerichtete, komplexe, fortgeschrittene Angriffe)	5,5%	30,8%	25,3%
Angriffe auf Website und Datenbanken	17,1%	22,9%	5,9%
Abhören/Spionage	2,3%	11,9%	9,6%
Betrug	6,5%	10,1%	3,7%
Social Engineering	14,7%	30,0%	15,2%
(Spear)Phishing	21,2%	21,1%	-0,1%
Spam	46,5%	17,6%	-28,9%
Einbrüche bzw. Diebstahl Systeme/mobile Geräte	13,4%	11,9%	-1,5%
Hardware- oder Software-Fehler	28,6%	24,7%	-3,9%
Datenverluste (Daten gelöscht/verloren, nicht wiederherstellbar)	15,7%	34,4%	18,7%
Datendiebstahl (unautorisierte Person erlangt Daten)	3,2%	49,3%	46,1%
(unbemerkte) Datenmanipulation	1,4%	21,1%	19,8%
Katastrophen/Höhere Gewalt	0,9%	10,6%	9,7%
Stromausfälle	25,3%	6,6%	-18,7%
Insider Missbrauch von Rechten/Systemen	7,4%	26,0%	18,6%
Fahrlässigkeit Mitarbeiter	28,6%	39,6%	11,1%
bewusstes schadhaftes Verhalten eigener Mitarbeitern	3,7%	16,3%	12,6%
Ausfälle oder Fehler von externen Partnern/Cloud	8,3%	9,3%	1,0%
Einsatz mobiler Geräte (BYOD)	6,5%	13,7%	7,2%
Social Media	2,3%	1,8%	-0,5%
Anzahl Beantwortungen	***217***	***227***	

Legende: Hellgrau: mehr Vorfälle als Risiko Einschätzung; Dunkelgrau: höhere Risiko Einschätzung als Vorfälle

Tabelle 4.1.: Differenz Einschätzung Risiken - Nennung Vorfälle

Grundsätzlich gilt es aber - wie bereits in [1, S. 35] beschrieben - insbesondere bei der Frage nach Informationssicherheitsvorfällen zu beachten, dass viele Vorfälle auch unerkannt bleiben können (eventuell hohe Dunkelziffer?) und zweifelhaft ist, ob diese Frage von allen teilnehmenden Unternehmen vollständig und wahrheitsgemäß beantwortet worden ist (oft wird angenommen, dass Unternehmen zu diesem sensiblen Thema nur sehr ungern Angaben machen).

Außerdem gilt es in Bezug auf die Identifikation von Vorfällen zu beachten, dass gemäß der Auswertung der Frage 21 zu den getroffenen organisatorischen Maßnahmen (siehe 4.2.5) knapp 40% der Unternehmen angaben, (noch) keinen Vorfall-Management-Prozess implementiert zu haben. Das Fehlen eines solchen Prozesses zur geordneten Meldung, Klassifikation, Behandlung und Dokumentation von Vorfällen kann sich ebenfalls auf die Vorfall-Erkennungsraten und somit die Beantwortungen dieser Frage auswirken.

Weiters muss auch berücksichtigt werden, dass unterschiedliche Arten von Vorfällen unterschiedlich leicht bzw. schwer erkannt werden können (siehe etwa auch [27, S. 6,S. 40f]). So sind beispielsweise Malware-Vorfälle oder Spam meist leichter erkennbar als Hacking, Datendiebstahl, APTs, Spionage, Social Engineering oder Betrug. Weiters sind Unternehmen in gewissen Bereichen (etwa im Virenschutz oder der Spam Erkennung) meistens organisatorisch und technisch gut aufgestellt, was wiederum zu höheren Erkennungsraten bei diesen Vorfallsarten führen kann.

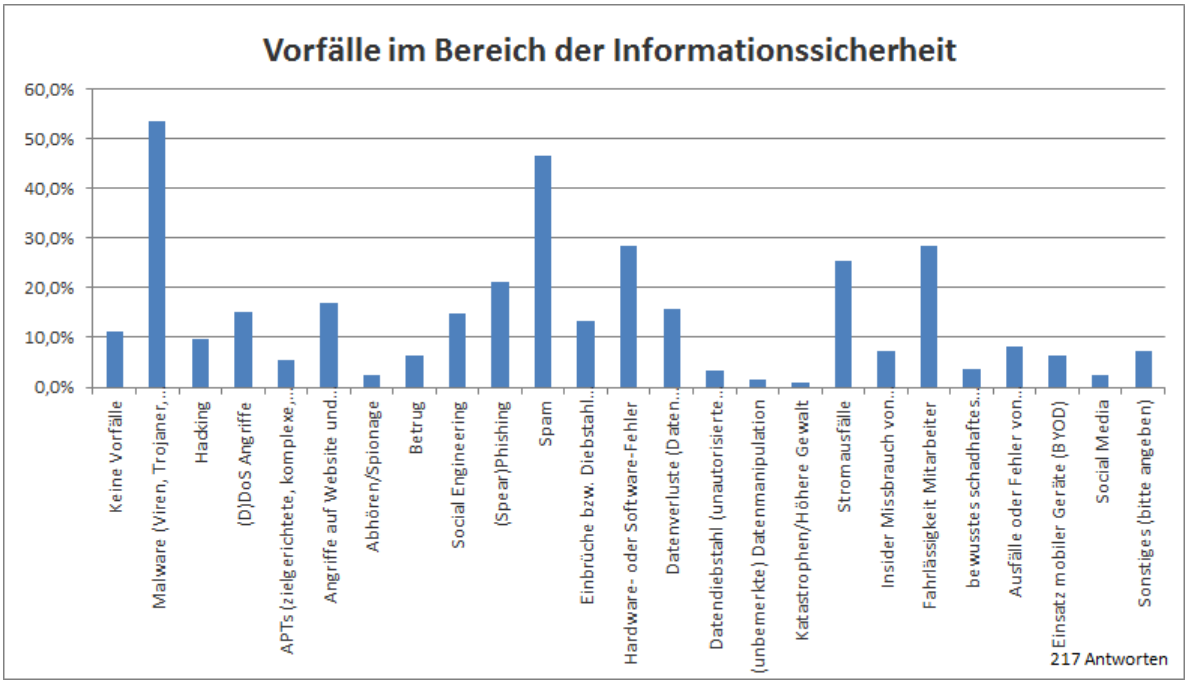

Abbildung 4.26.: Vorfälle im Bereich der Informationssicherheit

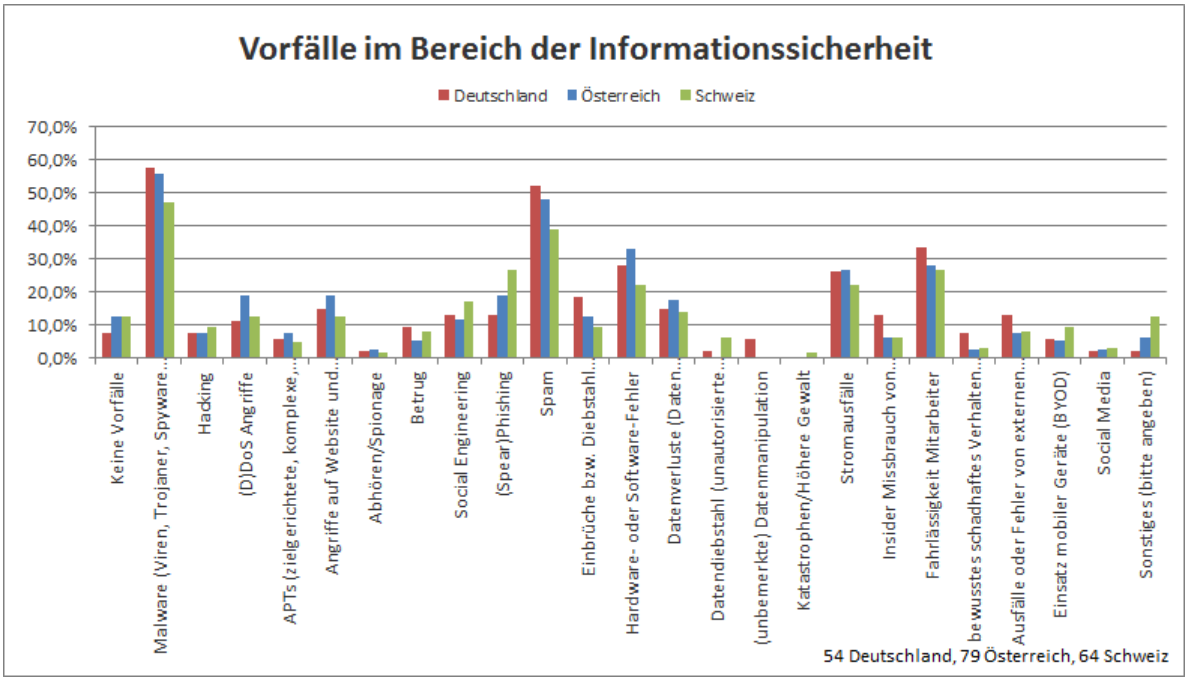

Abbildung 4.27.: Länderspezifisch: Vorfälle im Bereich der Informationssicherheit

4.2.4. „Trendthemen“ - mobile Geräte, Cloud & Outsourcing, Mitarbeiter-Awareness, Open Source Software, APTs, NSA-Enthüllungen

Die Ergebnisse der Frage zur Nutzung von mobilen Geräten und insbesondere „Bring your Own Device“ (BYOD), welche nun schon seit einigen Jahren ein wichtiges Thema sind, sind in Abbildung 4.28 dargestellt. Es ergibt sich das Bild, dass 37,7% der Unternehmen „mobile Geräte und BYOD nutzen und dabei spezifischen Sicherheitsmaßnahmen“ ergreifen. Weitere 12,3% nutzen zwar „mobile Geräte und BYOD, jedoch ohne spezielle Sicherheitsvorkehrungen“ zu treffen und wiederum 33,6% nutzen zwar mobile Geräte, jedoch kein BYOD. Lediglich eine Minderheit von 16,4% der Unternehmen gaben an, überhaupt keine mobilen Geräte und kein BYOD zu verwenden.

Im Ländervergleich in Abbildung 4.29 zeigen sich einige Unterschiede. Besonders auffällig ist, dass der Anteil der Schweizer Unternehmen, die angaben „mobile Geräte und auch BYOD inkl. spezieller Sicherheitsmaßnahmen“ einzusetzen mit 55,4% ungefähr doppelt so hoch wie in Deutschland und Österreich (mit 27,3% und 27,2%) ist. Österreich wiederum hatte bei der Nutzung von „mobilen Geräte und BYOD, jedoch ohne gesonderte Sicherheitsmaßnahmen“ zu ergreifen, mit 18,5% im Vergleich zu Deutschland und der Schweiz (7,3% bzw. 9,2%) relativ viele Antworten. In Deutschland gaben etwas über 47% der Unternehmen an, zwar mobile Geräte zu verwenden, jedoch explizit nicht in Form von BYOD (Österreich 34,6%, Schweiz 23,1%). Diese Antworten scheinen nahezulegen, dass in der Schweiz BYOD bereits am weitesten verbreitet und akzeptiert ist. Der Prozentsatz der Unternehmen, die weder mobile

Geräte noch BYOD einsetzen, ist im Ländervergleich relativ stabil (12,3% Schweiz, 18,2% Deutschland, 19,8% Österreich).

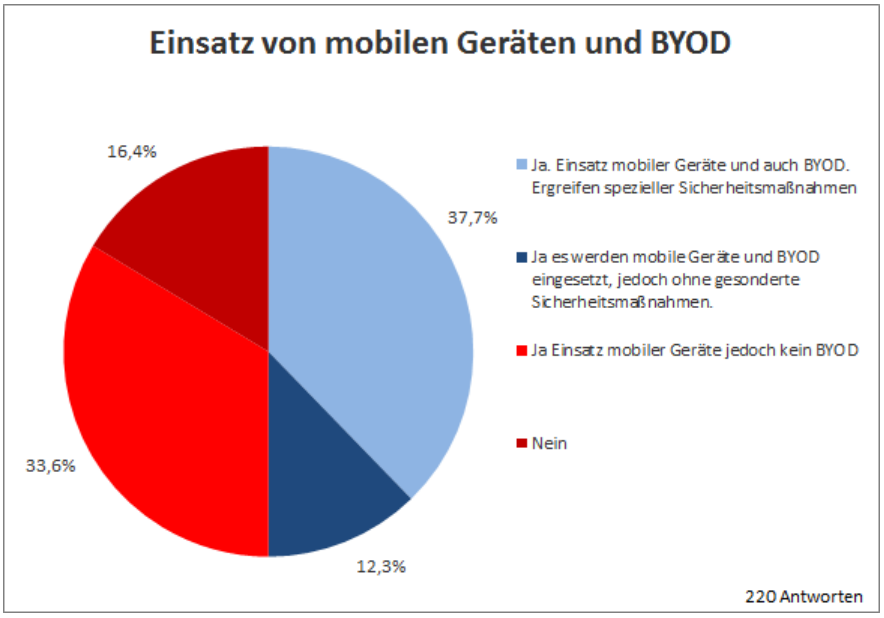

Abbildung 4.28.: Einsatz von mobilen Geräten und BYOD

In Abbildung 4.30 ist zu sehen, dass ein Großteil von 43,4% der Unternehmen angab „Cloud und/oder Outsourcing zu nutzen und dabei spezifische Sicherheitsmaßnahmen umgesetzt“ zu haben. Weitere 10,9% gaben zwar an im Bereich von „Cloud und Outsourcing aktiv zu sein, jedoch ohne Informationssicherheitsaspekte speziell zu berücksichtigen“. Von den verbleibenden Unternehmen erklärten 14,9% Cloud und Outsourcing „aufgrund von Sicherheitsbedenken und diverser Vorkommnisse (NSA-Skandal etc.)“ nicht zu nutzen, während weitere 30,8% keine speziellen Gründe nannten.

Im Ländervergleich in Abbildung 4.31 ist der auffallendste Unterschied, dass in Österreich lediglich 30,9% der Unternehmen angaben „Cloud und/oder Outsourcing zu nutzen und dabei spezifische Sicherheitsmaßnahmen umgesetzt“ zu haben (im Vergleich zu 52,7% Deutschland und 43,1% Schweiz). Dafür gaben jedoch in Österreich mit 16,0% die meisten Unternehmen an zwar im Bereich von „Cloud und Outsourcing aktiv zu sein, jedoch ohne Informationssicherheitsaspekte speziell zu berücksichtigen“ (im Vergleich zu 5,5% Deutschland und 10,8% Schweiz). Der Anteil der Unternehmen, die Cloud und Outsourcing aufgrund von Sicherheitsbedenken nicht nutzen, war in Österreich und der Schweiz (21,0% bzw. 15,4%) erheblich höher als in Deutschland mit nur 7,3%. Der Prozentsatz der Unternehmen die weder im Bereich von Cloud, noch in Bezug auf Outsourcing aktiv sind ist im Ländervergleich relativ stabil (34,5% Deutschland, 32,1% Österreich, 30,8% Schweiz).

Neben diversen technischen und organisatorischen Maßnahmen ist die Schulung, Aufklärung und Bewusstseinsbildung der Mitarbeiterinnen und Mitarbeiter in Bezug auf Themen der Informationssicherheit

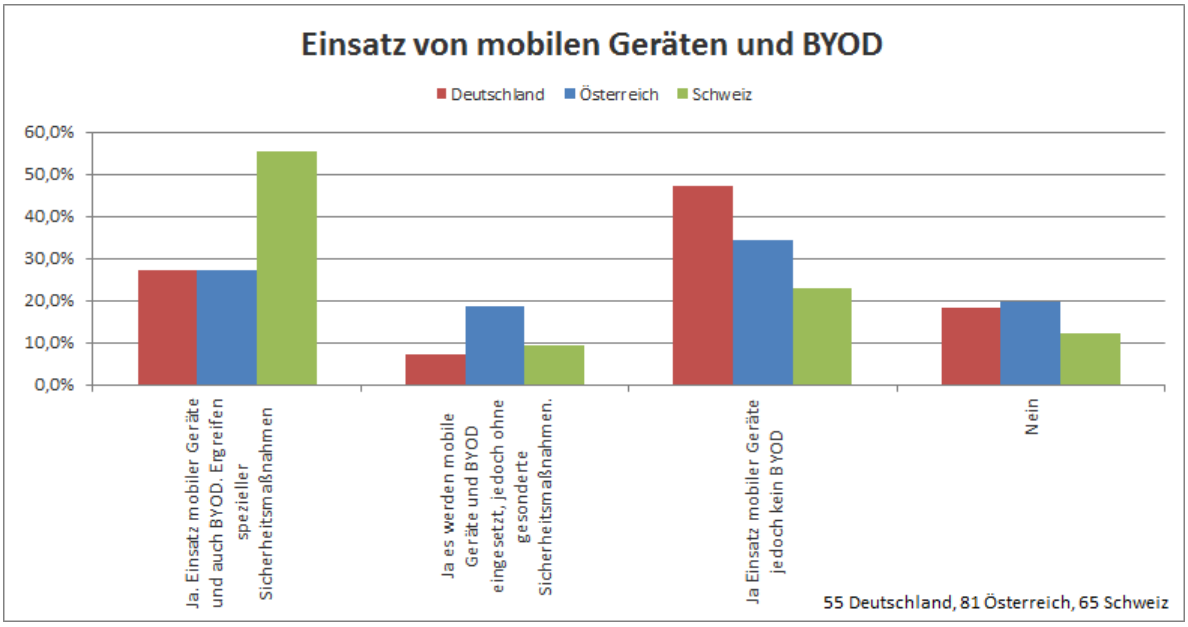

Abbildung 4.29.: Länderspezifisch: Einsatz von mobilen Geräten und BYOD

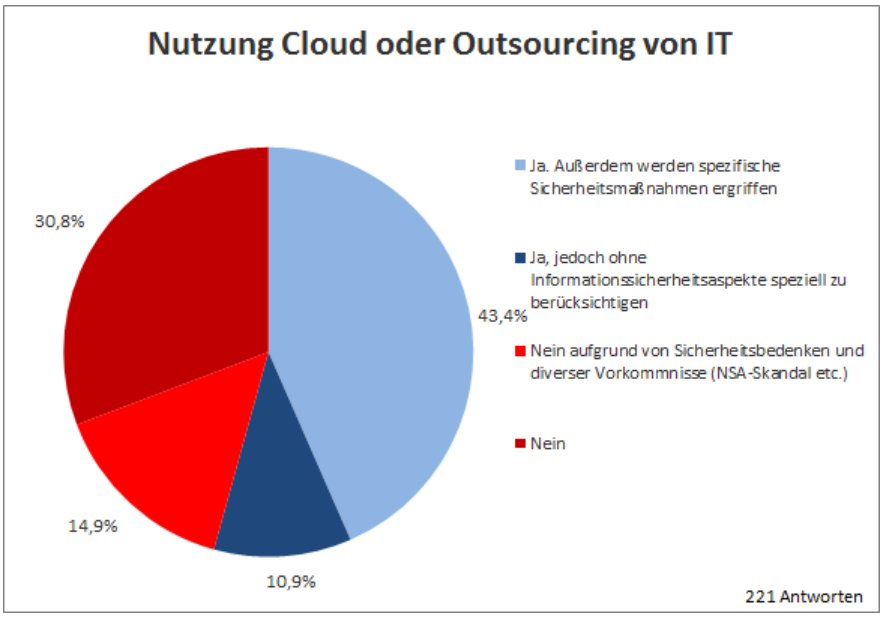

Abbildung 4.30.: Nutzung Cloud und/oder Outsourcing von IT

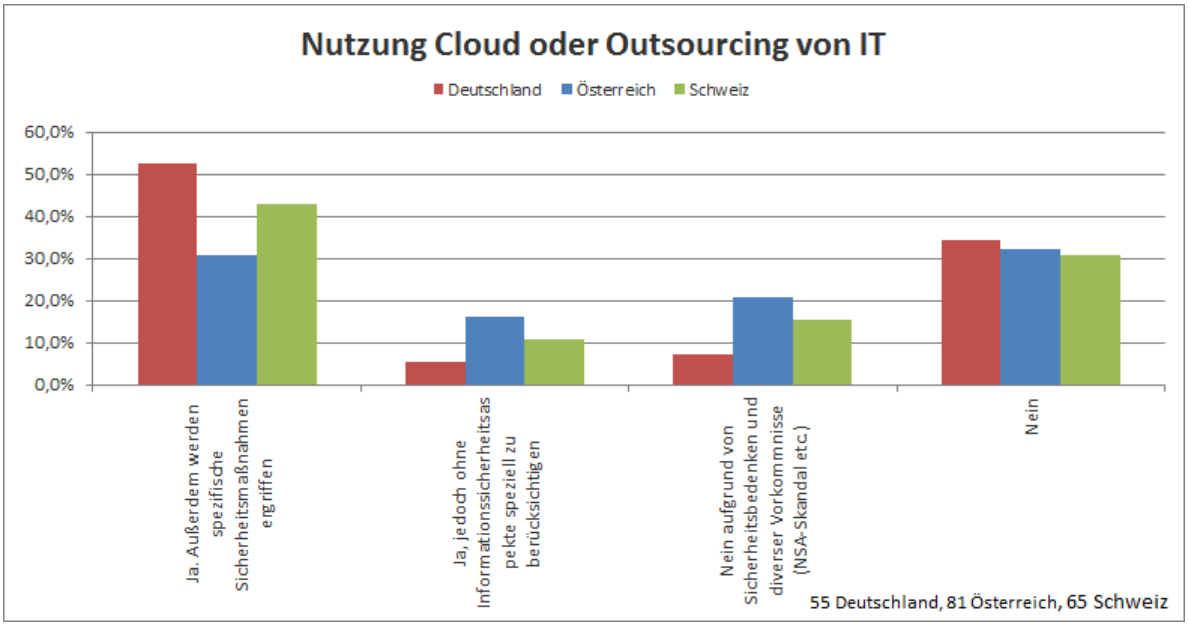

Abbildung 4.31.: Länderspezifisch: Nutzung Cloud und/oder Outsourcing von IT

von sehr hoher Wichtigkeit. Wie in Abbildung 4.32 zu sehen ist, gaben lediglich 16,8% der Unternehmen an, „keine Awareness-Aktivitäten“ durchzuführen. In den anderen Unternehmen waren „formale Vorgaben in diversen Dokumenten/Richtlinien“ (53,6%), „Intranet Portale“ (52,3%), sowie „Schulungen“ (53,6%) die häufigst genannten Aktivitäten. Auch „Newsletter und Infomaterial“ (38,2%), „Workshops“ (18,2%) und Kampagnen (30,5%) wurden von einigen Unternehmen genannt. Bei den sonstigen Aktivitäten wurden unter anderem auch „Web Bases Trainings“ bzw. „e-learning“ sowie „Video Clips“, „InfoSec Tage“ und Social Engineering Angriffe genannt.

Wie im Ländervergleich in Abbildung 4.33 zu sehen ist gibt es einige Unterschiede. So ist in Deutschland mit 11,2% der Anteil an Unternehmen, die keine Awareness-Aktivitäten durchführen etwas niedriger als in Österreich (23,5%) und der Schweiz (16,9%). Auch bei den meisten anderen Aktivitäten ist der Anteil der deutschen Unternehmen, die diese ausführen, meist höher als der der österreichischen oder Schweizer Firmen (insbesondere bei „formalen Vorgaben in diversen Dokumenten/Richtlinien“ und „Intranet Portalen“).

In Frage 9 (in Abbildung 4.20 und 4.21) gaben um die 90% der Unternehmen an, „Richtlinien & Vorgaben in Bezug zur Informationssicherheit“ zu besitzen. Es wäre daher interessant zu wissen, warum bei dieser Frage lediglich etwas mehr als 50% der Unternehmen angaben „formale Vorgaben in diversen Dokumenten/Richtlinien“ zu besitzen (eventuell weil hier explizit nach Awareness-Aktivitäten gefragt wurde und diese Vorgaben in einigen Unternehmen nicht dazu ausgelegt sind, Bewusstsein für die Bedeutung und Wichtigkeit der Informationssicherheit zu vermitteln).

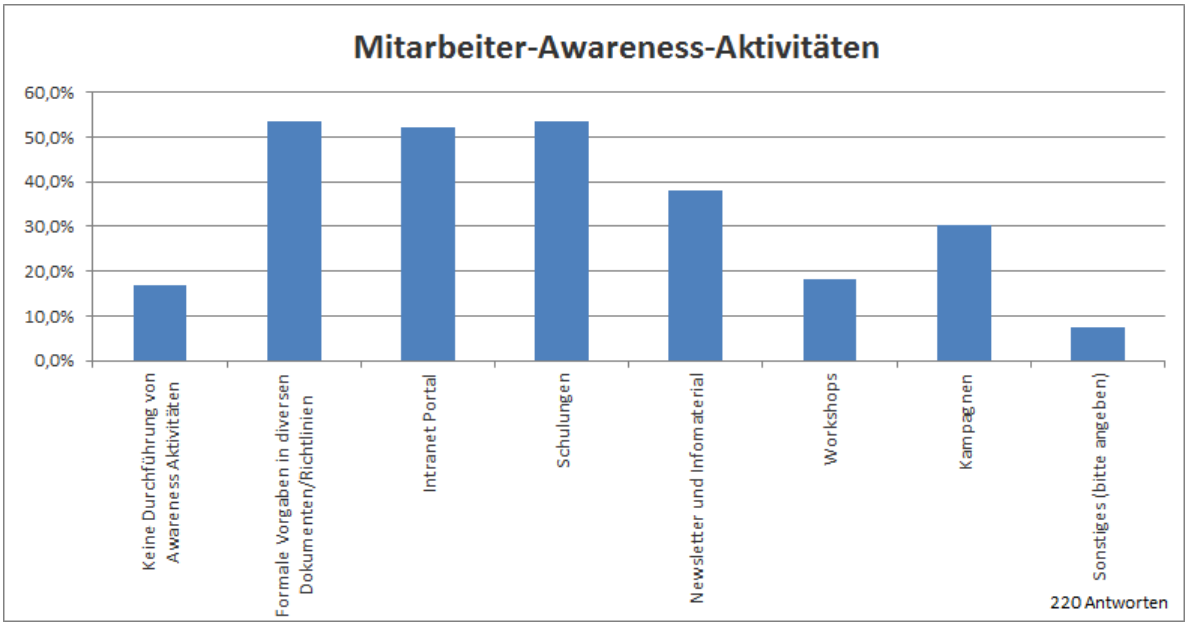

Abbildung 4.32.: Mitarbeiter-Awareness-Aktivitäten

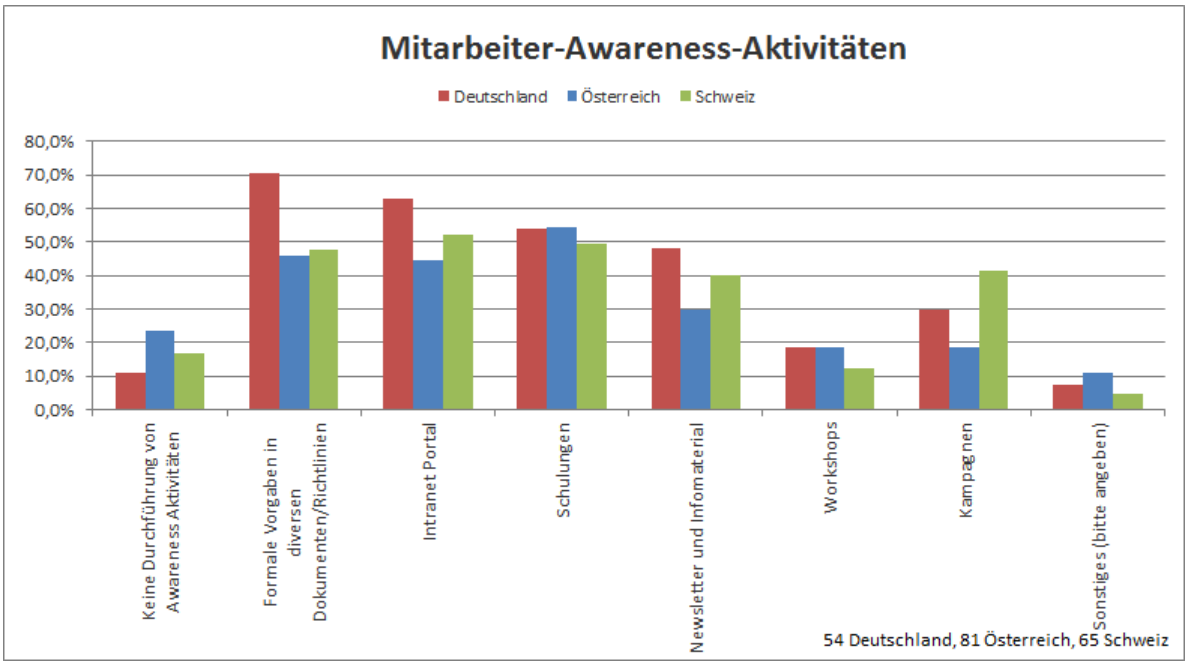

Abbildung 4.33.: Länderspezifisch: Mitarbeiter-Awareness-Aktivitäten

In Frage 16 werden Unternehmen bezüglich des Einsatzes von Open Source Software befragt und es wird erhoben, ob Unternehmen Maßnahmen treffen, um diese auf Fehlerfreiheit/Korrektheit und Qualität zu überprüfen. Die Ergebnisse in Abbildung 4.34 zeigen, dass lediglich 12,4% der Unternehmen angaben, „keine Open Source Software“ zu nutzen. Lediglich ein einziges Unternehmen (bei 217 Antworten) gab an „Open Source Software aufgrund von Sicherheitsbedenken nicht einzusetzen“. Die absolute Mehrheit von 58,1% der Unternehmen antworteten „Open Source Software einzusetzen, jedoch keine Überprüfung dieser durchzuführen“. Immerhin ein knappes Viertel (25,8%) nutzen Open Source Software und trafen dabei Maßnahmen wie „Durchführung von Code Reviews und Recherche zu Auditergebnissen, Sicherheitsanalysen und dem Entwicklerkreis“, um deren Sicherheit, Qualität und Vertrauenswürdigkeit zu überprüfen.

Im Ländervergleich in Abbildung 4.35 zeigen sich lediglich kleine Unterschiede. In der Schweiz ist mit 20,6% der Anteil an Unternehmen, welche keine Open Source Software nutzen, im Vergleich zu Österreich (8,6%) und Deutschland (12,7%) etwas höher. Der ungeprüfte Einsatz von Open Source Software war in allen Ländern beinahe gleich hoch (58,2% Deutschland, 61,7% Österreich, 55,6% Schweiz), während interessanterweise in Österreich 29,6% der Unternehmen angaben, Open Source Software gesondert zu überprüfen (im Vergleich zu 23,6% Deutschland und 19,0% Schweiz).

Generell ist zu dieser Frage anzumerken, dass die Zahl von 12,4% der Unternehmen, welche angaben „keine Open Source Software“ zu nutzen, relativ hoch scheinen kann, da gewisse Open Source Bibliotheken wie openssl oder verschiedene Browser und Addons eine sehr hohe Verbreitung haben und teilweise auch in kommerziellen Produkten genutzt werden. Auch ist mit einem Viertel die Anzahl der Unternehmen, welche Open Source Software nutzen und dabei Maßnahmen treffen um Sicherheit, Qualität und Vertrauenswürdigkeit zu überprüfen, relativ hoch. Es ist jedoch anzumerken, dass es sich bei „Durchführung von Code Reviews und Recherche zu Auditergebnissen, Sicherheitsanalysen und dem Entwicklerkreis“ nur um eine exemplarische Liste handelt und Unternehmen wahrscheinlich nicht immer alle Maßnahmen (insbesondere Code Reviews) durchführen. Es kann auch sein, dass Unternehmen nur recherchieren, ob die von ihnen eingesetzte Open Source Software unabhängig überprüft wurde (etwa durch das Coverity Scan Projekt oder unabhängige Audits) und sonstige Berichte und Informationen verfügbar sind. Nichtsdestotrotz sprechen die Antworten dieses knappe Viertels der Unternehmen für ein Bewusstsein hinsichtlich der potentiell mit dem Einsatz von Open Source Software verbundenen Problematiken.

Bei der Frage nach der Betroffenheit der Unternehmen von schwerwiegenden Sicherheitslücken in Open Source Software wie Heartbleed und Shellshock gaben, wie in Abbildung 4.36 ersichtlich, 59,4% an, dass sie von diesen Lücken betroffen gewesen waren, jedoch ohne dass es zu einer „Beeinträchtigung

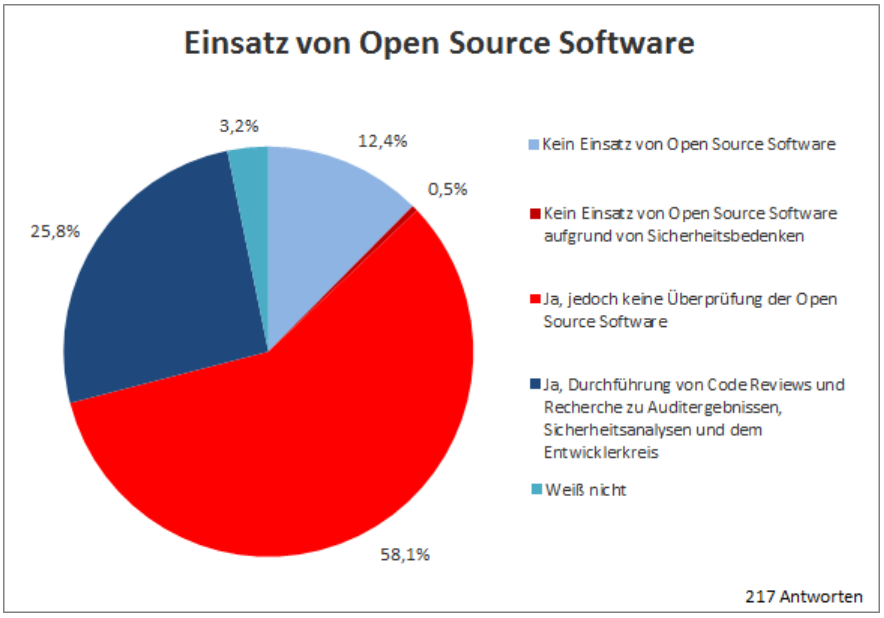

Abbildung 4.34.: Einsatz von Open Source Software

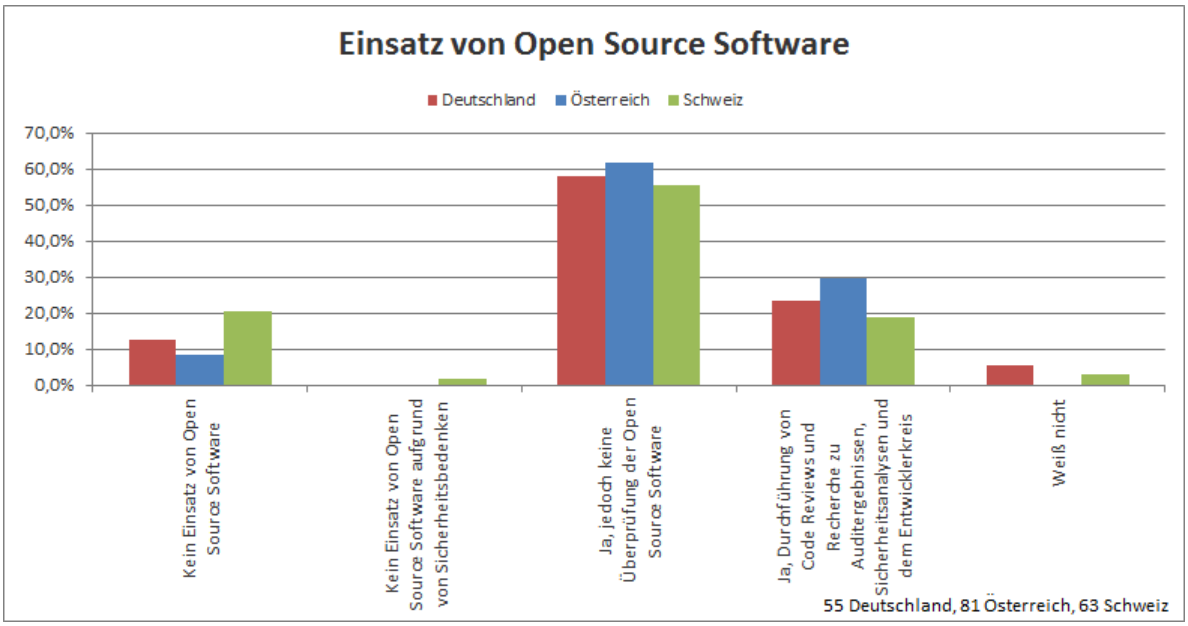

Abbildung 4.35.: Länderspezifisch: Einsatz von Open Source Software

der Geschäftstätigkeiten“ gekommen wäre (etwa durch Nichtverfügbarkeit wichtiger Dienste und außerplanmäßige Wartungsfenster für die Einspielung notwendiger NotfallPatches). 4,6% der Unternehmen gaben an, dass sie von den Lücken betroffen waren, wobei auch die „Geschäftstätigkeit beeinträchtigt wurde“. Abermals antwortete lediglich ein einziges Unternehmen (bei 217 Antworten), dass bei ihm „diese Lücken aktiv für Angriffe auf das Unternehmen ausgenutzt wurden“. Bei 29,0% stellten diese Lücken kein Problem dar und 6,5% der Teilnehmerinnen und Teilnehmern wussten nicht, ob sie betroffen gewesen waren.

Beim Vergleich der Antworten der verschiedenen Länder in Abbildung 4.37 zeigt sich eigentlich ein relativ einheitliches Bild. Lediglich auffallend ist, dass in Österreich nur 22,5% der Unternehmen angab, nicht von diesen Lücken betroffen gewesen zu sein, während diese in der Schweiz und Deutschland 32,8% bzw. 32,7% antworteten. Außerdem ist in Österreich die Anzahl der „weiß nicht“ Antworten mit 8,8% etwas höher (1,8% Deutschland 4,7% Schweiz). Die Betroffenheit von den Lücken ohne (60,0% Deutschland, 62,5% Österreich, 57,8% Schweiz) und mit Beeinträchtigung der Geschäftstätigkeiten (5,5% Deutschland, 6,3% Österreich, 3,1% Schweiz) waren in allen drei Ländern ähnlich hoch.

Allgemein muss bei dieser Frage jedoch berücksichtigt werden, dass eine tatsächliche Ausnutzung dieser Lücken (insbesondere Heartbleed) nur schwer bzw. kaum nachweisbar war, wodurch natürlich die Möglichkeit besteht, dass stattgefundene Angriffe von den Unternehmen gar nicht bemerkt wurden.

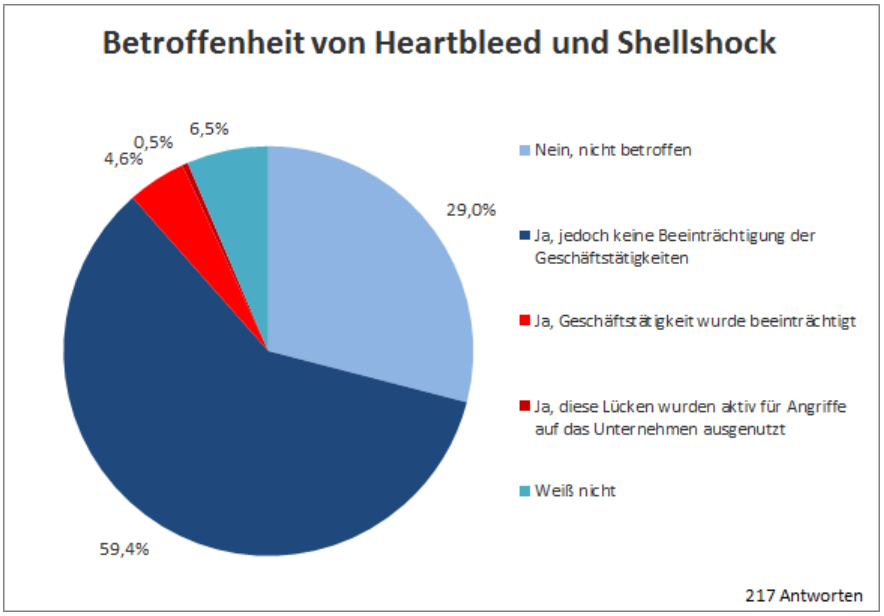

Abbildung 4.36.: Betroffenheit von Heartbleed und Shellshock

Bei Frage 18, welche sich mit dem Thema APTs beschäftigt, erklärten - wie in Abbildung 4.38 ersichtlich - mit 56,5% knapp mehr als der Hälfte der Unternehmen, dass sie „im letzten Jahr nicht Ziel eines komplexen, fortgeschrittenen, direkt auf sie gezielten IT-Angriffs (APT-Advanced Persistent Threat)“ waren.

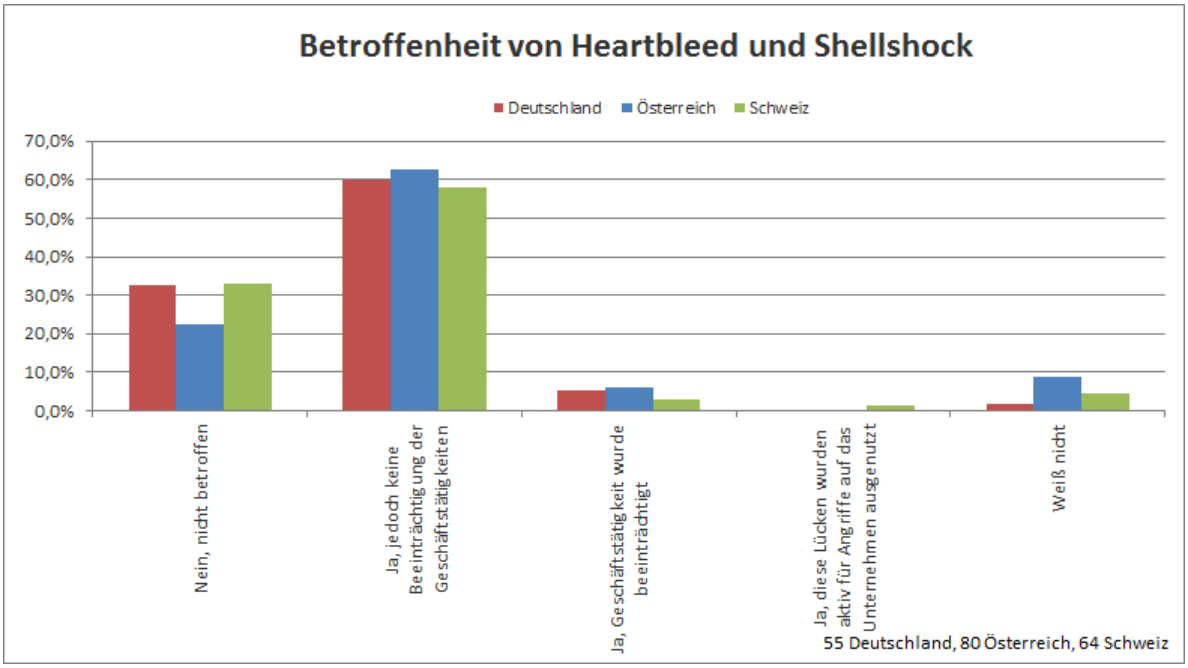

Abbildung 4.37.: Länderspezifisch: Betroffenheit von Heartbleed und Shellshock

9,3% gaben an, dass sie im vergangenen Jahr zwar „Ziel eines APTs waren, dieser jedoch erfolgreich abgewehrt werden konnte und keinen Schaden anrichtete“, während weitere 2,8% der Unternehmen angaben, dass sie im letzten Jahr „Ziel eines APTs gewesen waren und dieser auch Schaden anrichtete“. Mit 25,9% konnte knapp ein Viertel der Unternehmen auf diese Frage nur mit „weiß nicht“ antworten, während bei 5,6% zumindest ein Verdacht bezüglich des Auftretens eines APTs bestand.

Dies bedeutet, dass bei knapp einem Drittel der Unternehmen Unsicherheit bzw. Unwissenheit bezüglich des Auftretens eines APT besteht (25,9% „weiß nicht“ + 5,6% „Verdacht“), was natürlich auch der Tatsache geschuldet ist, dass APTs schon ihrer Definition nach komplex und schwer zu identifizieren bzw. nachzuweisen sind.

Im Ländervergleich in Abbildung 4.39 zeigen sich lediglich kleine Unterschiede. In Deutschland konnten mit 53,7% etwas weniger Unternehmen ausschließen „von einem APT betroffen gewesen zu sein“, als dies in der Schweiz und Österreich mit 59,4% bzw 59,5% der Fall war. Dafür war in Deutschland auch die Anzahl an „weiß nicht“ Antworten mit 31,5% am höchsten (24,1% Österreich, 23,4% Schweiz). Weiters auffallend ist, dass in der Schweiz 6,3% der Unternehmen angaben, von einem „APT betroffen gewesen zu sein, der Schaden anrichtete“, während dies in Deutschland und Österreich jeweils nur ein einziges Unternehmen antwortete. Auch auffallend ist, dass Österreich sowohl bei dem „Verdacht bezüglich des Auftretens“ und auch bei der „erfolgreichen Abwehr“ von APTs im Ländervergleich jeweils die höchsten Nennungen hat (wenn auch der Unterschied nur sehr gering ist).

Bei dem Vergleich dieser Ergebnissen mit den Antworten auf Frage 12 (Abbildung 4.26 und 4.27) fällt auf, dass bei der Frage nach Vorfällen insgesamt lediglich 5,5% angaben, von „einem APT betroffen gewesen zu sein“. Dies sind weniger als die ungefähr laut dieser Frage 12% betroffenen Unternehmen (9,3% + 2,8%). Eventuell erklärt sich dieser Unterschied dadurch, dass einige der Unternehmen, welche in dieser Frage angaben den APT erfolgreich abgewehrt zu haben, ihn nicht in Frage 12 bei den Vorfällen erwähnten (hier sollte eventuell der Begriff Vorfall dahingehend näher definiert werden, dass dieser nicht unbedingt Schaden verursachen muss).

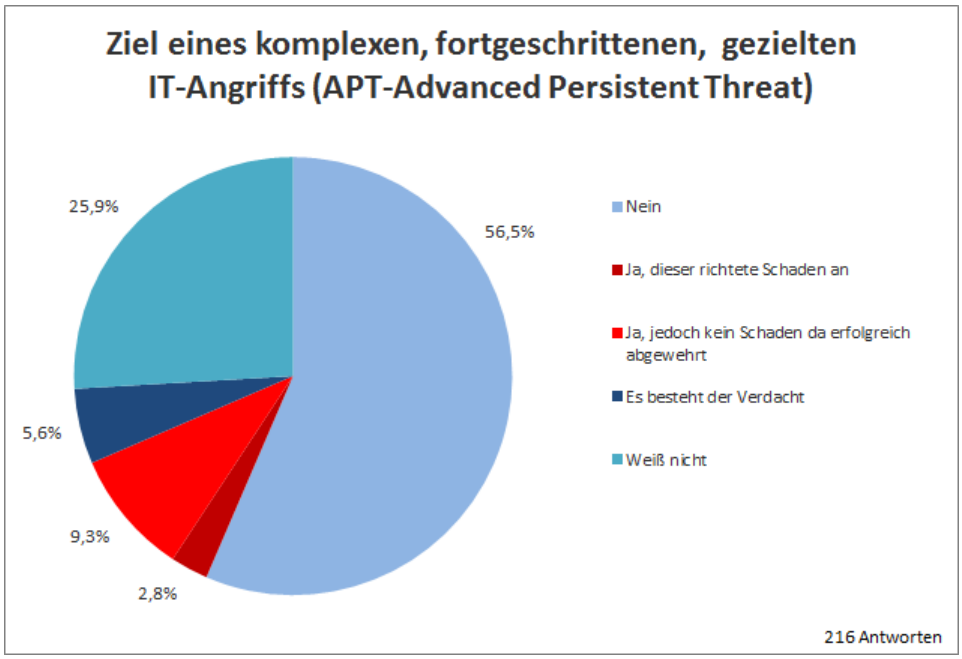

Abbildung 4.38.: Ziel eines komplexen, fortgeschrittenen, gezielten IT-Angriffs - APT

Die Antworten bezüglich der Bedeutung der NSA-Enthüllungen für Unternehmen werden in Abbildung 4.40 dargestellt. 39,1% antworteten, dass „die NSA-Enthüllungen bezüglich Überwachung und Spionage sowie der gezielten Manipulation von (amerikanischen) Soft- und Hardware-Produkten für ihr Unternehmen kein Thema“ waren. Fast ein genauso großer Teil von 36,7% der Unternehmen gaben an, dass diese Entwicklungen „für sie ein Thema waren“ und zu einer „wachsende Beachtung des Themas der Informationssicherheit“ geführt haben, während 17,2% angaben, dass dies „zwar ein Thema war, jedoch keine gezielten Maßnahmen ergriffen wurden“. Bezüglich Maßnahmen werden der „verstärkter Einsatz von Verschlüsselung“ (16,7%), „Achtsamkeit, im Fall von Cloud oder Outsourcing wird verstärkt auf heimische/europäische Anbieter gesetzt“ (16,3%) sowie die „Planung zur verstärkten Beschaffung von IT Made in Austria/Germany/Switzerland bzw. Europe“ (9,3%) genannt. Eine auf diese Enthüllungen folgende „Erhöhung des IT-Sicherheitsbudgets“ wurde von lediglich 1,9% der Unternehmen genannt.

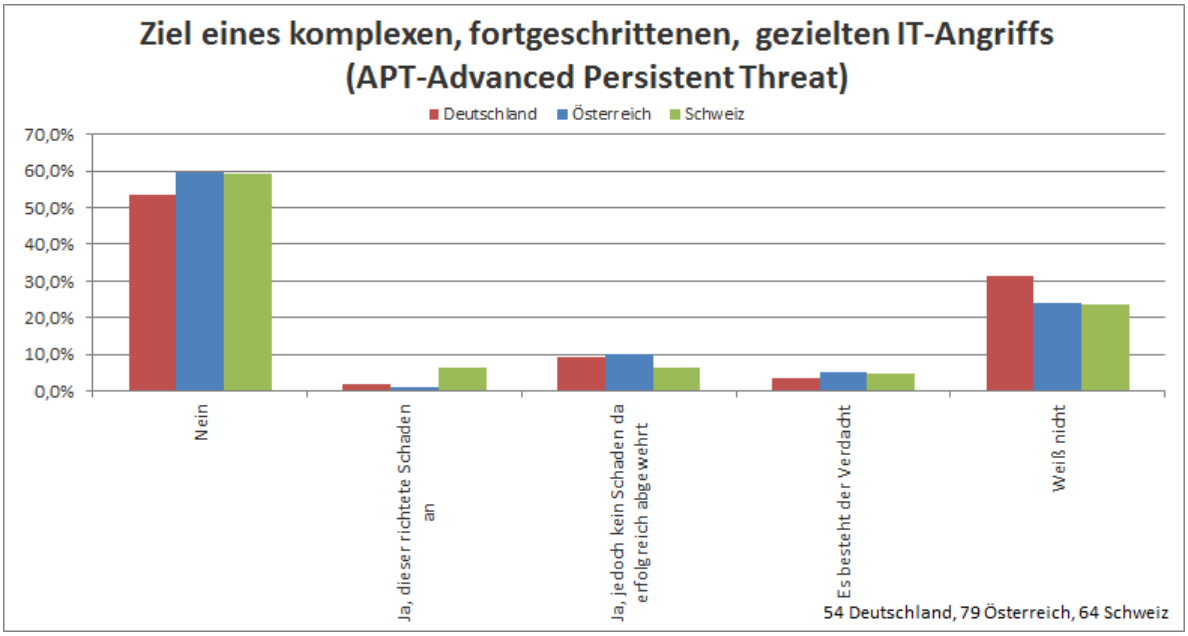

Abbildung 4.39.: Länderspezifisch: Ziel eines komplexen, fortgeschrittenen, gezielten IT-Angriffs -APT

Wie im Ländervergleich in Abbildung 4.41 zu sehen ist, gibt es einige Unterschiede. In Deutschland ist mit 46,3% der Anteil an Unternehmen, für die die NSA-Enthüllungen kein Thema waren am höchsten (im Vergleich zu 41,8% Österreich und 36,5% Schweiz). In der Schweiz gaben mit 28,6% relativ viele Unternehmen an, dass diese „Entwicklungen für sie ein Thema seien, jedoch ohne, dass sie gezielte Maßnahmen ergriffen haben“ (11,1% Deutschland, 11,4% Österreich). Eine auf diese Enthüllungen folgende „wachsende Beachtung des Themas der Informationssicherheit“ gaben in allen drei Ländern ungefähr gleich viele an (38,9% Deutschland, 35,4% Österreich, 31,7% Schweiz). Lediglich leichte Schwankungen gab es auch bei den Maßnahmen „verstärkter Einsatz von Verschlüsselung“ (13,0% Deutschland, 20,3% Österreich, 11,1% Schweiz), „Achtsamkeit, im Fall von Cloud oder Outsourcing wird verstärkt auf heimische/europäische Anbieter gesetzt“ (22,2% Deutschland, 11,4% Österreich, 15,9% Schweiz) sowie bei der „Planung zur verstärkten Beschaffung von IT Made in Austria/Germany/Switzerland bzw. Europe“ (9,3% Deutschland, 10,1% Österreich, 7,9% Schweiz).

Es fällt auf, dass Österreich bei dem „verstärkten Einsatz von Verschlüsselung“ mit 20% (im Vergleich zu 13,0% Deutschland und 11,1% Schweiz) leicht hervorsticht. Eine mögliche Erklärung ist, dass das Briefgeheimnis in Österreich einen relativ hohen Stellenwert genießt. Außerdem könnte es sein, dass viele der größeren Teilnehmer in Deutschland und der Schweiz sich bereits mit diesem Thema auseinandergesetzt haben und aufgrund diverser Schwierigkeiten (Aufwand, Komplexität, Schlüsselverwaltung, Performance etc.) und Akzeptanz-Problemen (End User, Partner etc.) der Verschlüsselung schon etwas desillusioniert gegenüberstehen.

Generell fällt in dieser Frage auf, dass sich trotz der umfassenden medialen Berichterstattung sehr viele Unternehmen dem Thema gegenüber „passiv“ verhalten (knapp unter 60% der Unternehmen gaben entweder an, das Thema nicht zu beachten oder keine gesonderten Maßnahmen daraus abzuleiten). Auch bei den 36,7% der Unternehmen bei denen es durch die NSA-Enthüllungen zu einer „wachsende Beachtung des Themas der Informationssicherheit“ kam muss hinterfragt werden, inwiefern nun zusätzliche Sicherheitsmaßnahmen umgesetzt werden. Eine auf die NSA-Enthüllung folgende Umsetzung spezifischer Maßnahmen wurde jeweils nur von einer Minderheit (2%-16%) der Befragten genannt.
Bezüglich sonstiger getroffenen Maßnahmen wurden unter anderem auch eine „vertiefte Prüfung von Software und Hardware“, „ein Haltung aller Daten so lokal wie möglich“, „Verbot von AES und elliptischen Kurven in Hochsicherheitsbereichen“, „NoSpy-Klauseln in Verträgen“ sowie der „Austausch von RSA-Dongles gegen einen europäischen Hersteller“ genannt.

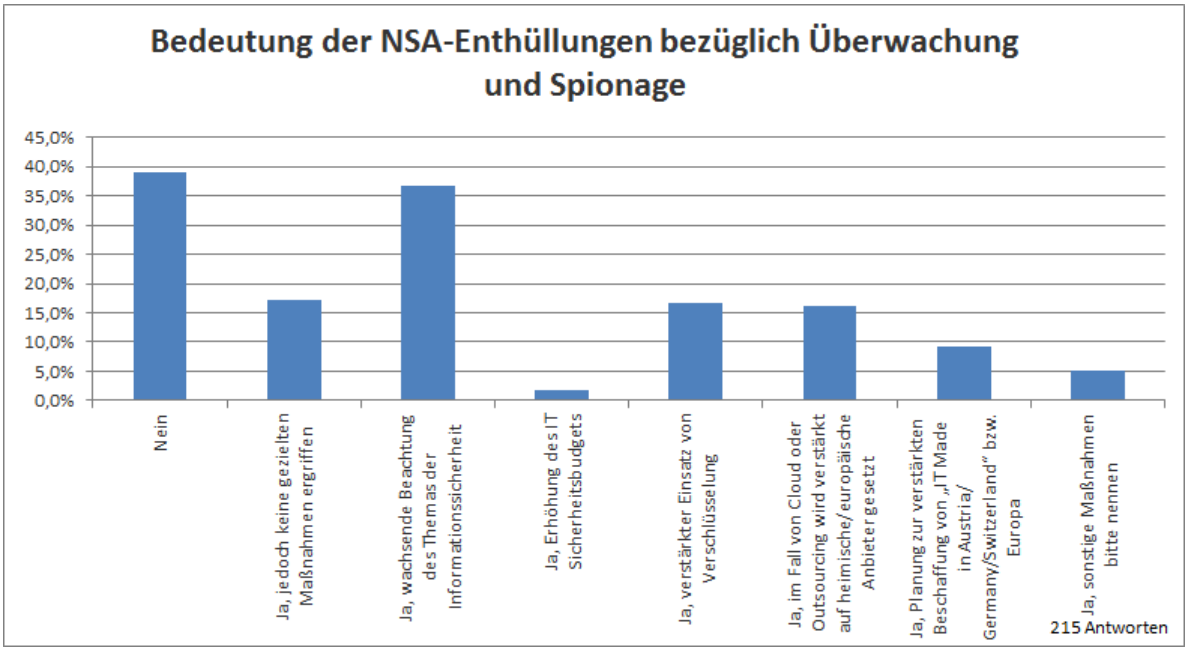

Abbildung 4.40.: Bedeutung der NSA-Enthüllungen bezüglich Überwachung und Spionage

4.2.5. Technische und organisatorische Aufstellung der Unternehmen

Die technische und organisatorische Aufstellung der Unternehmen wurde über zwei große Matrix Fragen ermittelt. In der folgenden Auswertung wurden bewusst absoluten Zahlen und keine Prozentwerte verwendet. Auf Prozentwerte wurde verzichtet, da wieder alle Beantwortungen (auch je einzelner Maßnahme) optional waren und nicht mit Sicherheit gesagt werden kann, ob bei Maßnahmen, die weniger absolute Beantwortungen bekommen haben, dies etwa darauf zurückzuführen ist, dass sie gar nicht bekannt bzw. beachtet sind und die „fehlenden“ Beantwortungen somit eigentlich als „nicht vorhanden“

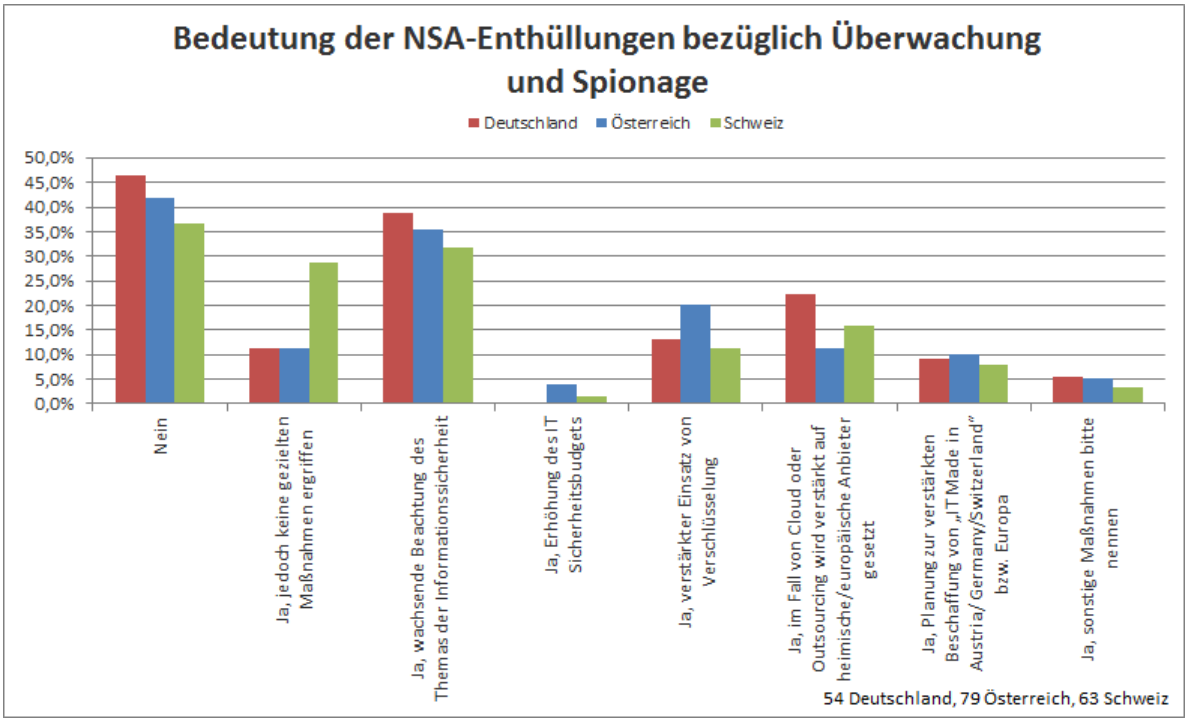

Abbildung 4.41.: Länderspezifisch: Bedeutung der NSA-Enthüllungen bezüglich Überwachung und Spionage

gewertet hätten werden müssen. Um eine Verfälschung der Ergebnisse zu vermeiden, beziehen sich die folgenden Abbildungen daher auf die absoluten Zahlen. Die vollständigen Ergebnistabelle (sowie die Ergebnistabellen für Deutschland, Österreich und die Schweiz) sind in der Tabelle A.23 und der Tabelle A.27 im Anhang A.3 ersichtlich.

Technische Aufstellung

Im Hinblick auf technische Maßnahmen, die in Frage 20 erhoben wurden und deren Gesamtüberblick (nicht länderspezifisch) in Abbildung 4.42 dargestellt ist, ergibt sich ein relativ übersichtliches und klares Bild, in dem verschieden Gruppen von Maßnahmen (Maßnahmen mit unterschiedlich hohem Implementierungsgrad) gut erkennbar sind.

Es stechen einige Tools bzw. Systeme sofort hervor, da diese durchgängig bzw. von fast allen Unternehmen eingesetzt werden. Zu diesen zählen „Firewall(s)“, „Virenschutz/Malware Scanner“, „Backupsoftware“, „Spamschutz“, „E-Mail Malware Scans“ und „VPNs“. Weiters werden auch die Themen „Client Sicherheit“, „Netzwerk Segmentierung“, „Verschlüsselungstechnologien“, „Monitoring Software“, sowie „Patch Management Software“ von einem Großteil der Unternehmen als implementiert genannt.

Die nun aufgezählten Systeme werden in Reihenfolge ihrer Aufzählung von immer weniger Unternehmen als „Implementiert“ angegeben. Während einige Maßnahmen wie „Web Content Inspection/-

Filtering/ Monitoring“, „Layer 2 Netzwerksicherheit“, „Zwei Faktor Authentifizierung“, „OS und Server Hardening“ und „PKI - Public Key Infrastruktur“ noch einigermaßen oft genannt wurden, werden die Nennungen von „IDS/IPS“, „E-Mail Verschlüsselung & Signatur“, „Web Application Firewalls“, „Mobile Device Management Software“, „Log Management Software“ und „Vulnerability Mgmt. Tools“ schnell weniger.

„MSSP - Managed Security Service Provider“, „DLP“, „SIEM Systeme“, „(Security) Configuration Management Software“ und „DDOS Protection“ werden nur von wenigen Unternehmen als „implementiert“ angesehen und sind bei einem großen Teil der Befragten nicht vorhanden. Außerdem fällt auf, dass hier auch insgesamt die wenigsten Antworten abgegeben wurden, was bedeuten könnte, dass die Anzahl an „nicht vorhanden“-Antworten eventuell noch höher sein müsste (es kann sein, dass Unternehmen, die diese Systeme nicht kannten, einfach diese Kategorie übersprungen und nicht als „nicht vorhanden“ bewertet haben).

Systeme, zu denen häufig angegeben wurde, dass deren Implementierung in Planung oder in Zukunft vorgesehen ist, sind unter anderem „SIEM Systeme“, „Log Management Software“, „E-Mail Verschlüsselung & Signatur“, „Mobile Device Management Software“, „IDS/IPS“, „Vulnerability Mgmt. Tools“ sowie das Thema „DLP“.

Zusammenfassend ist zu der technischen Aufstellung der Unternehmen zu sagen, dass grundlegende wichtige Sicherheitstools (wie Firewalls, Virenschutz, Backupsoftware, Spamschutz) beinahe durchgängig vorhanden sind, wobei sich aber in Bezug auf weiterreichende oder speziellere Maßnahmen ein gespaltenes Bild mit teilweise schnell sinkendem Implementierungsgrad zeigt. Hier wird der Implementierungsgrad in Unternehmen von Faktoren wie der Unternehmensgröße sowie dem allgemeinen Bewusstsein für und den Stellenwert der Informationssicherheit abhängig sein. Einige technisch komplexe und aufwändige Maßnahmen (wie DLP, SIEM oder auch (Security) Configuration Management Software) sind nur bei einer Minderheit der Befragten im Einsatz.

In den Abbildungen 4.43, 4.44 und 4.45 befinden sich die länderspezifischen Auswertungen für Deutschland, Österreich und die Schweiz. Aufgrund der Vielzahl an angeführten Systemen wird von einer detaillierten Vergleich des Implementierungsgrades einzelner Systeme in den verschiedenen Ländern Abstand genommen (Für einen Vergleich können auch die Tabellen A.20, A.21, A.22 im Anhang gut genutzt werden). Bei einem groben Vergleich der Abbildungen fällt jedoch auf, dass in der Schweiz tendenziell am wenigsten rote Flächen (entspricht nicht implementierte Maßnahmen) sichtbar sind, während Deutschland etwas mehr und Österreich den größten Anteil solcher Maßnahmen aufweist.

Diese Feststellung trifft jedoch hauptsächlich für die technisch „fortgeschritteneren“ Systeme zu, da sich bei grundlegenden wichtigen Sicherheitstools (wie Firewalls, Virenschutz, Backupsoftware, Spam-

schutz) über alle Länder hinweg ein einheitlich sehr hoher Implementierungsgrad zeigt. Diese Unterschiede könne jedoch auch teilweise darauf zurückzuführen sein, dass in Österreich im Vergleich zu Deutschland und Schweiz relativ viele kleine Unternehmen an der Umfrage teilnahmen, während in der Schweiz sehr viele Unternehmen mit mehr als 1000 Angestellten antworteten.
Es soll hier jedoch deutlich auf die Einschränkung hingewiesen werden, dass die einfache Frage, ob eine Maßnahme „implementiert“, „in Planung“ oder „nicht vorhanden“ ist, eine sehr grobe und oberflächliche Behandlung des Themas der technischen Aufstellung der Unternehmen darstellt. Die tatsächliche Qualität bzw. der Reifegrad der implementierten Maßnahmen kann nämlich stark schwanken und sehr unterschiedlich sein. Beispiele hierfür sind etwa eine einzelne Firewall gegen ein mehrstufiges Firewall-Konzept mit DMZ oder Virenschutz lediglich auf Clients (im Worst Case nicht aktuell und ohne automatisch aktualisierte Signaturen) im Gegensatz zu auf allen Systemen des Unternehmens ausgerollter und zentral verwalteter (mehrstufiger bzw. multi Engine) Virenschutzsoftware die Maßnahmen zum Umgang mit privaten Geräten inkludiert.

Organisatorische Aufstellung

Im Hinblick auf organisatorische Maßnahmen, die in Frage 21 erhoben wurden und deren Gesamtüberblick (nicht länderspezifisch) in Abbildung 4.46 dargestellt ist, ergibt sich ein nicht so ganz eindeutiges Bild wie bei den technischen Maßnahmen, wo schnell Gruppen von Maßnahmen mit verschieden hohen Implementierungsgraden erkennbar waren. Es scheint so, als ob sich hier ein etwas homogeneres Bild zeigt und der Grad der Umsetzungen/Nicht Umsetzungen verschiedener Maßnahmen nicht so stark schwankt wie bei den technischen Maßnahmen.
Nichtsdestotrotz gibt es, wie bei den technischen Maßnahmen auch im organisatorischen Bereich zwei Maßnahmen, welche fast durchgängig umgesetzt sind, nämlich „Spam & Antivirus“ sowie „Backup und Wiederherstellung“. Fast bei jeder anderen Maßnahme gibt es auch Beantwortungen, dass diese „in Planung“ oder „nicht vorhanden“ ist. Abgesehen von den zwei sehr stark verbreiteten Maßnahmen gibt es nicht viele Themen, die (hinsichtlich ihrer Verbreitung) so eindeutig wie einige technische Systeme hervorstechen.
Weitere organisatorische Maßnahmen, welche verbreitet genannt wurden sind „Physische Sicherheit", „Patch & Update Management“, „Medien-/Datenvernichtung“, „Dokumentation“, „Change Management“, „Identitäts- und Zugriffsmanagement“, „Logging & (Performance) Monitoring“, „Risikomanagement“ sowie die Durchführung von „Audits/ Penetration Tests und Vulnerability Scans“. Obwohl diese Maßnahmen relativ verbreitet genannt wurden, gibt es auch hier schon einige Unternehmen, die mit „in Planung“ oder „nicht vorhanden“ antworteten.

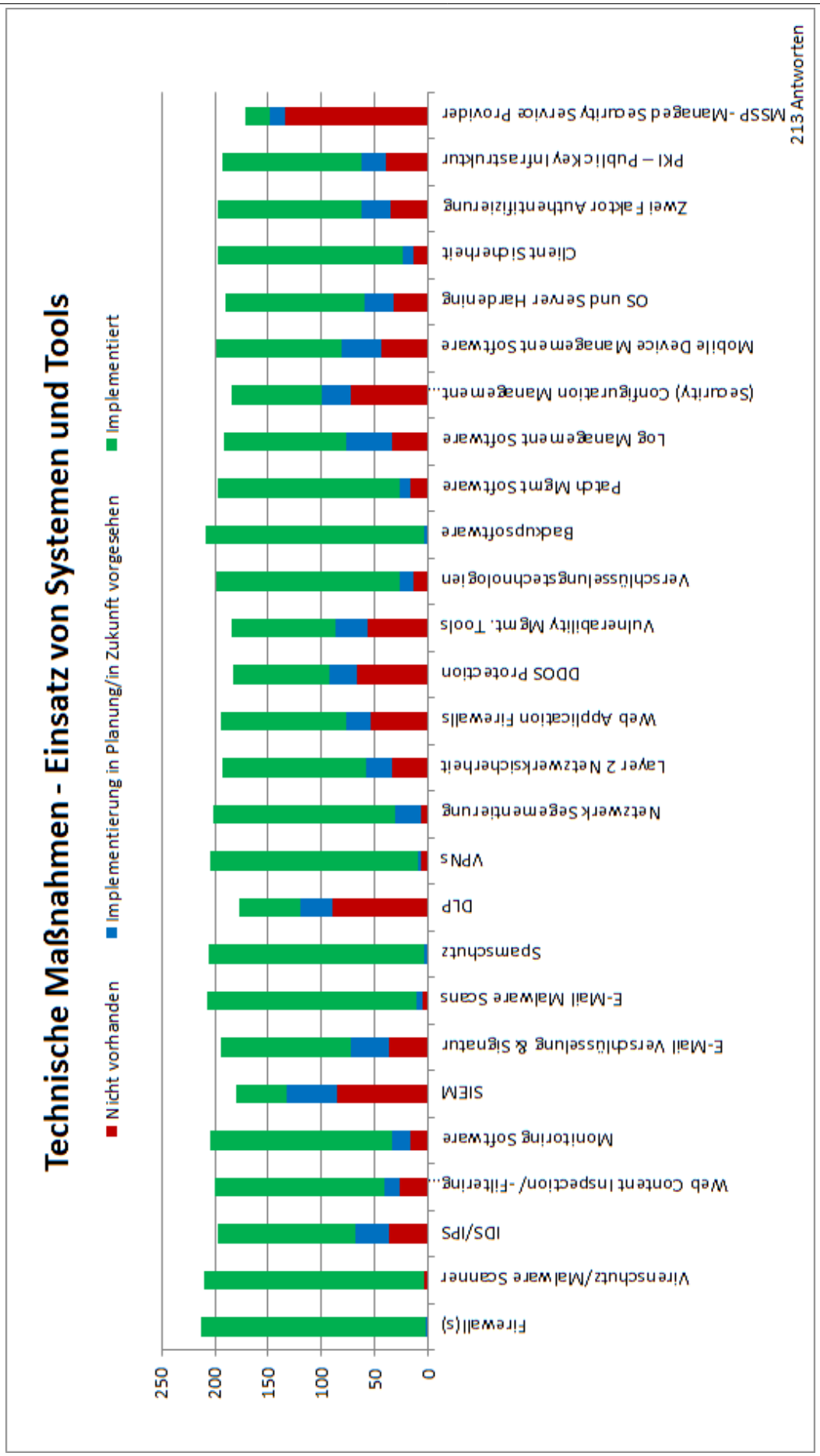

Abbildung 4.42.: Technische Maßnahmen - Einsatz technischer Systeme und Tools - Gesamt

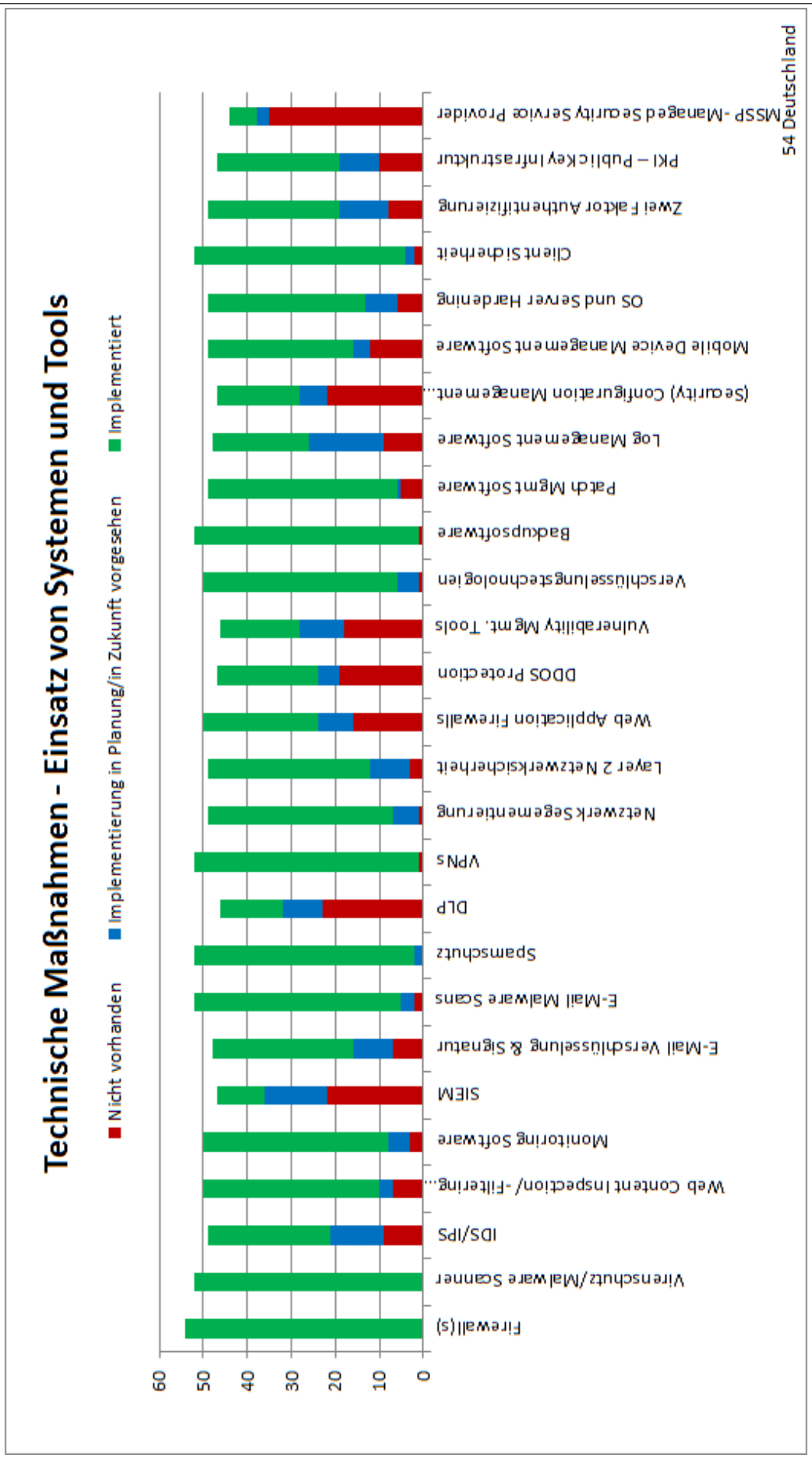

Abbildung 4.43.: Technische Maßnahmen - Einsatz technischer Systeme und Tools - Deutschland

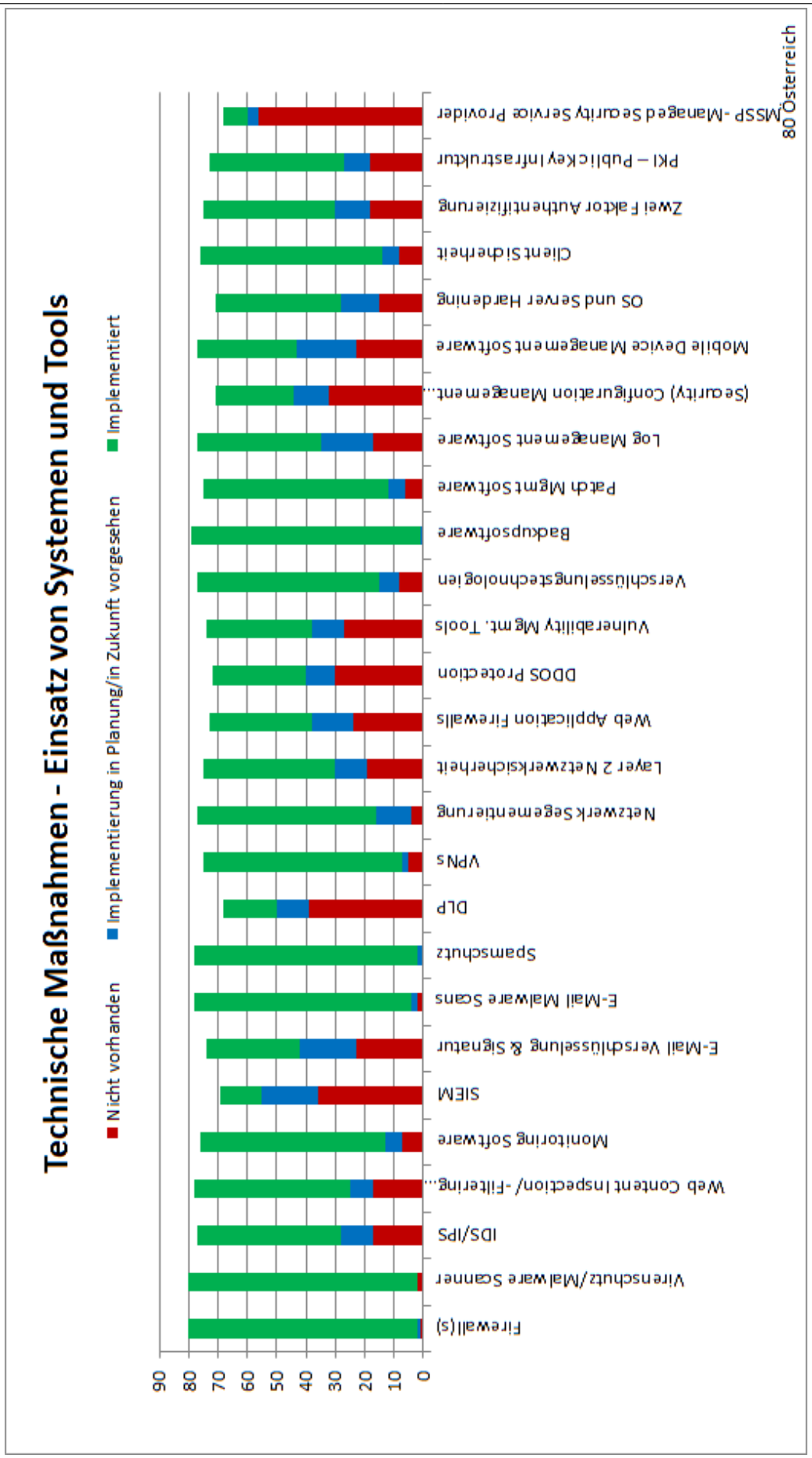

Abbildung 4.44.: Technische Maßnahmen - Einsatz technischer Systeme und Tools - Österreich

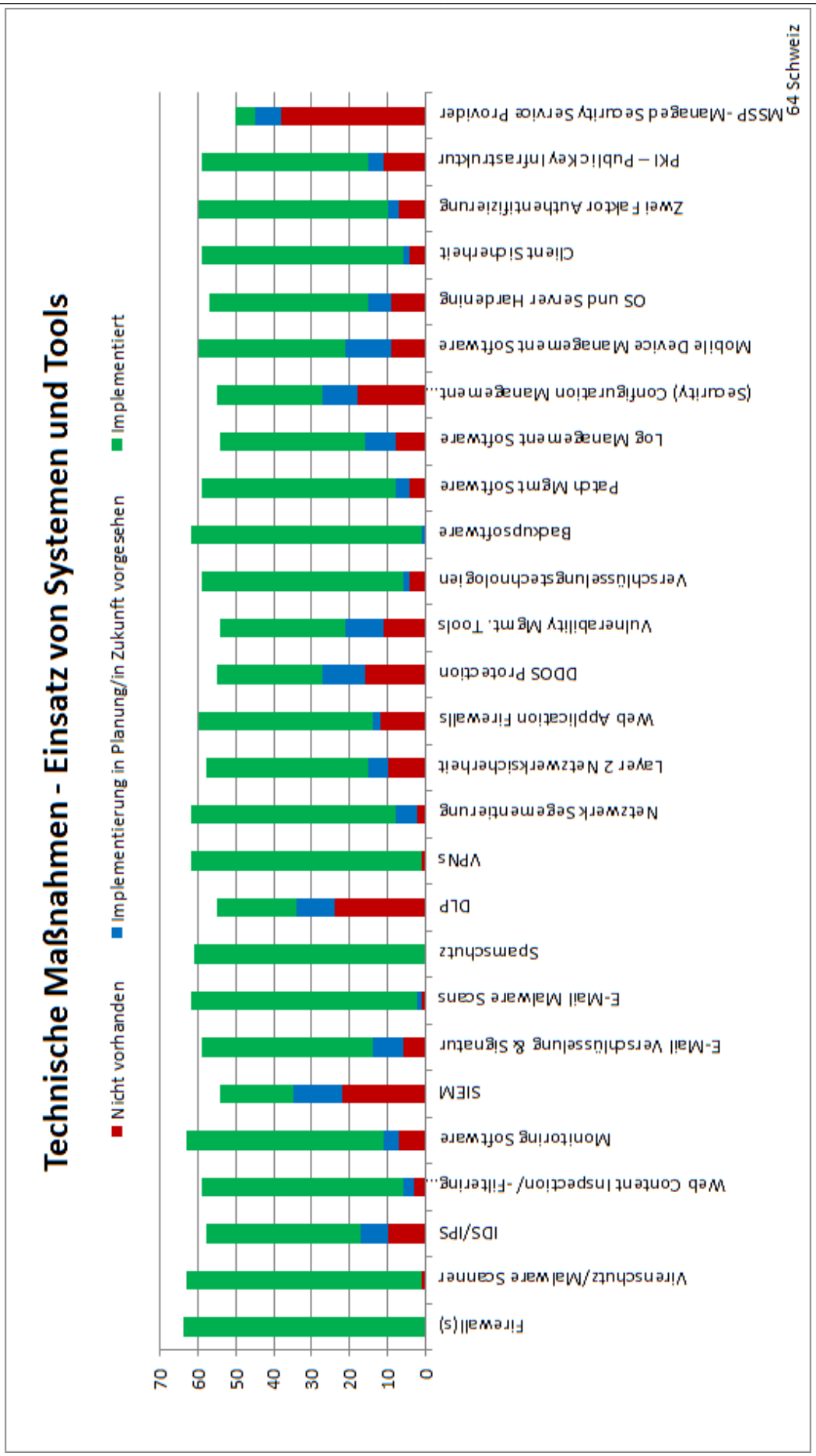

Abbildung 4.45.: Technische Maßnahmen - Einsatz technischer Systeme und Tools - Schweiz

Die organisatorische Maßnahmen „Asset Management“, „Awareness Aktivitäten“, „Configuration/ Capacity Management“, „Management der Leistungserbringung/Verträge Externe IT Dienstleister“, „Personal Management“, „BCM und BIA/ Notfallplanung/-vorsorge“, „Vulnerability Management“, „Vorfallmanagement“, „Betrieb eines ISMS“ sowie „Informationsklassifikation und -Verarbeitung“ weisen in Reihenfolge dieser Aufzählung eine fallenden Implementierungsgrad auf.
Am wenigsten verbreitet waren Maßnahmen wie „sichere Software-/Webapplikationsentwicklung“, „Betrieb eines IKS inklusive IT-Kontrollen“, „Firmeneigenes CERT“, „Durchführung/Teilnahme an Cyber-Übungen“ und die „Versicherung gegen Cyber/IT-Angriffe“.
Im Vergleich zu den technischen Maßnahmen wurde die Option „Implementierung in Planung/In Zukunft vorgesehen“ etwas öfter genutzt (hier wäre eine vertiefende Untersuchung interessant, ob diese Tatsache darauf zurückzuführen ist, dass die meisten Unternehmen bereits technisch besser aufgestellt sind als dies organisatorisch der Fall ist und daher nun verstärkt der organisatorische Bereich im Fokus liegt). Besonders oft wurden die Themen „Sichere Software-/Webapplikationsentwicklung“, „Betrieb eines ISMS“, „Informationsklassifikation und -Verarbeitung“, „BCM und BIA/ Notfallplanung/-vorsorge“, „Vorfallmanagement“, „Logging & (Performance) Monitoring“ sowie „Vulnerability Management“ genannt. Auch „Awareness Aktivitäten“, „Betrieb eines IKS inklusive IT-Kontrollen“, „Durchführung/Teilnahme an Cyber Übungen“, „Management der Leistungserbringung/Verträge Externe IT Dienstleister“, „Dokumentation“, „Risikomanagement“ und „Configuration/ Capacity Management“ wurden relativ häufig als Ziel für zukünftiges Engagement angegeben.
Weiters können in den Beantwortungen dieser Matrix Frage noch gewisse Übereinstimmungen zu anderen Fragen des Fragebogens untersucht werden. In Frage 10 bezüglich Aktivitäten zur Überprüfung der Informationssicherheit (siehe Abbildung 4.22) gaben nur 14,8% an „keine regelmäßigen Überprüfungsaktivitäten“ durchzuführen. Wenn diese Zahl den Beantwortungen der Matrix Frage gegenübergestellt wird, ergibt sich ein sehr stimmiges/konsistentes Bild, da auch hier die absolute Mehrheit der Unternehmen angegeben hat, sich mit „Audits/Penetration Tests oder Vulnerability Scans“ zu beschäftigen, um das eigene Informationssicherheitsniveau zu erheben und zu verbessern (191 Antworten: Implementiert 142, In Planung 21, Nicht vorhanden 28).
In Frage 15 gaben lediglich 16,8% der Unternehmen an, „keine Awareness-Aktivitäten“ durchzuführen. In der Matrix Frage wurde auch die Durchführung von Awareness Aktivitäten von einem Großteil der Unternehmen bejaht (194 Antworten: Implementiert 129, In Planung 29, Nicht vorhanden 36) und es ergibt sich auch hier wieder eine gute Übereinstimmung zu den Beantwortungen auf Frage 15.
Zusammenfassend ist zu der organisatorischen Aufstellung zu sagen, dass einige Maßnahmen (Spam & Antivirus, Backup und Wiederherstellung) beinahe durchgängig vorhanden sind. In Bezug auf weitere

Maßnahmen zeigt sich beim Implementierungsgrad ein relativ homogenes Bild, in dem nur wenige Maßnahmen so stark wie gewisse technische Systeme bezüglich deren Verbreitung hervorstechen. Fast bei jeder Maßnahme gibt es auch Beantwortungen, dass diese „in Planung“ oder „nicht vorhanden“ ist. Der Implementierungsgrad und die Qualität der zusätzlich zu den beinahe in allen Unternehmen vorhandenen organisatorischen Maßnahmen wird von Faktoren wie der Unternehmensgröße sowie dem allgemeinen Bewusstsein für und dem Stellenwert der Informationssicherheit abhängig sein. Einige organisatorische Maßnahmen wie „Versicherung gegen Cyber/IT-Angriffe“, „Firmeneigenes CERT“, „Durchführung/Teilnahme an Cyber Übungen“ oder der „Betrieb eines IKS inklusive IT-Kontrollen“ sind nur bei einer Minderheit der Unternehmen umgesetzt.

In den Abbildungen 4.47, 4.48 und 4.49 befinden sich die länderspezifischen Auswertungen für Deutschland, Österreich und die Schweiz. Aufgrund der Vielzahl an organisatorischen Maßnahmen wird ebenfalls auf einen detaillierten Vergleich des Implementierungsgrades einzelner Maßnahmen in den verschiedenen Ländern verzichtet. Bei einem groben Vergleich der Abbildungen fällt jedoch abermals auf, dass in der Schweiz tendenziell am wenigsten rote Flächen (=nicht implementierte Maßnahmen) sichtbar sind.

Der Unterschied zwischen der Schweiz und Deutschland ist aber nicht so eindeutig sichtbar wie zuvor bei den technischen Maßnahmen (abgesehen von den Beantwortungen zum „Betrieb eines IKS inklusive IT-Kontrollen“, wo die Verbreitung in der Schweiz erheblich höher ist), und es gibt auch einige Maßnahmen bei denen Deutschland eine höhere Verbreitung aufweist (etwa bei „Awareness Aktivitäten“, „Identitäts- und Zugriffsmanagement“, „Vorfallmanagement“ sowie „Durchführung/Teilnahme an Cyber Übungen“). Im Vergleich weist Österreich abermals den größten Anteil an nicht implementierten Maßnahmen auf. Wie auch schon bei den technischen Maßnahmen angemerkt können diese Unterschiede jedoch auch teilweise darauf zurückzuführen sein, dass in Österreich im Vergleich zu Deutschland und Schweiz relativ viele kleine Unternehmen an der Umfrage teilnahmen, während in der Schweiz sehr viele Unternehmen mit mehr als 1000 Abgestellten antworteten.

Natürlich muss auch bezüglich der organisatorischen Maßnahmen auf die Problematik der relativ groben und oberflächlichen Behandlung des Themas hingewiesen werden. Grundsätzlich wäre es sehr interessant zu erheben, wie die „Qualität“ bzw. der tatsächliche „Reifegrad“ der in den Unternehmen implementierten technischen und organisatorischen Maßnahmen aussieht (dieser kann sehr unterschiedlich sein. Beispielsweise könnten einige Unternehmen bereits bei einem vorhandenen und einigermaßen gut verwalteten Active Directory ihr Identitäts- & Zugriffsmanagement als „Implementiert“ ansehen, während andere sich hierzu viel genauer mit dem Rechtevergabe-, Rechteüberprüfungs- & Genehmigungsprozess und einer zentralen Benutzerverwaltung (insbesondere auch auf nicht AD-Systemen) auseinandersetzen).

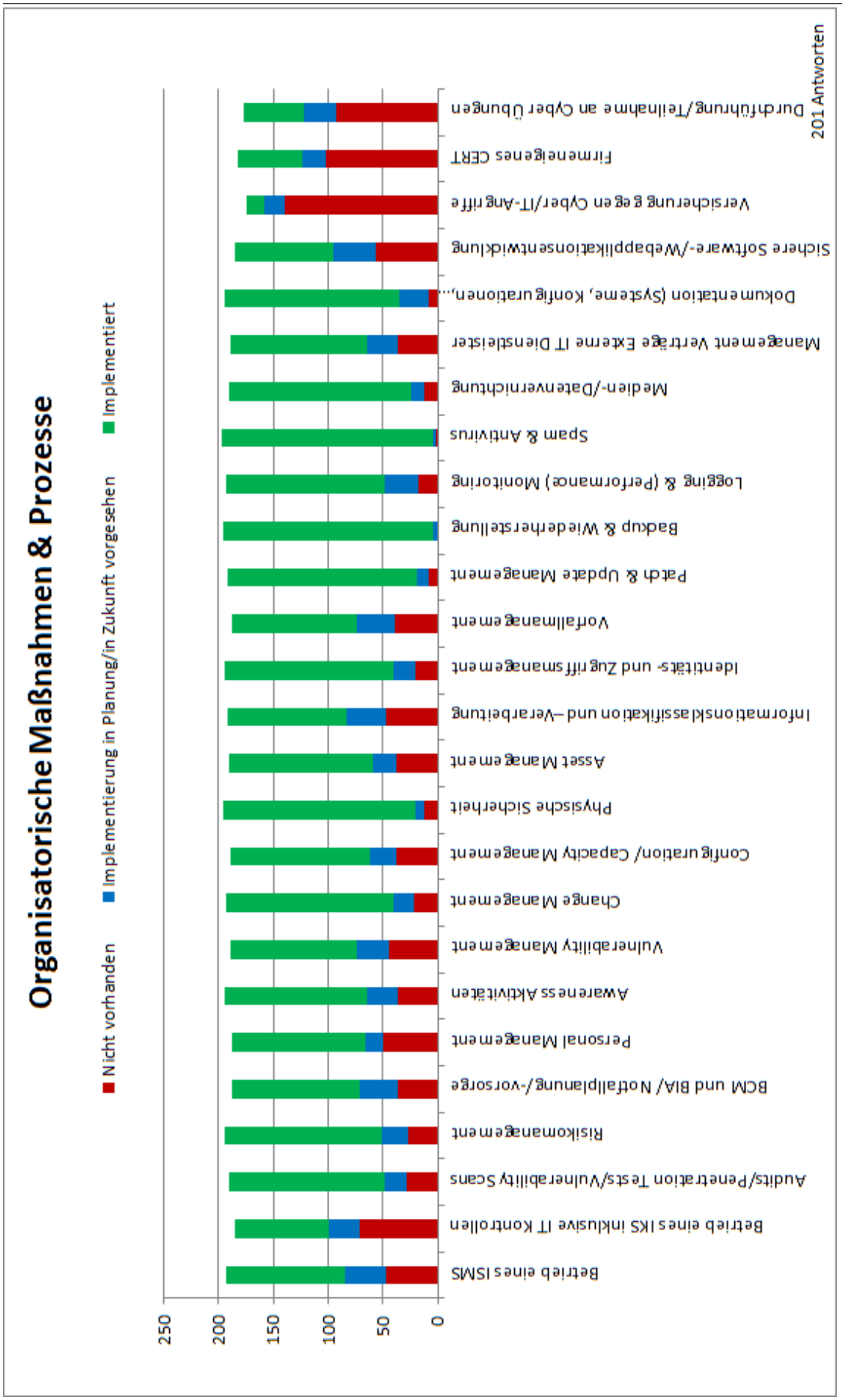

Abbildung 4.46.: Organisatorische Maßnahmen & Prozesse - Gesamt

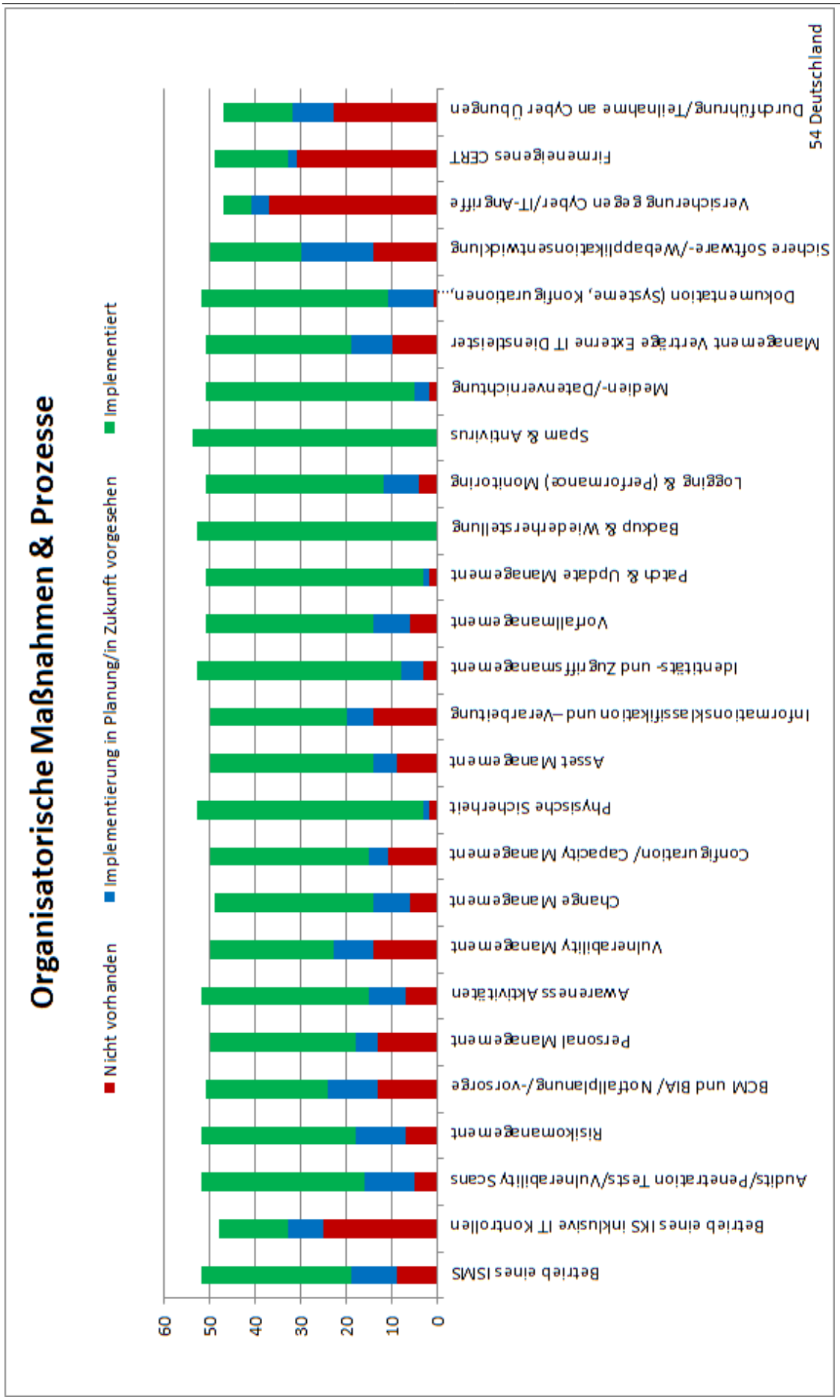

Abbildung 4.47.: Organisatorische Maßnahmen & Prozesse - Deutschland

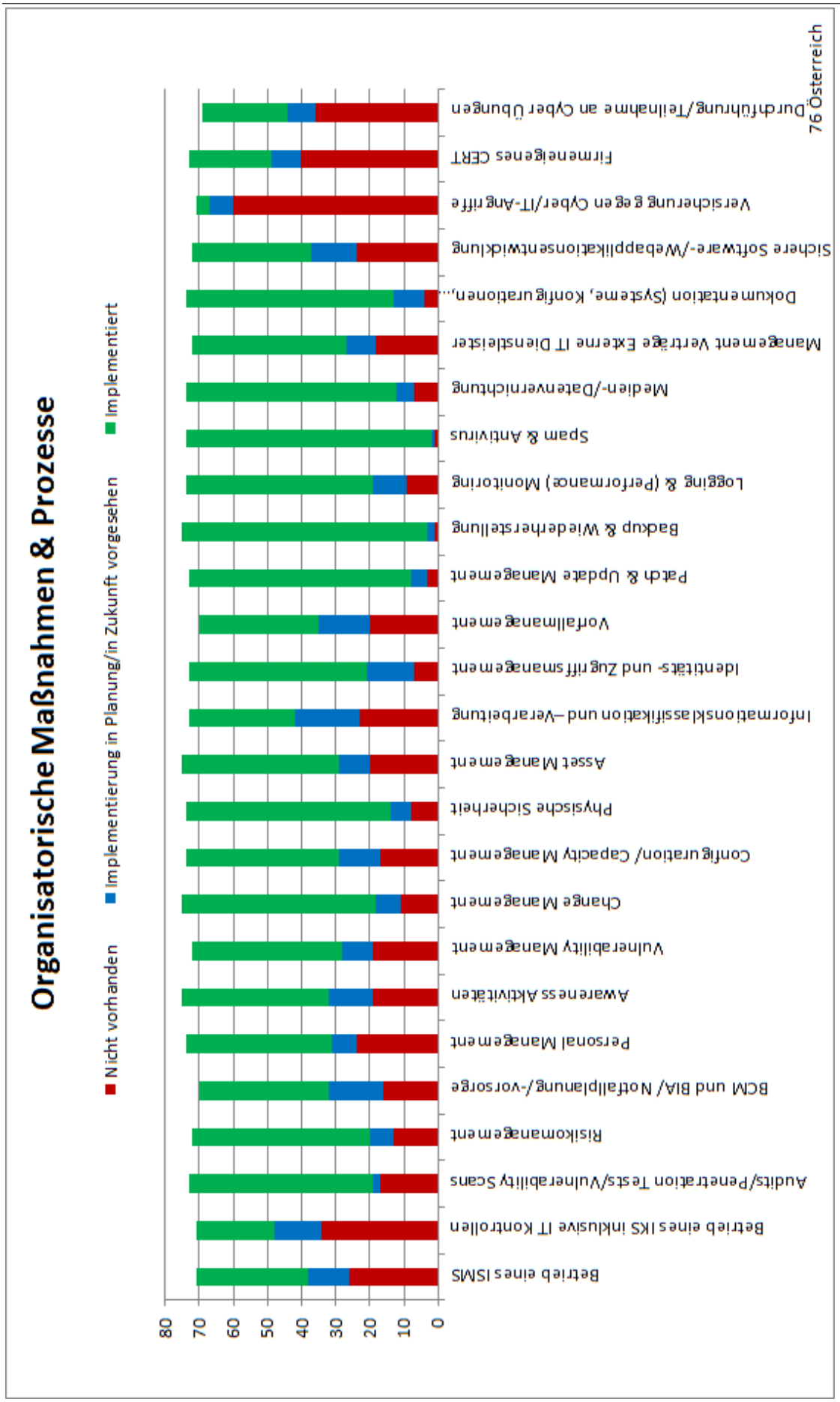

Abbildung 4.48.: Organisatorische Maßnahmen & Prozesse - Österreich

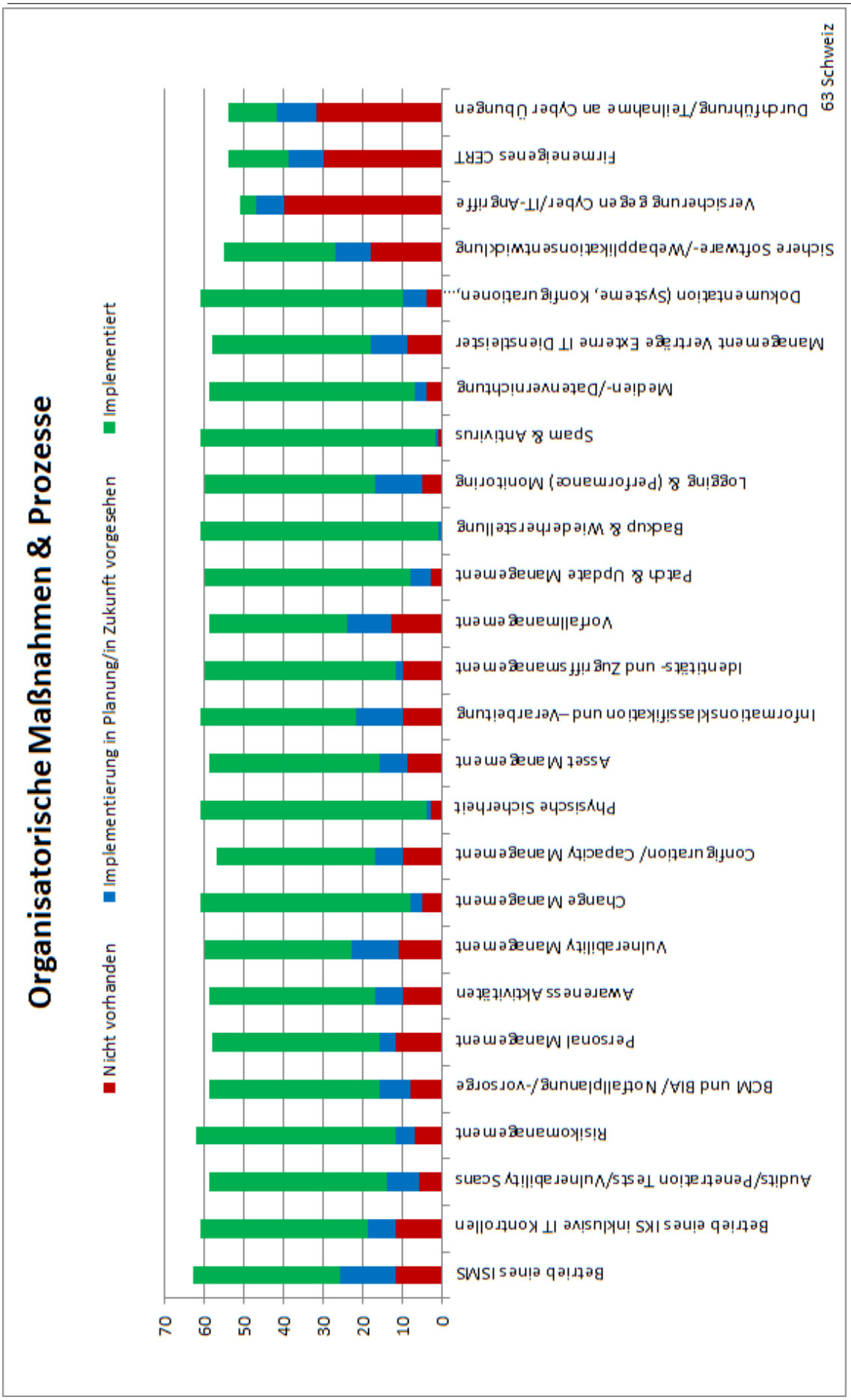

Abbildung 4.49.: Organisatorische Maßnahmen & Prozesse - Schweiz

Hierzu müsste jedoch der Umfang des Fragebogens drastisch erhöht werden, um in Detailfragen genauer auf die Ausprägung und den Reifegrad einzelner Maßnahmen eingehen zu können. Eine Bewertung der „Qualität“ (sowie eventuell der Relevanz, siehe Kapitel 2.3.5) der implementierten Maßnahmen (etwa nach Schulnoten) durch die Unternehmen könnte ein erster Ansatz sein. Hierbei wäre jedoch wieder zu beachten, dass Unternehmen den Reifegrad dabei leicht über- bzw. unterschätzen könnten, sofern keine umfangreiche Begleitbeschreibung mitgeliefert wird (und sich der Umfang und der Zeitaufwand für die Beantwortung ebenfalls weiter erhöhen würde, siehe auch Überlegungen in Kapitel 5.2).

4.3. Verifikation der Hypothesen

Im Folgenden werden nun die in Kapitel 1.4 aufgestellten Hypothesen überprüft und beschrieben.
Natürlich muss auch bei der Auswertung der Hypothesen die bereits in Kapitel 4.2 aufgezeigte Problematik berücksichtigt werden, dass die meisten Teilnehmerinnen und Teilnehmer dieser Umfrage ein höheres Bewusstsein und Interesse für das Thema der Informationssicherheit aufweisen und hierin besser aufgestellt sind als ein „typisches durchschnittliches Unternehmen“. Es ist somit möglich und wahrscheinlich, dass die Gesamtsituation der Informationssicherheit, verglichen mit den hier aufgeführten Ergebnissen und Schlüssen, „anders“ bzw. „schlechter“ sein könnte, als hier nahegelegt wird.
Hypothese I, dass ein Großteil der Unternehmen stark von der eigenen IT abhängig ist, kann eindeutig bestätigt werden. So geben - wie in Abbildung 4.4 ersichtlich - 57,6% der Unternehmen an, „sehr stark“ von der eigenen IT abhängig zu sein, während sich weitere 31,4% als „stark“ von der eigenen IT abhängig einschätzen. Lediglich 11% der Unternehmen meinen „nur in Teilbereichen“ oder nur in „geringem Ausmaß“ von der eigenen IT abhängig zu sein.
Die Annahme, dass große Unternehmen häufiger angeben, stark von der eigenen IT abhängig zu sein, kann über die in der Tabelle 4.2 und Abbildung 4.50 ersichtlichen Ergebnisse nicht eindeutig bestätigt werden. Während bei den Unternehmen mit 1-49 Mitarbeiterinnen und Mitarbeitern 57% die höchste Abhängigkeit angaben, taten dies bei den Unternehmen >1000 knapp 62% (bei den Unternehmen 250-999 gibt es jedoch einen Ausreißer nach unten mit nur 48%, während ebenfalls 54% der Unternehmen 50-249 diese Angabe machten). Große Unternehmen (>1000) gaben im Vergleich zu den drei anderen Unternehmensgrößenklassen die beiden geringsten Abhängigkeiten nur sehr selten an, was doch für eine gewisse Tendenz zu einer mit der Unternehmensgröße steigenden Abhängigkeit von der IT spricht.
Bei dieser Auswertung ist jedoch zu berücksichtigen, dass die unterschiedlichen Unternehmensgrößenklassen unterschiedlich stark vertreten sind (1-49: 49, 50-249: 28 250-999: 43, >1000: 90) und der Stichprobenumfang von 210 relativ klein ist, wodurch sich durch einzelne Beantwortungen relativ starke Schwankungen bei den Prozentwerten ergeben können. Diese Ergebnisse können daher nur als Indiz für

die Richtigkeit der Behauptung, dass große Unternehmen häufiger eine starke Abhängigkeit angeben, gesehen werden.

Anmerkung: Diese Einschränkung bezüglich des geringen Stichprobenumfangs (insbesondere hinsichtlich der Unternehmensgrößenklassen) und der daraus resultierenden starken Schwankungen aufgrund der Antworten einzelner Unternehmen muss auch bei der Behandlung der weiteren Hypothesen berücksichtigt werden, da sich diese Tatsache auf die Aussagekräftigkeit der Ergebnisse auswirken kann.

Abhängigkeit	**1-49**	**50-249**	**250-999**	**>1000**
sehr starke Abhängigkeit von IT	57,14%	53,57%	48,84%	62,22%
	28	15	21	56
starke Abhängigkeit von IT	26,53%	39,29%	32,56%	30,00%
	13	11	14	27
Abhängigkeit von IT lediglich in Teilbereichen	10,20%	7,14%	13,95%	5,56%
	5	2	6	5
geringe Abhängigkeit von IT	6,12%	0,00%	4,65%	2,22%
	3	0	2	2
Anzahl Beantwortungen	***49***	***28***	***43***	***90***

Legende: Hell-/Dunkelgrau Min/Max der Zeilen

Tabelle 4.2.: Abhängigkeit IT nach Unternehmensgröße

Hypothese II, dass es in einem Großteil der Unternehmen Vorfälle im Bereich der Informationssicherheit gab, kann unter Berücksichtigung der Ergebnisse zu Frage 12, welche in Abbildung 4.26 dargestellt sind, bestätigt werden. Dort gab lediglich eine Minderheit von 11,1% der Unternehmen an, im vergangenen Jahr von keinen Vorfällen betroffen gewesen zu sein. Dies bedeutet, dass ein Großteil von knapp 89% der Unternehmen, im letzten Jahr von zumindest einem Vorfall im Bereich der Informationssicherheit betroffen war. Die Annahme, dass die Betroffenheit von Vorfällen unabhängig von der Unternehmensgröße ist, muss angesichts der Daten in Tabelle 4.3 eher bezweifelt werden. Während noch 18% der Unternehmen mit 1-49 Mitarbeiterinnen und Mitarbeitern angaben, von keinen Vorfällen betroffen gewesen zu sein, machten diese Angabe nur noch knapp 6% der >1000 Unternehmen.

Die Annahme, dass Unternehmen, die von Vorfällen betroffen waren, häufiger und mehr technische und organisatorische Maßnahmen einsetzen, kann nicht bestätigt werden (Grund für die Annahme war, dass diese Unternehmen aufgrund von Vorfällen ein höheres Sicherheitsbewusstsein haben und daher vermehrt Maßnahmen umsetzen). Ein Vergleich der Umsetzung von technischen und organisatorischen Maßnahmen in Unternehmen, welche Vorfälle bzw. keine Vorfälle hatten, scheint eher anzudeuten, dass die Unternehmen ohne Vorfälle etwas besser aufgestellt sind.

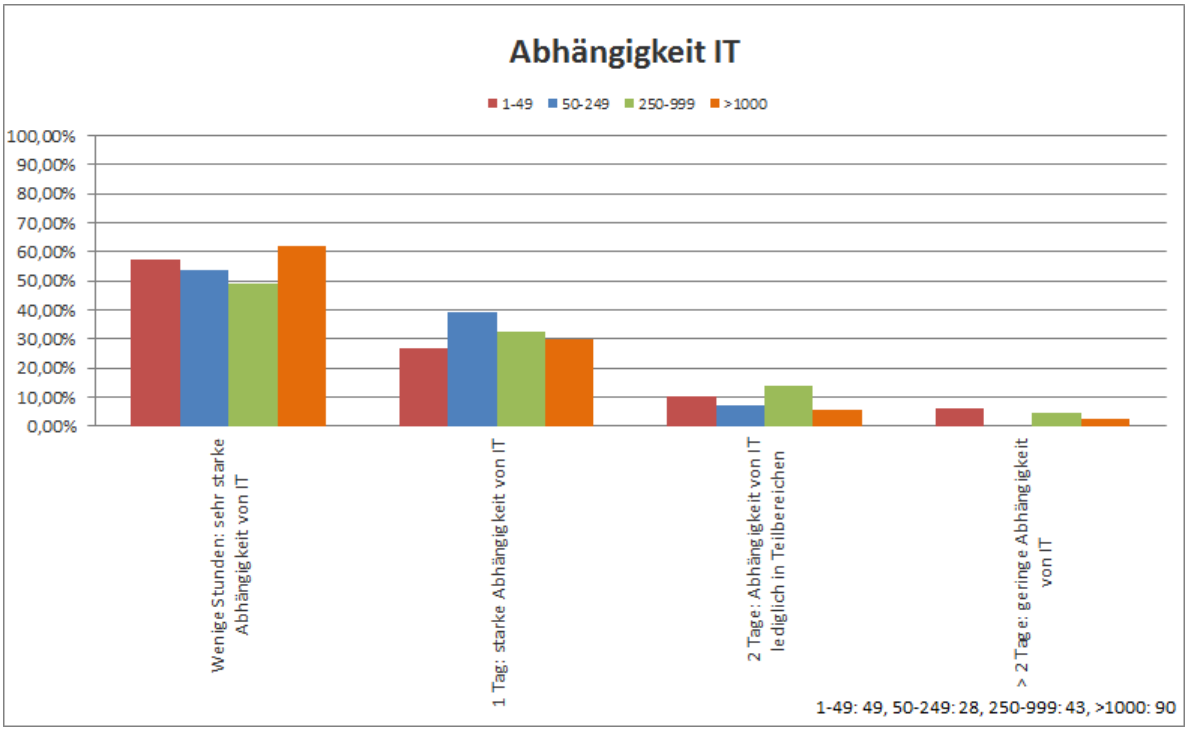

Abbildung 4.50.: Abhängigkeit IT nach Unternehmensgröße

Da jedoch nur sehr wenige (22) Unternehmen keinen Vorfälle hatten, muss dieser Vergleich jedoch nicht unbedingt aussagekräftig sein (die Diagramme sind im Anhang A.2 ersichtlich). Er könnte aber zu vertiefenden Untersuchungen anregen (etwa auf Grundlage der Hypothese, dass Unternehmen, die technisch und organisatorisch besser aufgestellt sind, auf Grund ihres höheren Sicherheitsbewusstseins weniger bzw. keine Vorfälle haben. Es müsste jedoch auch berücksichtigt werden, dass die besser aufgestellten Unternehmen auch eine höhere Erkennungsrate aufweisen können und bei anderen Unternehmen die Vorfälle einfach unbemerkt passieren).

Vorfälle	**1-49**	**50-249**	**250-999**	**>1000**
keine Vorfälle	18,37%	11,54%	11,63%	5,88%
	9	3	5	5
Vorfälle	81,63%	88,46%	88,37%	94,12%
	40	23	38	80
Anzahl Beantwortungen	***49***	***26***	***43***	***85***
Legende: Hell-/Dunkelgrau Min/Max der Zeilen				

Tabelle 4.3.: Vorfälle nach Unternehmensgröße

Hypothese III, dass „Malware“, „Hacking“, „Datenverluste“, „Fahrlässigkeit von Mitarbeitern“ und „physischer Diebstahl“ von Unternehmen als Hauptrisiken bzw. Bedrohung in Bezug zur Informationssicherheit angesehen werden, kann unter Berücksichtigung der Ergebnisse der Frage 6 in Abbildung 4.14 für „Malware“, „Fahrlässigkeit eigener Mitarbeiter“ sowie „Datenverluste“ bestätigt werden. „Hacking“ und „physischer Diebstahl“ werden hingegen nicht als Hauptrisiken angesehen. Dafür wurden in Frage 6 auch „Datendiebstahl“ sowie „APTs“ und „Social Engineering“ häufig genannt.

Hypothese IV, dass „Malware“, „Hacking“ und „physischer Diebstahl“ zu den häufigsten Vorfallsarten gehören, kann über die Ergebnisse der Frage 12, welche in Abbildung 4.26 ersichtlich sind, überprüft werden. In diesen wurde „Malware“ tatsächlich am häufigsten genannt. Von „Hacking“ oder „physischen Diebstahl“ waren aber anscheinend nur relativ wenige Unternehmen betroffen. Vorfallsarten wie „Spam“, „Fahrlässigkeit von Mitarbeitern“, „Hardware- oder Software-Fehler“, „Stromausfälle“ sowie „(Spear)Phishing“ wurden häufiger genannt.

Wie in Abbildung 4.27 zu sehen ist, ist das Auftreten der Vorfälle relativ unabhängig vom Land (nur geringe länderspezifische Unterschiede) und auch in Abbildung 4.51 wird ersichtlich, dass es je nach Unternehmensgröße meist nur geringe Schwankungen bezüglich der Häufigkeit der verschiedenen Vorfallsarten gibt. Kleine Unternehmen (1-49) weisen jedoch oft gewisse Unterschiede im Vergleich zu den größeren Unternehmen auf.

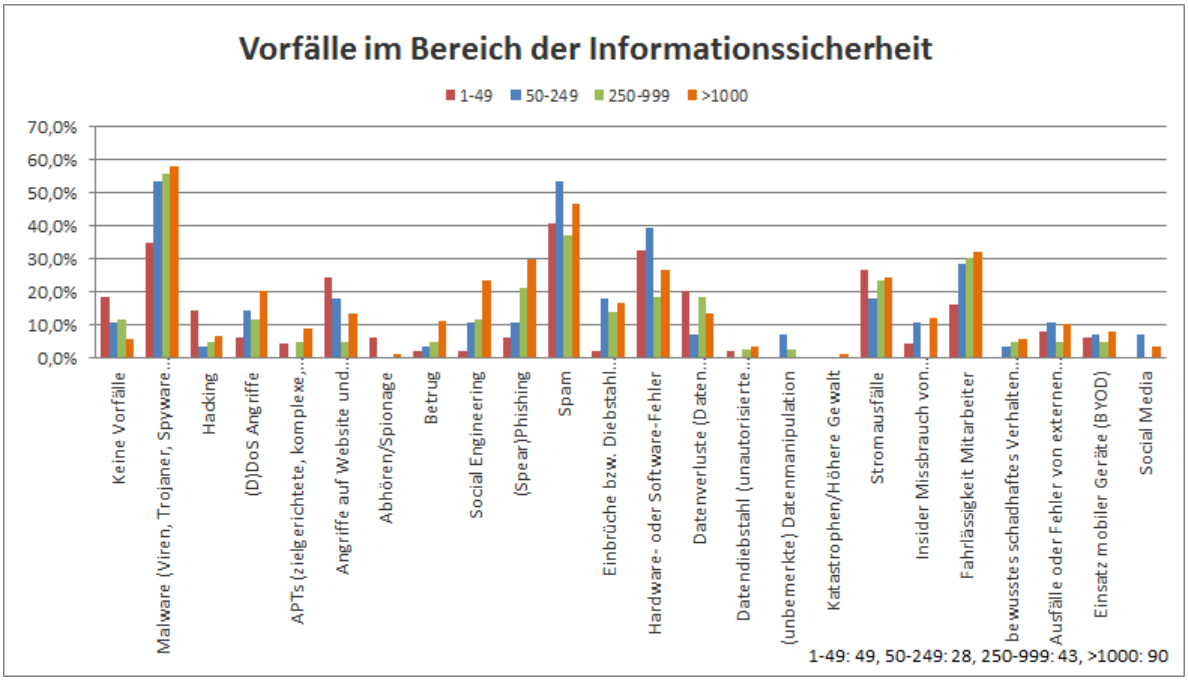

Abbildung 4.51.: Vorfälle im Bereich der Informationssicherheit nach Unternehmensgröße

Hypothese V, dass ein Großteil der Unternahmen von aktuellen Sicherheitslücken wie Heartbleed oder Shell Shock betroffen war, kann über die in Abbildung 4.36 dargestellten Ergebnisse eindeutig bestätigt werden. Beinahe zwei Drittel der Unternehmen gaben an, dass sie von diesen Lücken betroffen gewesen waren. Allerdings kam es nur bei einer Minderheit der Unternehmen dadurch zu einer tatsächlichen Beeinträchtigung der Geschäftstätigkeiten, und für Angriffe wurden diese Lücken nur bei einem der 217 Unternehmen genutzt. Es muss jedoch berücksichtigt werden, dass eine tatsächliche Ausnutzung dieser Lücken (insbesondere Heartbleed) nur schwer bzw. kaum nachweisbar war, wodurch die Möglichkeit besteht, dass stattgefundene Angriffe von den Unternehmen gar nicht bemerkt wurden.
Die Annahme, dass große Unternehmen häufiger von diesen Lücken betroffen gewesen waren (sie haben eine größere Infrastruktur), lässt sich über die in Abbildung 4.52 ersichtlichen Ergebnisse bestätigen. So gaben lediglich 20% der >1000 Unternehmen an, von diesen Lücken nicht betroffen gewesen zu sein, während dies bei den kleineren Unternehmen zwischen 33%-38% angaben.

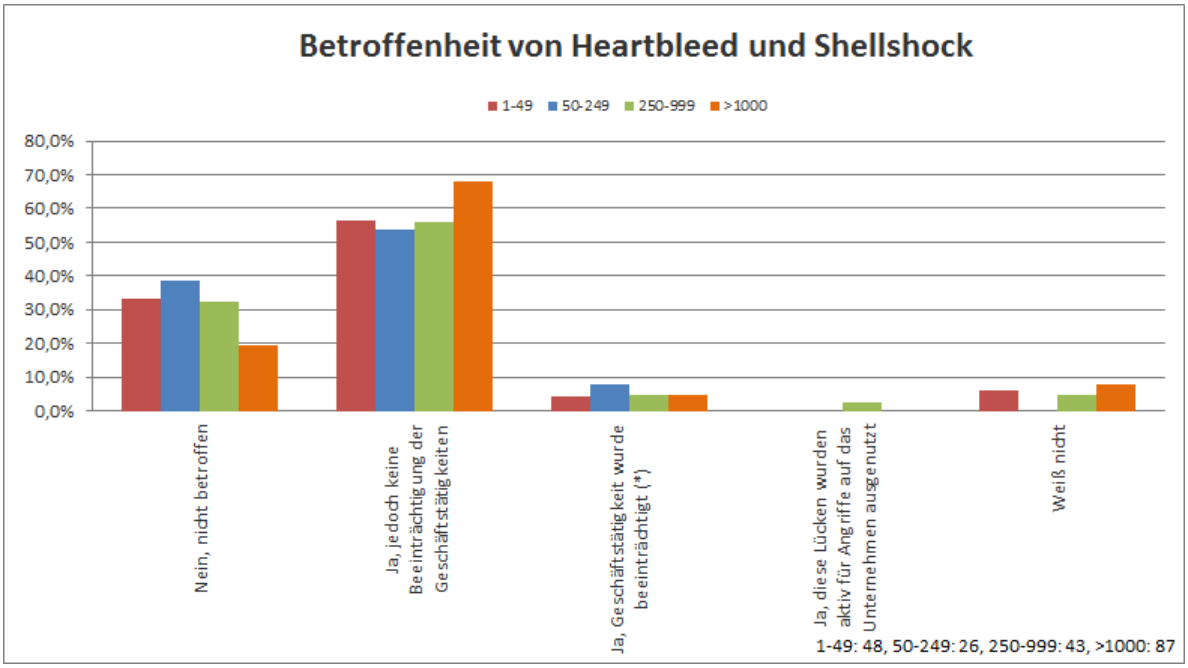

Abbildung 4.52.: Betroffenheit von Heartbleed und Shellshock nach Unternehmensgröße

Hypothese VI, dass ein Großteil der Unternehmen als wichtigste Beweggründe für IT-/Informationssicherheit „gesetzliche Vorgaben und Compliance“, die „Vermeidung von Datenverlusten oder Verfälschungen“ sowie die „Sicherstellung der Stabilität des Betriebes“ ansieht, kann über die in Abbildung 4.10 dargestellten Ergebnisse eindeutig bestätigt werden. Es ist jedoch anzumerken, dass auch die „Vermeidung von (Geld/Image)Verlusten durch Sicherheitsvorfälle oder Datenpannen“ von über 70% der Unternehmen als Grund für deren Informationssicherheitsengagement genannt wurde.
Die Annahme, dass „Gesetzliche Vorgaben und Compliance“ von großen Unternehmen öfter als Grund

für Informationssicherheit angeführt werden, kann anhand der in Abbildung 4.53 dargestellten Daten für sehr kleine Unternehmen bestätigt werden. So werden „Gesetzliche Vorgaben und Compliance“ nur von ca. 47% der kleine Unternehmen (1-49) als Grund genannt, während ca. 97% der großen Unternehmen (>1000) dies als Motivation anführten. Auch schon bei den etwas größeren Unternehmen (50-249 und 249-999) geben über 80% dies als Beweggrund für ihr Informationssicherheitsengagement an.

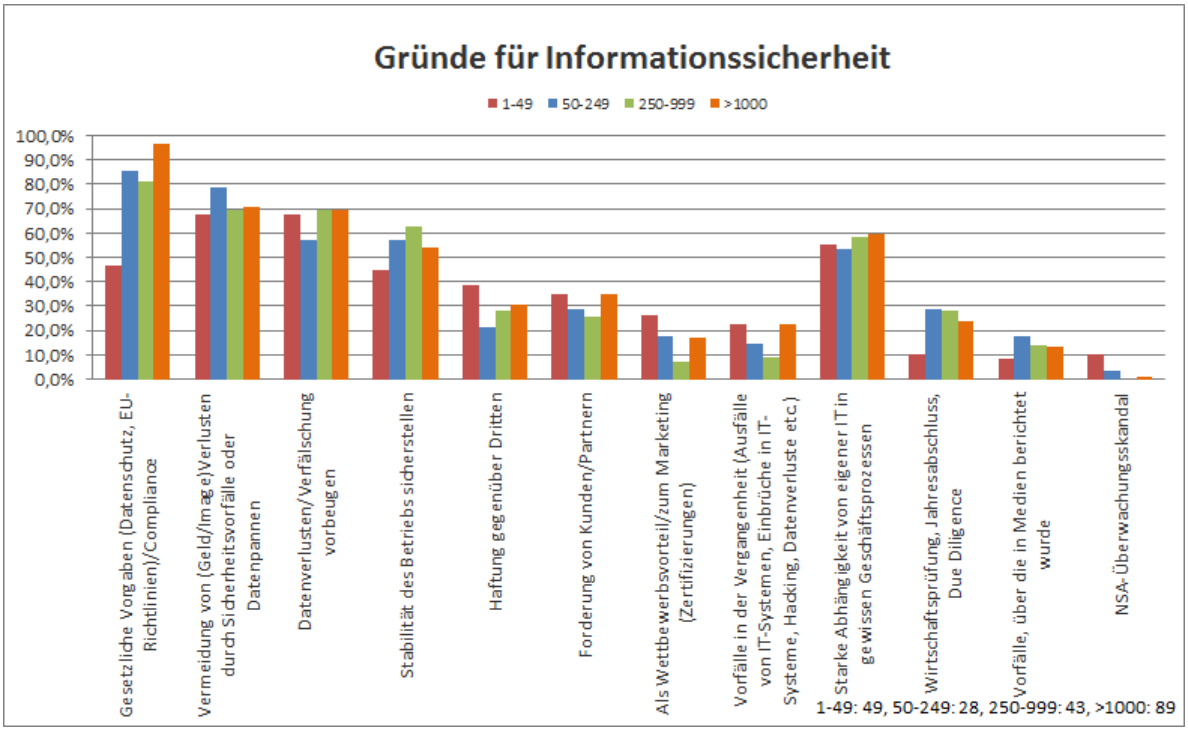

Abbildung 4.53.: Gründe und Motivation für Informationssicherheit nach Unternehmensgröße

Hypothese VII, in welcher vermutet wird, dass ein Großteil der Unternehmen Open Source Software einsetzt und die meisten keine weiteren Schritte zur Überprüfung dieser auf Fehlerfreiheit, Qualität, Korrektheit und Zuverlässigkeit durchführen, kann über die Ergebnisse in Abbildung 4.34 eindeutig bestätigt werden. Es gaben lediglich 12,4% der Unternehmen an, „keine Open Source Software“ zu nutzen (ein einziges Unternehmen - bei 217 Antworten - gab an „Open Source Software aufgrund von Sicherheitsbedenken nicht einzusetzen“), während die absolute Mehrheit von 58,1% der Unternehmen antwortete, „Open Source Software einzusetzen, jedoch keine Überprüfung dieser durchzuführen“. Immerhin ein knappes Viertel (25,8%) nutzen Open Source Software und trafen dabei Maßnahmen wie „Durchführung von Code Reviews und Recherche zu Auditergebnissen, Sicherheitsanalysen und dem Entwicklerkreis“, um deren Sicherheit, Qualität und Vertrauenswürdigkeit zu überprüfen. Insbesondere hier sei nochmals darauf verwiesen, dass die meisten Unternehmen, welche an dieser Umfrage teilnahmen, ein relativ hohes Sicherheitsbewusstsein aufweisen (siehe Anmerkung in Kapitel 4.2).

Generell ist anzumerken, dass die Zahl von 12,4% der Unternehmen ohne Nutzung von Open Source Software relativ hoch scheinen kann, da gewisse Open Source Bibliotheken wie openssl oder verschiedene Browser und Addons eine sehr hohe Verbreitung haben und teilweise auch in kommerziellen Produkten genutzt werden. Auch ist mit einem Viertel die Anzahl der Unternehmen, welche Open Source Software nutzen und dabei Maßnahmen treffen um Sicherheit, Qualität und Vertrauenswürdigkeit zu überprüfen, relativ hoch. Bei „Durchführung von Code Reviews und Recherche zu Auditergebnissen, Sicherheitsanalysen und dem Entwicklerkreis“ handelt es sich jedoch nur um eine exemplarische Liste und Unternehmen werden nicht immer alle Maßnahmen (insbesondere selbstständige Code Reviews) treffen. Nichtsdestotrotz sprechen die Antworten dieses knappen Viertels der Unternehmen für ein Bewusstsein hinsichtlich der potentiell mit dem Einsatz von Open Source Software verbundenen Problematiken.

Zu der ***Hypothese VIII***, welche sich mit dem auf das NSA Skandal steigendem Interesse für „IT Made in Austria/Germany/Switzerland/Europe“ auseinandersetzt, kann über die in Abbildung 4.40 dargestellten Ergebnisse nur eine bedingte Aussage gemacht werden. In Frage 19 nennen nur 9,3% der Unternehmen die „Planung zur verstärkten Beschaffung von IT Made in Austria/Germany/Switzerland bzw. Europe“ als eine von ihnen in Hinsicht auf die NSA Enthüllungen getroffene Maßnahme. Dies ist lediglich eine Minderheit der Unternehmen und da keine Vergleichsdaten vorliegen (wie viele Unternehmen hatten vor den NSA Enthüllungen besonderes Interesse an heimischer bzw. europäischer IT), kann keine endgültige Aussage zu dieser Hypothese gemacht werden.

Hier wäre eine vertiefende Untersuchung und Marktforschung sicherlich interessant. Wie auch in Abbildung 4.41 zu sehen ist, ist das Interesse an heimischer bzw. europäischer IT in den Deutschland, Österreich und der Schweiz ungefähr gleich hoch (9,3% Deutschland, 10,1% Österreich, 7,9% Schweiz). Die Annahme, dass dieses Thema für kleine Firmen nicht sehr bedeutend ist, kann anhand der Daten in Abbildung 4.54 verneint werden. In dieser gaben 12,2% der kleinen Unternehmen an, in dieser Hinsicht Maßnahmen getroffen zu haben während dies ebenfalls nur 9,3% der großen Unternehmen (>1000) taten. Interessanterweise nutzten nur 7,7% bzw. 4,9% der etwas größere Unternehmen (50-249 und 249-999) diese Antwortoption.

Hypothese IX, in welcher vermutet wird, dass der NSA Skandal zu größerer Vorsicht bei der Nutzung von Cloud Services und zu einer verstärkten Nutzung bzw. Nachfrage von heimischen bzw. europäischen Anbietern führt, kann über die Ergebnisse in den Abbildungen 4.30 und 4.40 bedingt bestätigt werden. So erklärten in Frage 14 14,9% der Unternehmen Cloud und Outsourcing „aufgrund von Sicherheitsbedenken und diverser Vorkommnisse (NSA-Skandal etc.)“ nicht zu nutzen, während in Frage 19 ebenfalls 16,3% antworteten „im Fall von Cloud oder Outsourcing verstärkt auf heimische/europäische Anbieter zu setzen“. Es ist jedoch zu beachten, dass hier bei den Antworten länderspezifisch gewisse Unterschiede

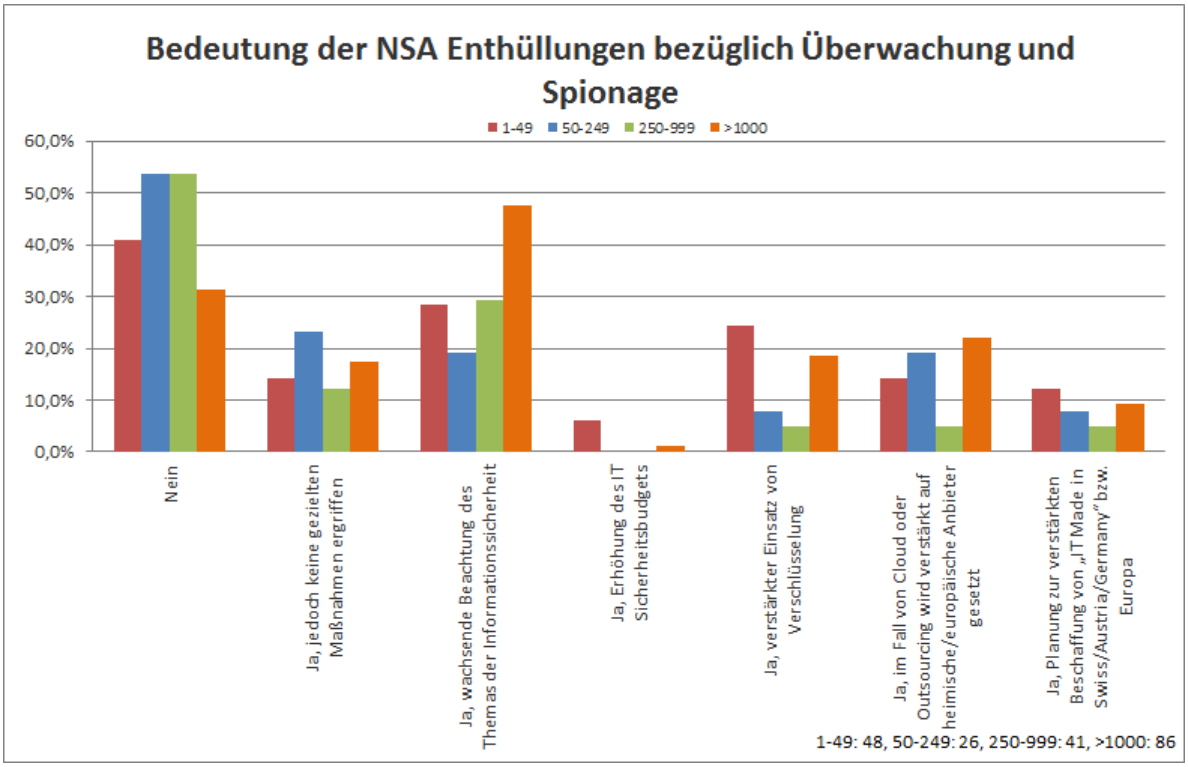

Abbildung 4.54.: Bedeutung der NSA-Enthüllungen bezüglich Überwachung und Spionage nach Unternehmensgröße

vorhanden waren. Insgesamt kann hinsichtlich dieser Hypothese festgehalten werden, dass dieses Thema zwar eher von einer Minderheit angesprochen wurde, aber trotzdem eine gewisse Tendenz zu größerer Vorsicht bei der Nutzung von Cloud Services und zu einer verstärkten Nutzung bzw. Nachfrage von heimischen bzw. europäischen Anbietern erkennbar ist.

Hypothese X, dass die Nutzung von Standards bzw. Empfehlungen im Bereich der Informationssicherheit insbesondere in kleinen Unternehmen nicht sehr weit verbreitet ist, kann anhand der Ergebnisse in 4.55 bestätigt werden. Mit über 28% war der Anteil an kleinen Unternehmen (1-49), die angaben keine Standards oder Empfehlungen zu nutzen, relativ hoch (im Vergleich zu 50-249:10%, 250-999: 7%, >1000 10%).

Generell ist die Nutzung von Standards oder Empfehlungen jedoch relativ weit verbreitet. So gaben in Abbildung 4.12 insgesamt lediglich 12,7% der Unternehmen an, solche Werke und Hilfestellungen nicht zu verwenden. Die bei weitem höchste Verbreitung weisen ISO 27001, BSI-Grundschutz und ITIL auf, sowie bei großen Unternehmen (>1000) auch COBIT.

Hypothese XI, dass Cyber Versicherungen (noch) nicht sehr verbreitet sind und sich hauptsächlich große Unternehmen hierfür interessieren, kann über die Ergebnisse in Abbildung 4.46 eindeutig bestätigt werden. Unter allen organisatorischen Maßnahmen sind Cyber Versicherungen diejenige, die mit Abstand

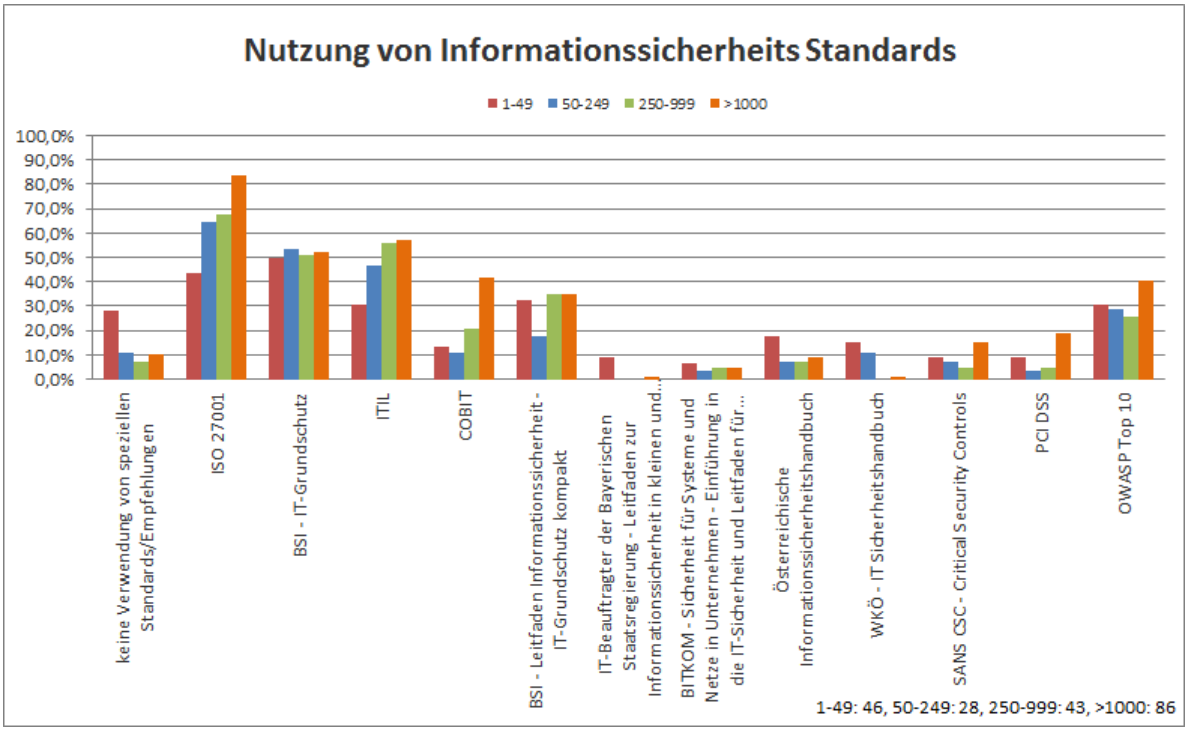

Abbildung 4.55.: Nutzung von Standards & Empfehlungen im Bereich der Informationssicherheit nach Unternehmensgröße

am seltensten als „implementiert“ und am öftesten als „nicht vorhanden“ bezeichnet wurde. Bei insgesamt lediglich 173 Antworten zu dieser Maßnahme (im Vergleich zu den anderen Maßnahmen hat diese Maßnahme auch die wenigsten Antworten insgesamt) gaben lediglich 16 Unternehmen an, eine Cyber Versicherung zu besitzen. Hierbei wurde diese Maßnahme noch am häufigsten von großen Unternehmen (bei den 70 Unternehmen >1000 wurde sie von 10 als „implementiert“ gemeldet), während bei allen anderen Unternehmensgrößen diese Maßnahme nur in Einzelfällen genannt wurde. Auch in Hinblick auf einen zukünftigen Einsatz zeigt sich dasselbe Bild, da Cyber Versicherung wiederum hauptsächlich von großen Unternehmen (abermals bei 10 der 70Unternehmen >1000) als „in Planung/In Zukunft“ vorgesehen bezeichnet wurde.

Hypothese XII, dass APT zwar ein beachtetes Thema sind aber bei weitem keine der „vorrangigen“ Vorfallsarten (hinsichtlich der Anzahl an Meldungen bzw. betroffenen Unternehmen), kann eindeutig bestätigt werden. In Frage 6 zu den Hauptrisiken und Bedrohungen in Bezug auf Informationssicherheit geben knapp 30% an, dass APTs für sie hierzu zählen. Damit nehmen APTs in Abbildung 4.14 zwar keine führenden Position, aber einen Platz im oberen Mittelfeld ein. Dies spricht dafür, dass APTs ein doch weit beachtetes Thema sind.

Die Annahme, dass und nur wenige Unternehmen angeben im letzten Jahr Ziel eines APT gewesen zu sein kann bedingt bestätigt werden. In Frage 18, deren Ergebnisse in Abbildung 4.38 ersichtlich

sind, geben mit 56% knapp mehr als der Hälft der Unternehmen an, dass sie im letzten Jahr nicht Ziel eines APT waren. Mit 25% konnte knapp ein Viertel der Unternehmen auf diese Frage nur mit „weiß nicht“ antworten, während bei 5% zumindest ein Verdacht bezüglich des Auftretens eines APTs bestand. Lediglich ca. 12% erklärten, dass sie im vergangenen Jahr Ziel eines APTs waren, wobei nur bei einer Minderheit durch diesen auch tatsächlich ein Schaden entstand.

Bezüglich der tatsächlichen Häufigkeit des Auftretens von APTs muss natürlich berücksichtigt werden, dass APTs schon ihrer Definition nach komplex und schwer zu identifizieren bzw. nachzuweisen sind. Dies spiegelt sich auch in der Tatsache wider, dass bei knapp einem Drittel der Unternehmen Unsicherheit bzw. Unwissenheit bezüglich des Auftretens eines APT herrschte (25,9% „weiß nicht“ + 5,6% „Verdacht“).

Bei Frage 12 zu Vorfällen insgesamt gaben lediglich 5% der Unternehmen an, von einem APT betroffen gewesen zu sein. Dies sind weniger als die ungefähr laut Frage 18 12% betroffenen Unternehmen. Eventuell erklärt sich dieser Unterschied dadurch, dass einige der Unternehmen, welche in Frage 18 angaben den APT erfolgreich abgewehrt zu haben ihn nicht in Frage 12 bei den Vorfällen erwähnt haben (oder APTs unter den vielen anderen Vorfallsarten nicht beachtet bzw. übersehen wurde). In Abbildung 4.26, welche die Ergebnisse der Frage 12 darstellt, wird eindeutig ersichtlich, dass APT keine „vorrangige“ Vorfallsart sind und nur wenige andere Vorfallsarten von Unternehmen noch seltener genannt wurden.

Hypothese XIII bezüglich der technischen Aufstellung und der Verbreitung diverser Tools kann eindeutig bestätigt werden. In Abbildung 4.42 ist ersichtlich, dass grundlegende wichtige Sicherheitstools (wie Firewalls, Virenschutz, Backupsoftware, Spamschutz, VPNs) beinahe durchgängig vorhanden sind, wobei sich aber in Bezug auf weiterreichende oder speziellere Maßnahmen (Vulnerability Management Tools, IDS/IPS, WAF, E-Mail Verschlüsselung & Signatur, Log Management) ein gespaltenes Bild mit teilweise schnell sinkendem Implementierungsgrad zeigt (hier wird der Implementierungsgrad in Unternehmen von Faktoren wie der Unternehmensgröße sowie dem allgemeinen Bewusstsein für und dem Stellenwert der Informationssicherheit abhängig sein).

Einige technisch komplexe und aufwändige Maßnahmen (wie DLP, SIEM oder auch (Security) Configuration Management Software) sind nur bei einer Minderheit der Befragten im Einsatz.

Hypothese XIV bezüglich der organisatorischen Aufstellung und der Verbreitung diverser organisatorischen Maßnahmen kann ebenfalls eindeutig bestätigt werden. Wie in Abbildung 4.46 zu sehen ist, sind einige Maßnahmen (Spam & Antivirus, Backup und Wiederherstellung) beinahe durchgängig vorhanden. Auch die Themen physische Sicherheit Medien-/Datenvernichtung wurden sehr häufig genannt. Das Identitäts- und Zugriffsmanagement wurde hingegen schon etwas seltener aufgezählt.

Auch die Annahme, dass aufwändige und umfangreiche Maßnahmen wie der Betrieb eines ISMS, eines

IKS oder eines firmeneigenes CERT hauptsächlich von großen Unternehmen umgesetzt werden, kann bestätigt werden (generell sind solche Maßnahmen nur bei einer Minderheit der Unternehmen umgesetzt). In Tabelle 4.4 ist ein Überblick über die Umsetzung von 5 aufwändigen organisatorischen Maßnahmen nach Unternehmensgröße dargestellt. Bei allen Maßnahmen ist die eindeutige Tendenz erkennbar, dass der Umsetzungsgrad mit der Unternehmensgröße steigt.

Anmerkung: Dieser Trend zu einer mit der Unternehmensgröße steigenden Umsetzungsrate kann bei fast allen organisatorischen Maßnahmen (in unterschiedlicher Stärke und oft nicht so stark wie in Tabelle 4.4) beobachtet werden (außer natürlich bei den ohnehin schon sehr weit verbreiteten Maßnahmen). Durch die Nutzung von Prozentwerten entsteht eine gewisse Problematik, welche in der Anmerkung in Kapitel 4.3 genauer beschrieben ist.

Organisatorische Maßnahme	**1-49**	**50-249**	**250-999**	**>1000**
Betrieb eines ISMS	25,58%	50,00%	56,41%	72,62%
Implementiert	11	13	22	61
Insgesamt	43	26	39	84
Betrieb eines IKS inklusive IT Kontrollen	19,05%	37,50%	40,54%	64,63%
Implementiert	8	9	15	53
Insgesamt	42	24	37	82
Versicherung gegen Cyber/IT-Angriffe	6,82%	8,33%	2,86%	14,29%
Implementiert	3	2	1	10
Insgesamt	44	24	35	70
Firmeneigenes CERT	20,93%	23,08%	22,22%	46,75%
Implementiert	9	6	8	36
Insgesamt	43	26	36	77
Durchführung/Teilnahme an Cyber Übungen	21,43%	12,00%	30,56%	43,84%
Implementiert	9	3	11	32
Insgesamt	42	25	36	73

Legende: Hell-/Dunkelgrau Min/Max der Zeilen

Tabelle 4.4.: Organisatorische Maßnahmen nach Unternehmensgröße

Hypothese XV, dass die technische Aufstellung der Unternehmen oft besser als die organisatorische Aufstellung ist, kann bedingt bestätigt werden. Wie in den Zusammenfassungen der Ergebnisse der Abbildungen 4.42 und 4.46 beschrieben sind grundlegende wichtige technische Sicherheitstools (wie Firewalls, Virenschutz, Backupsoftware, Spamschutz) beinahe durchgängig vorhanden, während in Hin-

blick auf die organisatorische Aufstellung nur sehr wenige Maßnahmen (Spam & Antivirus, Backup und Wiederherstellung) beinahe durchgängig vorhanden sind und es fast bei jeder Maßnahme auch viele Beantwortungen gibt, dass diese „in Planung“ oder „nicht vorhanden“ ist. Generell fällt bei einem Vergleich der beiden Abbildungen auf, dass es mehr technische Maßnahmen mit sehr hohem Umsetzungsgrad gibt. Eine weitere, wenn auch eher grobe und nicht unbedingt streng wissenschaftliche Auswertung, welche einen Anhaltspunkt für diese Annahme bietet, ist die Berechnung der „Antwortquoten“ für die Optionen „Implementiert“, „in Planung“ und „Nicht vorhanden“ über die Summe aller technischen und organisatorischen Maßnahmen. Hierbei fällt - wie in Tabelle 4.5 ersichtlich - auf, dass über alle technischen Maßnahmen gerechnet knapp über 71% der Beantwortungen auf die Option „Implementiert“ fielen, während diese Option nur bei etwas über 66% aller Beantwortungen zu den organisatorischen Maßnahmen genutzt wurde. Auch die Option „nicht vorhanden“ wurde bei den organisatorischen Maßnahmen, über alle Maßnahmen gerechnet, häufiger genutzt (technisch 18% zu knapp 21% organisatorisch). Ebenso kann auch für die Option „in Planung“ beobachtet werden, dass sie insgesamt bei den organisatorischen Maßnahmen etwas öfter genutzt wurde als bei den technischen Maßnahmen (technisch 10% zu knapp 12% organisatorisch).

Maßnahmen: Summe aller Maßnahmen, ***Imp***: Implementiert, ***Pl***: Implementierung in Planung/ in Zukunft vorgesehen, ***NA***: Nicht vorhanden

Maßnahmen	***Imp***	***Pl***	***NA***	***Summe***
Technisch	71,27%	10,59%	18,14%	
Anzahl Beantwortungen	3761	559	957	5277
Organisatorisch	66,72%	12,29%	20,98%	
Anzahl Beantwortungen	3294	607	1036	4937

Legende: Hell-/Dunkelgrau Min/Max der Spalten

Tabelle 4.5.: Vergleich Gesamtumsetzung technische und organisatorische Maßnahmen

Auch die Annahme, dass viele organisatorische Maßnahmen erst in großen Unternehmen eingesetzt werden kann bestätigt werden. Hierbei sei auf die Ergebnisse in Hypothese XIV sowie insbesondere auf die in Hypothese XVI aufgeführten Ergebnisse verwiesen.

Hypothese XVI, dass KMU (alle Unternehmen <250 Mitarbeiterinnen und Mitarbeiter) insbesondere in Bezug auf organisatorisch Sicherheitsmaßnahmen schlechter aufgestellt sind als große Unternehmen, kann anhand der in den Tabelle 4.6 dargestellten Ergebnisse für Unternehmen <49 eindeutig bestätigt werden. Im Vergleich zu Unternehmen >1000 haben sie bei allen organisatorischen Maßnahmen eine niedrigere Umsetzungsrate und auch im Vergleich zu Unternehmen 250-999 weisen sie nur bei drei der

Maßnahmen eine leicht höhere Umsetzungsrate auf, während sich bei allen anderen Maßnahmen eine niedrigere Umsetzungsrate zeigt.

Auch Unternehmen der Kategorie <250 weisen im Vergleich zu Unternehmen >1000 bei allen organisatorischen Maßnahmen eine geringere (bzw. bei einer Maßnahme gleich hohe) Umsetzungsrate auf, während sich beim Vergleich mit Unternehmen 250-999 schon einige Maßnahmen zeigen, bei denen die Unternehmen <250 eine höhere Umsetzungsrate aufweisen, wobei bei der absoluten Mehrheit der Maßnahmen die Unternehmen 250-999 noch besser aufgestellt sind.

Diese Feststellung gilt jedoch nicht nur für organisatorische Maßnahmen. Auch bei den technischen Maßnahmen ist, wie in Tabelle 4.7 ersichtlich, ein eindeutiger Trend erkennbar, dass mit der Unternehmensgröße die Umsetzungsrate gewisser Maßnahmen teilweise deutlich steigt. Generell ist dieser Trend meist aber nicht ganz so stark ausgeprägt wie bei den organisatorischen Maßnahmen, was auch darauf zurückzuführen ist, dass bei den technischen Maßnahmen mehrere Maßnahmen beinahe durchgängig umgesetzt sind.

Natürlich muss bei all diesen Auswertungen nach Unternehmensgröße immer berücksichtigt werden, dass die oft höheren Umsetzungsraten und „besseren“ Ergebnisse nicht unbedingt in einem direkten Zusammenhang (Ursache –> Wirkung) zur Unternehmensgröße alleine stehen müssen (eher besteht eine gewisse Korrelation). Bei den großen Unternehmen ist etwa auch - wie in Hypothese X (siehe Abbildung 4.55) beschrieben - die Nutzung von Standards (etwa ISO 27002) weiter verbreitet, welche sich ebenfalls sehr stark auf die organisatorische und technische Aufstellung der Unternehmen auswirken kann. Auch in Tabelle 4.6 ist etwa ersichtlich, dass bei den kleinen Unternehmen knapp ein Viertel angab, ein ISMS zu betreiben, während dies beinahe drei Viertel der Unternehmen >1000 angaben, was wiederum ebenfalls dafür spricht, dass diese Unternehmen besser aufgestellt sind.

Der tatsächliche Implementierungsgrad der organisatorischen und technischen Maßnahmen in spezifischen Unternehmen wird neben der Unternehmensgröße jedenfalls ebenfalls von Faktoren wie dem allgemeinen Bewusstsein für Informationssicherheit, dem Stellenwert bzw. der Notwendigkeit dieser im Unternehmenskontext, sowie der Nutzung von Standards etc. abhängig sein.

Anmerkung: (*)Die Prozentwerte in den Tabellen 4.6, 4.7 und 4.4 beziehen sich immer auf die Anzahl der Beantwortungen je Maßnahme (diese sind bei zwei der Tabellen aus Platzgründen nicht aufgeführt). Hierbei wird durch die Nutzung von Prozentwerten die in 4.2.5 beschriebene Problematik ignoriert(dadurch, dass bei allen Maßnahmen die Beantwortungen optional waren, kann nicht mit Sicherheit gesagt werden, ob bei Maßnahmen, die weniger absolute Beantwortungen bekommen haben, dies darauf zurückzuführen ist, dass sie gar nicht bekannt sind und die „fehlenden“ Beantwortungen als „nicht vorhanden“ gewertet werden hätten müssen). Während ein Vergleich der Prozentwerte je Unternehmensgröße innerhalb einer Maßnahme zulässig ist, ist ein Vergleich der Prozentwerte unterschiedlicher Maßnah-

men nicht unbedingt aussagekräftig und sollte, wenn überhaupt, eher als Richtwert angesehen werden.

Organisatorische Maßnahmen	1-49	50-249	250-999	>1000
Betrieb eines ISMS	25,58%	50,00%	56,41%	72,62%
Betrieb eines IKS inklusive IT Kontrollen	19,05%	37,50%	40,54%	64,63%
Audits/Penetration Tests/Vulnerability Scans	52,38%	65,38%	71,05%	89,29%
Risikomanagement	54,55%	69,23%	68,42%	87,06%
BCM und BIA/ Notfallplanung/-vorsorge	39,53%	73,08%	52,78%	73,17%
Personal Management	44,44%	64,00%	56,76%	80,00%
Awareness Aktivitäten	45,45%	57,69%	74,36%	76,19%
Vulnerability Management	40,91%	61,54%	62,16%	70,37%
Change Management	56,82%	73,08%	86,84%	89,29%
Configuration/ Capacity Management	51,11%	65,38%	70,27%	75,00%
Physische Sicherheit	73,33%	92,31%	89,47%	96,51%
Asset Management	45,45%	64,00%	71,05%	81,93%
Informationsklassifikation und -Verarbeitung	40,00%	38,46%	56,76%	69,88%
Identitäts- und Zugriffsmanagement	67,44%	69,23%	75,68%	88,51%
Vorfallmanagement	31,82%	50,00%	66,67%	76,54%
Patch & Update Management	85,71%	92,31%	81,58%	95,29%
Backup & Wiederherstellung	93,33%	96,15%	100,00%	98,84%
Logging & (Performance) Monitoring	66,67%	80,77%	64,86%	80,95%
Spam & Antivirus	93,33%	100,00%	97,30%	100,00%
Medien-Datenvernichtung	77,78%	91,67%	78,38%	95,24%
Management der Leistungserbringung/Verträge Externe IT Dienstleister	40,48%	65,38%	63,16%	79,27%
Dokumentation (Systeme, Konfigurationen, Organisatorische Prozesse etc.)	78,26%	76,92%	79,49%	86,75%
Sichere Software-/Webapplikationsentwicklung	45,65%	40,00%	48,65%	52,63%
Versicherung gegen Cyber/IT-Angriffe	6,82%	8,33%	2,86%	14,29%
Firmeneigenes CERT	20,93%	23,08%	22,22%	46,75%
Durchführung/Teilnahme an Cyber Übungen	21,43%	12,00%	30,56%	43,84%
Anzahl Beantwortungen bis zu (*4.3)	***46***	***26***	***39***	***88***
Legende: Hell-/Dunkelgrau Min/Max der Zeilen				

Tabelle 4.6.: Umsetzung organisatorische Maßnahmen nach Unternehmensgröße

Technische Maßnahmen	1-49	50-249	250-999	>1000
Firewall(s)	95,83%	100,00%	100,00%	100,00%
Virenschutz/Malware Scanner	93,48%	100,00%	100,00%	100,00%
IDS/IPS	48,89%	61,54%	59,46%	76,83%
Web Content Inspection/ -Filtering /Monitoring	50,00%	79,17%	89,74%	89,29%
Monitoring Software	75,56%	88,00%	80,49%	88,24%
SIEM	14,63%	30,43%	16,22%	36,11%
E-Mail Verschlüsselung & Signatur	53,33%	52,00%	45,95%	76,25%
E-Mail Malware Scans	91,49%	92,31%	97,44%	95,40%
Spamschutz	95,65%	92,31%	100,00%	100,00%
DLP	23,08%	25,00%	20,00%	44,59%
VPNs	88,64%	100,00%	95,00%	97,70%
Netzwerk Segmentierung	79,07%	88,46%	90,24%	82,35%
Layer 2 Netzwerksicherheit	42,22%	72,00%	84,62%	75,95%
Web Application Firewalls	46,67%	44,00%	71,05%	67,07%
DDOS Protection	39,13%	36,00%	48,48%	58,11%
Vulnerability Mgmt. Tools	36,36%	54,17%	40,54%	65,33%
Verschlüsselungstechnologien	78,26%	80,00%	81,08%	94,05%
Backupsoftware	93,62%	100,00%	100,00%	100,00%
Patch Mgmt Software	71,11%	80,00%	91,67%	94,05%
Log Management Software	45,45%	65,38%	51,43%	66,25%
(Security) Configuration Management Software	34,88%	33,33%	38,24%	55,84%
Mobile Device Management Software	29,55%	48,00%	65,00%	73,49%
OS und Server Hardening	65,91%	54,17%	66,67%	75,64%
Client Sicherheit	81,82%	88,00%	84,21%	91,67%
Zwei Faktor Authentifizierung	45,45%	69,23%	65,79%	81,71%
PKI-Public Key Infrastruktur	55,56%	61,54%	60,00%	78,48%
MSSP-Managed Security Service Provider	7,14%	12,00%	5,88%	21,21%
Anzahl Beantwortungen bis zu (*4.3)	***48***	***26***	***42***	***89***
Legende: Hell-/Dunkelgrau Min/Max der Zeilen				

Tabelle 4.7.: Umsetzung technische Maßnahmen nach Unternehmensgröße

4.4. Schlüsse und Interpretation

Hier sollen nun auf die in Kapitel 1.3 aufgestellten forschungsleitenden Fragestellungen eingegangen werden.

- Wie ist das Bewusstsein in deutschen, Schweizer und österreichischen Unternehmen und Organisationen in Bezug zur Informationssicherheit, was ist deren Stellenwert und wie lässt sich die derzeitige Situation beschreiben?

Besonders in Hinblick auf die im Kapitel 4.2.1 beschriebenen Ergebnissen der Grundsatzfragen lässt sich festhalten, dass das Thema der Informationssicherheit für die meisten der teilnehmenden Unternehmen von großer bis sehr großer Bedeutung ist. Außerdem zeigt sich, dass sich eine große Mehrheit der Wichtigkeit von korrekten Daten und Informationen sowie der Abhängigkeit von der eigenen IT bewusst ist.
Im Hinblick auf die Wichtigkeit der Informationssicherheit in den Unternehmen antworteten über 35%, dass dieses Thema für sie „sehr wichtig“ sei und in allen wesentlichen Geschäftsprozessen einen definierten, integralen Bestandteil darstellt, während weitere 40% die Informationssicherheit als „wichtiges“ Thema sahen, für welches eine dedizierte Rolle verantwortlich ist. Knapp etwas mehr als ein Fünftel empfanden die Informationssicherheit als „weniger wichtiges“ Thema, welches hauptsächlich in der IT angesiedelt ist, und lediglich für ein einziges der teilnehmenden Unternehmen stellt Informationssicherheit ein „unwichtiges oder nebensächliches“ Thema dar, welches keine besondere Beachtung findet.
Zu der Wichtigkeit von Daten und Informationen für das Kerngeschäft der Unternehmen und den möglichen Auswirkungen eines Verlustes, Nichtverfügbarkeit oder Verfälschung bzw. einer Veröffentlichung dieser (etwa an Mitbewerber) gaben etwas mehr als die Hälfte der Unternehmen an, dass bei solchen Vorfälle mit „sehr hohen“ Auswirkungen auf das Kerngeschäft zu rechnen sei (schwerwiegenden Imageschäden, Know-How Verluste, Geldverluste, rechtliche Konsequenzen und langfristige Auswirkungen auf die Neukunden- bzw. Auftragsgewinnung). Ein weiteres Viertel rechnete in solchen Fällen mit „hohen“ Konsequenzen auf das Geschäft, während nur 17,6% bzw. 4% der Teilnehmerinnen und Teilnehmer „lediglich spürbare“ bzw. „geringe“ Konsequenzen befürchteten.
Bezüglich der Abhängigkeit von IT antworteten knapp 89% der Unternehmen „sehr stark“ oder „stark“ von der eigenen IT abhängig zu sein, wodurch bereits bei einem Ausfall von Kernsystemen für wenige Stunden oder einem Tag das Kerngeschäft dieser Unternehmen stark negativ beeinträchtigt oder unmöglich gemacht werden würde. Lediglich 11% der Unternehmen gaben an „nur in Teilbereichen“ oder nur in „geringem Ausmaß“ von der eigenen IT abhängig zu sein.

Die aktuelle Situation der Informationssicherheit (Nutzung von Standards, Motivation, Vorfälle, Risiken, Probleme, Überprüfungsaktivitäten etc.) wird in der Auswertung ab Kapitel 4.2.2 beschrieben, doch es lässt sich schon anhand der Tatsache, dass lediglich eine Minderheit von knapp 11% angab, im vergangenen Jahr von keinen Informationssicherheits-Vorfällen betroffen gewesen zu sein drauf schließen, dass durchaus noch viel Handlungsbedarf in diesem Bereich besteht.
Wie bereits an mehreren Stellen erwähnt (siehe Kapitel 4.5 und Anmerkung 4.2) ist es äußerst wahrscheinlich, dass die meisten Teilnehmerinnen und Teilnehmer dieser Umfrage ein höheres Bewusstsein und Interesse für das Thema der Informationssicherheit haben und hierin besser aufgestellt sind als ein „typisches durchschnittliches Unternehmen“ dies ist. Daher ist es möglich und wahrscheinlich, dass die Gesamtsituation der Informationssicherheit in Deutschland, Österreich und der Schweiz, verglichen mit den in dieser Studie aufgeführten Ergebnissen und Schlüssen, „anders“ bzw. „schlechter“ sein könnte, als durch die Ergebnisse hier nahegelegt wird.

- Welche technischen und organisatorischen Maßnahmen werden von Unternehmen und Organisationen im Bezug zur Informationssicherheit getroffen?

Bezüglich technischer und organisatorischer Maßnahmen, welche von Unternehmen im Bezug zur Informationssicherheit getroffen werden, kann zusammengefasst werden, dass bei der technischen Aufstellung grundlegende wichtige Sicherheitstools (wie Firewalls, Virenschutz, Backupsoftware, Spamschutz, E-Mail Malware Scans und VPNs) beinahe durchgängig vorhanden sind, wobei sich in Bezug auf weiterreichende oder speziellere Maßnahmen ein gespaltenes Bild mit teilweise schnell sinkendem Implementierungsgrad zeigt. Einige technisch komplexe und aufwändige Maßnahmen (wie DLP, SIEM oder auch (Security) Configuration Management Software) sind nur bei einer Minderheit der Befragten im Einsatz.
Zu der organisatorischen Aufstellung ist zu sagen, dass sich im Vergleich zu den technischen Maßnahmen ein nicht so „offensichtliches“ Bild zeigt und nur wenige Maßnahmen (Spam & Antivirus, Backup und Wiederherstellung) beinahe durchgängig vorhanden sind. Zwar gib es auch weitere organisatorische Maßnahmen, welche verbreitet genannt wurden (Physische Sicherheit, Patch & Update Management, Medien-/Datenvernichtung, Dokumentation oder Change Management), doch gibt es auch hier schon einige Unternehmen, bei denen diese Maßnahmen nicht vorhanden oder in Planung waren. Generell gib es kaum organisatorische Maßnahmen, die hinsichtlich ihrer Verbreitung so eindeutig wie einige technische Systeme hervorstechen. Einige aufwändige bzw fortgeschrittene organisatorische Maßnahmen wie „Versicherung gegen Cyber/IT-Angriffe“, „Firmeneigenes CERT“, „Durchführung/Teilnahme an Cyber Übungen“ oder der „Betrieb eines IKS inklusive IT-Kontrollen“ sind nur bei einer Minderheit der Unternehmen umgesetzt.

Grundsätzlich kann auch festgehalten werden, dass die technische Aufstellung der Unternehmen oft etwas besser als die organisatorische Aufstellung ist (siehe Kapitel 4.2.5 und 4.2.5 sowie Hypothese XV in Kapitel 4.3).

- Gibt es länderabhängig große Unterschiede bezüglich Stellenwert und Aufstellung in Bezug zur Informationssicherheit zwischen Unternehmen in Österreich, Deutschland und der Schweiz?

Zu länderabhängigen Unterschieden bezüglich Stellenwert und Aufstellung in Bezug zur Informationssicherheit kann festgehalten werden, dass der Anteil der Unternehmen, für die die Informationssicherheit ein sehr wichtiges Thema ist, bei den Teilnehmerinnen und Teilnehmern aus Deutschland, Österreich und der Schweiz mit je etwas über einem Drittel beinahe gleich hoch ist, während in Deutschland mit knapp 45% im Vergleich mit der Schweiz und Österreich etwas mehr Unternehmen angaben, dass es sich bei der Informationssicherheit für sie um ein wichtiges Thema handelt. Dementsprechend war auch der Anteil der deutschen Unternehmen, die in der Informationssicherheit lediglich ein IT Thema sehen, mit unter 20% im Ländervergleich am geringsten.
In einigen Fragen wie zum Beispiel der Nutzung von Standards, in den Unternehmen umgesetzte Richtlinien, Informationssicherheits-Überprüfungsaktivitäten, dem Einsatz von mobilen Geräten oder der Nutzung von Cloud und Outsourcing gibt es durchaus Unterschiede in den Antworten der Teilnehmerinnen und Teilnehmer aus der Schweiz, Deutschland und Österreich, wobei die Antworten von Unternehmen aus Deutschland und der Schweiz meist etwas „sicherheitsbewusster bzw. stärker in diverse Informationssicherheitsaktivitäten involviert“ erscheinen.
Zur Aufstellung der Unternehmen in Bezug zur Informationssicherheit kann bei den technischen Maßnahmen festgehalten werden, dass in der Schweiz tendenziell am wenigsten nicht implementierte Maßnahmen vorhanden sind, während Deutschland etwas mehr und Österreich den größten Anteil solcher Maßnahmen aufweist, wobei diese Feststellung jedoch hauptsächlich für die technisch „fortgeschritteneren“ Systeme zutrifft, da sich bei grundlegenden wichtigen Sicherheitstools (wie Firewalls, Virenschutz, Backupsoftware, Spamschutz) über alle Länder hinweg ein einheitlich sehr hoher Implementierungsgrad zeigt.
Bei der organisatorischen Maßnahmen fällt abermals auf, dass in der Schweiz tendenziell am wenigsten nicht implementierte Maßnahmen vorhanden sind, wobei der Unterschied zwischen der Schweiz und Deutschland aber nicht so eindeutig sichtbar wie zuvor bei den technischen Maßnahmen ist und es auch einige Maßnahmen gibt, bei denen Deutschland eine höhere Umsetzungsrate aufweist. Im Vergleich weist Österreich abermals den größten Anteil an nicht implementierten Maßnahmen auf.
Es ist jedoch anzumerken, dass einige dieser Unterschiede auch teilweise darauf zurückzuführen sein können, dass in Österreich im Vergleich zu Deutschland und der Schweiz relativ viele kleine Unter-

nehmen an der Umfrage teilnahmen, während in der Schweiz sehr viele Unternehmen mit mehr als 1000 Abgestellten antworteten. Auch auf Grund der Tatsache, dass bei den kleinen Unternehmen Informationssicherheitsmanagementsysteme viel weniger weit verbreitet sind (siehe Tabelle 4.6 können verschieden Unterschiede in der länderspezifischen Auswertung erklärbar sein.

4.5. Limitations of Validity

Im folgenden Unterkapitel soll auf Faktoren, welche sich auf die Aussagekraft dieser Studie (und Studien im Allgemeinen) auswirken und diese beschränken können, aufmerksam gemacht werden. Grundsätzlich ist festzuhalten, dass „freie bzw. offene Umfragen“ (bei denen keine spezielle Verfahren zur Stichprobenauswahl eingesetzt werden) nicht unbedingt das ideale Werkzeug sind, um genaue, repräsentative und unverzerrte Daten zu erheben, da bei ihnen immer ein gewisser „Self Selection Bias“ vorhanden ist.
Zu dem „Self Selection Bias“ kommt es, „wenn die im Rahmen einer Stichprobe untersuchten Personen nicht durch ein zufälliges oder systematisches Stichprobenverfahren selektiert werden, sondern selbst die Entscheidung treffen, zu der Stichprobe zu gehören“ [60, o. S.]. Es wird beschrieben, dass „Selbstselektion [...] im Vergleich zu Zufallsauswahlverfahren dazu [führt, d. Verf.], dass die Stichprobe nicht repräsentativ ist und Rückschlüsse auf die Eigenschaften der Grundgesamtheit daher nur in eingeschränktem Maße zulässig sind“ [60, o. S.].
Die Selbstselektion ist insbesondere ein „Problem, wenn zwischen den Teilnehmern und Nicht-Teilnehmern einer Befragung systematische Unterschiede existieren, d.h. wenn sich Teilnehmer und Nicht-Teilnehmer in wichtigen, für die Untersuchung relevanten Merkmalen unterscheiden“ [60, S. 7]. Da die durchgeführte Arbeit sehr stark auf das Thema Informationssicherheit fokussiert ist, muss davon ausgegangen werden, dass so eine spezifische Umfrage meist von Unternehmen beantwortet wird, die einen gewissen Bezug zur IT-/Informationssicherheit haben und sich durch eine gewisse Technik/IT-Affinität auszeichnen.
Daher muss berücksichtigt werden, dass diese Unternehmen bei Merkmalen wie Bewusstsein und der Umsetzung diverser Maßnahmen wahrscheinlich besser aufgestellt sind als „ein typisches Unternehmen der Grundgesamtheit“. Außerdem wurden bei der Verteilung diverse Organisationen und Gemeinschaften genutzt, deren Mitglieder an Informationssicherheit interessiert sind und sich mit diesem Thema befassen (sonst wären sie keine Mitglieder dieser Gruppen). Auch diese Tatsache unterstützt die Annahme, dass die meisten Teilnehmerinnen und Teilnehmer dieser Umfrage ein höheres Bewusstsein für das Thema der Informationssicherheit haben als „ein typisches Unternehmen der Grundgesamtheit“.
Es muss weiters festgehalten werden, dass nur eine relativ kleine Stichprobe erhoben werden konnte (obwohl diese im Vergleich zu anderen deutschen und österreichischen Informationssicherheitsstudien oft

nicht sehr viel kleiner ist), auf deren Basis repräsentative Schlüsse auf die Gesamtsituation der Informationssicherheit in den Ländern Deutschland, Österreich und der Schweiz nicht möglich und nicht zulässig sind. Es muss jedoch angemerkt werden, dass es auch diverse Beispiele dafür gibt, dass große Stichproben alleine zu keiner höhere „Repräsentativität“ führen, da insbesondere das zur Bildung der Stichproben verwendete Auswahlverfahren sowie die Zusammensetzung der Stichprobe selbst hohe Bedeutung haben [61, o. S.].

Weiters muss auch berücksichtigt werden, dass die Unternehmen die Antworten ohne Unterstützung abgegeben haben und somit die Möglichkeit besteht, dass sich gewisse Teilnehmerinnen und Teilnehmer bei Fragen über- oder unterschätzt oder inkorrekte Angaben gemacht haben.

Aufgrund dieser Faktoren und Einschränkungen ist eine gewisse Verzerrung der Ergebnisse (Über-/Unterrepräsentation von Unternehmen gewisser Größe/Branche bzw. IT-Affinität & Sicherheitsbewusstsein etc.) möglich und wahrscheinlich. Die Gesamtsituation der Informationssicherheit in Deutschland, Österreich und der Schweiz könnte, verglichen mit den in dieser Studie aufgeführten Ergebnissen und Schlüssen, „anders“ bzw. „schlechter“ sein, als hier nahegelegt wird.

Trotz der oben beschriebenen Einschränkungen ist es möglich, zumindest in Bezug auf die teilnehmenden Unternehmen den aktuellen Stand der Informationssicherheitssituation zu beschreiben und Vergleiche mit anderen Studien im Bereich der Informationssicherheit zu ziehen. Weiters bieten die Ergebnisse dieser Studie zumindest eine interessante und fundierte Diskussionsgrundlage und könnten außerdem sehr gut im Rahmen umfangreicher Studien überprüft werden.

Weitere Quellen, in denen mögliche Faktoren bezüglich der Einschränkungen der Aussagekraft von Informationssicherheitsstudien beschrieben werden, sind etwa die Diplomarbeit zur Informationssicherheit in österreichischen klein- und mittelständischen Unternehmen [24, S. 62, S. 76], die Computer Crime and Security Survey [20, S. 3] und insbesondere die MELANI Studie zu Informationssicherheit in Schweizer Unternehmen [62, S. 11, S. 43ff] in der sehr genau auf die Qualität und Gewichtung der Stichprobe eingegangen wird. Eine sehr gute Behandlung der unterschiedlichen in Umfragen möglichen Fehlerarten und insbesondere der Probleme bei „Verlust-Schätzungen“ in diversen „Cybercrime-Surveys“ findet sich in [63, o. S.].

Generell ist die „Repräsentativität“ (dieser Begriff ist teilweise sehr umstritten und es gibt sehr viele unterschiedliche Definitionen und Auffassungen dazu, was tatsächlich unter Repräsentativität zu verstehen ist geschweige denn, wie sie zu erreichen ist) von Studien und Stichproben ein sehr umfangreiches und komplexes Themengebiet, auf welches hier nicht näher eingegangen werden soll. Gute Informationen hierzu findet man etwa unter [64, o. S.] oder auch auf der Seite der Wirtschaftspsychologische Gesellschaft [65, o. S.].

Bezüglich der länderspezifischen Auswertung und den Vergleich der Ergebnisse muss noch darauf hingewiesen werden, dass die Stichproben für die Länder unterschiedlich groß und unterschiedlich zusammengesetzt sind, wodurch eine direkte Vergleichbarkeit nur bedingt gegeben ist. Diverse Unterschiede können auch teilweise darauf zurückzuführen sein, dass in Österreich im Vergleich zu Deutschland und Schweiz relativ viele kleine Unternehmen an der Umfrage teilnahmen, während in der Schweiz sehr viele Unternehmen mit mehr als 1000 Abgestellten antworteten. Auch auf Grund der Tatsache, dass bei den kleinen Unternehmen viel weniger angaben ein ISMS zu betreiben (wodurch ein gewisses organisatorisches und technisches Niveau erwartet werden kann), während dies beinahe drei Viertel der Unternehmen >1000 taten (siehe Tabelle 4.6) können diverse Unterschiede in der länderspezifischen Auswertung erklärbar sein.

4.6. Alle Ergebnisse

Die Detailergebnisse aller Fragen, in denen sowohl die gesamten, als auch die länderspezifischen Beantwortungen angeführt sind, sind im Anhang in Kapitel A.3 ersichtlich.

5. Ergebniszusammenfassung, Erfahrungen und Überlegungen & Ausblick

In diesem abschließenden Kapitel werden nochmals kurz die wichtigsten Ergebnisse und die Durchführung meiner Studie zusammengefasst und ein Ausblick zu möglichen Folgestudien gegeben. Außerdem werden einige eigene Erfahrungen bezüglich der Durchführung der Umfrage sowie Hinweise und Überlegungen zu möglichen Vertiefungen bzw. Erweiterungen der Studie dargelegt. Schlussendlich folgt die Beschreibung einiger Rückmeldungen von Teilnehmerinnen und Teilnehmer.

5.1. Ergebniszusammenfassung

Im Rahmen der in dieser Diplomarbeit durchgeführten Studie zum Thema Informationssicherheit in Unternehmen und Organisation in Deutschland, Österreich und der Schweiz wurden in einer Online-Umfrage mit 21 fachspezifischen Fragen 229 Teilnehmerinnen und Teilnehmer zu der Informationssicherheitssituation in ihrem Unternehmen befragt (56 Deutschland, 82 Österreich, 65 Schweiz, 26 sonstige). Im Folgenden werden einige der wichtigsten Ergebnisse beschrieben.

Im Teilnehmerfeld befanden sich Unternehmen unterschiedlicher Größe. 21,4% der Unternehmen waren klein Unternehmen mit 1-49 Angestellten. 12% der Unternehmen hatten zwischen 50 und 249 Angestellten, während weitere 12,2 % 250-999 Menschen beschäftigten. 39% der teilnehmenden Unternehmen waren große Unternehmen und hatten mehr als 1000 Angestellte (siehe 4.2)

Die Umfrage wurde in 5 große Teilbereiche gegliedert, in denen verschiedene organisatorische und technische Aspekte der Informationssicherheit sowie einige „Trendthemen“ wie mobile Geräte und BYOD, Cloud Computing und Outsourcing sowie APTs behandelt wurden. Außerdem wird auf die Verwendung von Open Source Software und die Betroffenheit von schweren Sicherheitslücken in dieser sowie die Bedeutung (und Konsequenzen) der NSA Enthüllungen eingegangen.

Neben einigen allgemeinen Fragen zur Informationssicherheit selbst und Vorfällen sowie Risiken in diesem Gebiet wurde auch erhoben, wie das Bewusstsein der Unternehmen bezüglich der Abhängigkeit von der eigenen IT und der Schutzwürdigkeit von verarbeiteten Daten und Informationen aussieht, welche technischen und organisatorischen Maßnahmen derzeit umgesetzt werden und welche Maßnahmen in Zukunft implementiert werden sollen.

Aufgrund der Ergebnisse der durchgeführten Umfrage lässt sich festhalten, dass das Thema der Informationssicherheit für die meisten der teilnehmenden Unternehmen von großer bis sehr großer Bedeutung ist. Außerdem zeigt sich, dass sich eine große Mehrheit der Wichtigkeit von korrekten Daten und Informationen sowie der Abhängigkeit von der eigenen IT bewusst ist.

So antworteten 35%, dass die Informationssicherheit für sie „sehr wichtig“ sei und in allen wesentlichen Geschäftsprozessen einen definierten, integralen Bestandteil darstellt, während weitere 40% die Informationssicherheit als „wichtiges“ Thema sahen, für welches eine dedizierte Rolle verantwortlich ist. Knapp mehr als ein Fünftel empfand die Informationssicherheit als „weniger wichtiges“ Thema, welches hauptsächlich in der IT angesiedelt ist und lediglich für ein einziges der teilnehmenden Unternehmen stellt Informationssicherheit ein „unwichtiges oder nebensächliches“ Thema dar, welches keine besondere Beachtung findet (siehe Abbildung 4.8).

Konsistent mit der Einschätzung der Wichtigkeit der Informationssicherheit selbst gaben etwas mehr als die Hälfte der Unternehmen an, dass bei Verlust, Nichtverfügbarkeit, Verfälschung oder Weitergabe (etwa an Mitbewerber oder unautorisierte Dritte) von wichtigen Unternehmens-Informationen mit „sehr hohen“ Auswirkungen auf das Kerngeschäft zu rechnen sei (schwerwiegenden Imageschäden, Know-How Verluste, Geldverluste, rechtliche Konsequenzen und langfristige Auswirkungen auf die Neukunden- bzw. Auftragsgewinnung). Ein weiteres Viertel erwartete in solchen Fällen „hohen“ Konsequenzen für das eigene Geschäft, während nur knapp über 20% der Teilnehmerinnen und Teilnehmer mit „lediglich spürbaren“ bzw. „geringen“ Konsequenzen rechneten (siehe Abbildung 4.6).

Weiters antworteten knapp 89% der Unternehmen „sehr stark“ oder „stark“ von der eigenen IT abhängig zu sein, wodurch bereits bei einem Ausfall von Kernsystemen für wenigen Stunden oder einem Tag das Kerngeschäft stark negativ beeinträchtigt oder unmöglich gemacht werden würde. Lediglich 11% der Unternehmen gaben an „nur in Teilbereichen“ oder nur in „geringem Ausmaß“ von der eigenen IT abhängig zu sein (siehe Abbildung 4.4).

Generell gibt es für Unternehmen viele unterschiedliche Gründe, sich mit dem Thema Informationssicherheit auseinanderzusetzen. Die wichtigsten sind „Gesetzliche Vorgaben (Datenschutz, EU-Richtlinien) /Compliance“ (80%), die „Vermeidung von (Geld/Image)Verlusten durch Sicherheitsvorfälle oder Datenpannen“ (71%), die Vorbeugung von „Datenverlusten/Verfälschung“ (69%) sowie die „starke Abhängigkeit von eigener IT in gewissen Geschäftsprozessen„ (55%). Das NSA-Überwachungsskandal hingegen wurde lediglich von 3% genannt (siehe Abbildung 4.10).

Als Hauptprobleme bei der Aufrechterhaltung & Verbesserung der Informationssicherheit wurden „fehlendes Budget“ (54,0%), „fehlende Unterstützung und Bewusstsein (z.B. zu Risiken und Gefahren) im (Top)Management“ (54,5%), „fehlendes Bewusstsein der Mitarbeiter“ (66,1%), „fehlende Mitarbeiter-

Akzeptanz für Sicherheitsmaßnahmen, die die Usability/Benutzbarkeit einschränken“ (65,2%) sowie „sich schnell ändernde Systemumgebung und Angriffsarten“ (42,0%) genannt (siehe Abbildung 4.16).
Hinsichtlich Risiken und Bedrohung in Bezug zur Informationssicherheit, denen sich Unternehmen ausgesetzt fühlen, wurden „Malware (Viren, Trojaner, Spyware etc.)“ (57%), „Datendiebstahl“ (49%), „Fahrlässigkeit eigener Mitarbeiter“ (39%), „Datenverluste“ (34%) sowie „APTs“ (30%) und „Social Engineering“ (30%) am häufigsten genannt (siehe Abbildung 4.14).
Zu den grundlegenden organisatorischen Rahmenbedingungen ist festzuhalten, dass es in über drei Viertel der Unternehmen einen „Informationssicherheits-Verantwortlichen und eine Informationssicherheits-Policy“ gibt. In knapp 15% der Unternehmen gab es zwar eine verantwortliche Person, jedoch ohne unternehmensweite Richtlinie zur Informationssicherheit und lediglich in 10% der Unternehmen war weder die Verantwortung, noch eine Richtlinie definiert (siehe Abbildung 4.18).
Bei der Nutzung von Standards und Empfehlungen im Bereich der Informationssicherheit, werden wie zu erwarten „ISO 27001“ (69,1%), „BSI - IT-Grundschutz“ (52,3%), „ITIL“ (49,1%) und „COBIT“ (26,4%) am häufigsten genannt. Der „BSI - Grundschutz kompakt“ (31,8%) sowie die „OWASP Top 10“ (32,7%) werden ebenfalls verbreitet genutzt. Auch die relativ neuen „SANA Critical Security Controls“ fanden bei 10,9% der Unternehmen Anwendung. Lediglich 12,7% der Unternehmen geben an, „keine speziellen Standards oder Empfehlungen“ im Bereich der Informationssicherheit zu verwenden (siehe Abbildung 4.12).
Lediglich eine Minderheit von 11% gab an, im vergangenen Jahr von keinen Informationssicherheits-Vorfällen betroffen gewesen zu sein. Dies bedeutet, dass beim Großteil von knapp 89% der Unternehmen, im letzten Jahr zumindest ein Vorfall im Bereich der Informationssicherheit aufgetreten war. Mit knapp 54% gaben mehr als die Hälfte der Unternehmen an, dass sie von „Malware (Viren, Trojaner, Spyware etc.)“ betroffen waren, während als zweithäufigste Vorfallsart „Spam“ von 46% genannt wurde. Auch die „Fahrlässigkeit von Mitarbeitern“ (28%), „Hardware- oder Software-Fehler“ (28%), „Stromausfälle“ (25%) sowie „(Spear)Phishing“ (21%) wurden häufig aufgeführt. Mit Hacking oder D(DOS) Angriffen waren anscheinend nur relativ wenige Unternehmen konfrontiert (9% bzw. 15%) (siehe Abbildung 4.26).
Ein Großteil von 43% der Unternehmen gab an „Cloud und/oder Outsourcing zu nutzen und dabei spezifische Sicherheitsmaßnahmen umgesetzt“ zu haben. Weitere 11% gaben zwar an im Bereich von „Cloud und Outsourcing aktiv zu sein, jedoch ohne Informationssicherheitsaspekte speziell zu berücksichtigen“. 15% der verbleibenden Unternehmen erklärten Cloud und Outsourcing „aufgrund von Sicherheitsbedenken und diverser Vorkommnisse (NSA-Skandal etc.)“ nicht zu nutzen, während weitere 30% keine speziellen Gründe für den Nichteinsatz von Cloud oder das Outsourcing von IT-Dienstleistungen nannten (siehe Abbildung 4.30).

Bezüglich des Einsatzes von Open Source Software gaben lediglich 12% der Unternehmen an „keine Open Source Software“ zu nutzen und nur ein einziges Unternehmen (bei 217 Antworten) gab an „Open Source Software aufgrund von Sicherheitsbedenken nicht einzusetzen“. Die absolute Mehrheit von 58% der Unternehmen setzten Open Source Software ein, jedoch ohne eine (Sicherheits-)Überprüfung dieser durchzuführen. Immerhin ein knappes Viertel nutzen Open Source Software und trafen dabei Maßnahmen wie „Durchführung von Code Reviews und Recherche zu Auditergebnissen, Sicherheitsanalysen und dem Entwicklerkreis“, um deren Sicherheit, Qualität und Vertrauenswürdigkeit zu überprüfen (siehe Abbildung 4.34).

Hinsichtlich der Betroffenheit von schwerwiegenden Sicherheitslücken in Open Source Software wie Heartbleed und Shellshock gaben, knapp 60% an, dass sie zwar von diesen Lücken betroffen gewesen waren, dass es jedoch zu keiner „Beeinträchtigung der Geschäftstätigkeiten“ gekommen sei (etwa durch Nichtverfügbarkeit wichtiger Dienste und außerplanmäßige Wartungsfenster für die Einspielung notwendiger NotfallPatches). Nur 5% der Unternehmen gaben an, dass sie von den Lücken betroffen waren und ihre „Geschäftstätigkeit beeinträchtigt wurde“, während für 29,0% diese Lücken kein Problem darstellten. Lediglich ein einziges Unternehmen (bei 217 Antworten) gab an, dass bei ihm „diese Lücken aktiv für Angriffe auf das Unternehmen ausgenutzt wurden“ (siehe Abbildung 4.36).

Mit 56% geben knapp mehr als der Hälfte der Unternehmen an, dass sie im letzten Jahr nicht Ziel „eines komplexen, fortgeschrittenen, direkt auf sie gezielten IT-Angriffs (APT-Advanced Persistent Threat)“ waren. Mit 25% konnte knapp ein Viertel der Unternehmen auf diese Frage nur mit „weiß nicht“ antworten, während bei 5% zumindest ein Verdacht bezüglich des Auftretens eines APTs bestand. Dies bedeutet, dass bei knapp einem Drittel der Unternehmen Unsicherheit bzw. Unwissenheit bezüglich des Auftretens eines APT besteht („weiß nicht“ + „Verdacht“), was natürlich auch der Tatsache geschuldet ist, dass APTs schon ihrer Definition nach komplex und schwer zu identifizieren bzw. nachzuweisen sind. Lediglich ca. 12% erklärten, dass sie im vergangenen Jahr Ziel eines APTs waren, wobei nur bei einer Minderheit von 3% durch diesen auch tatsächlich ein Schaden entstand (siehe Abbildung 4.38).

Knapp 40% der Unternehmen gaben an, dass „die NSA-Enthüllungen bezüglich Überwachung und Spionage sowie der gezielten Manipulation von (amerikanischen) Soft- und Hardware-Produkten für sie kein Thema“ waren, während für 37% der Unternehmen diese Entwicklungen ein Thema waren und zu einer „wachsende Beachtung des Themas der Informationssicherheit“ geführt haben. Weitere 17% antworteten, dass die NSA-Enthüllungen „zwar ein Thema waren, jedoch keine gezielten Maßnahmen ergriffen wurden“. Bezüglich Maßnahmen werden der „verstärkter Einsatz von Verschlüsselung“ (16%), „Achtsamkeit, im Fall von Cloud oder Outsourcing wird verstärkt auf heimische/europäische Anbieter gesetzt“ (16%) sowie die „Planung zur verstärkten Beschaffung von IT Made in Austria/Germany/Switzerland

bzw. Europe“ (9%) genannt. Eine auf diese Enthüllungen folgende „Erhöhung des IT-Sicherheitsbudgets“ wurde von lediglich 2% der Unternehmen genannt (siehe Abbildung 4.40).

Generell fällt auf, dass sich trotz der umfassenden medialen Berichterstattung sehr viele Unternehmen dem Thema gegenüber „passiv“ Verhalten (knapp unter 60% der Unternehmen gaben entweder an das Thema nicht zu beachten oder keine gesonderten Maßnahmen daraus abzuleiten). Auch bei den 37% der Unternehmen bei denen es durch die NSA-Enthüllungen zu einer „wachsende Beachtung des Themas der Informationssicherheit“ kam muss hinterfragt werden, inwiefern nun zusätzliche Sicherheitsmaßnahmen umgesetzt werden.

Hinsichtlich der technischen Aufstellung der Unternehmen ist erkennbar, dass grundlegende wichtige Sicherheitstools (wie Firewalls, Virenschutz, Backupsoftware, Spamschutz) beinahe durchgängig vorhanden sind, wobei sich aber in Bezug auf weiterreichende oder speziellere Maßnahmen ein gespaltenes Bild mit teilweise schnell sinkendem Implementierungsgrad zeigt. Einige technisch komplexe und aufwändige Maßnahmen (wie DLP, SIEM oder auch (Security) Configuration Management Software) sind nur bei einer Minderheit der Befragten im Einsatz (siehe Diagramm 4.42)

Zu der organisatorischen Aufstellung kann festgehalten werden, dass einige Maßnahmen (Spam & Antivirus, Backup und Wiederherstellung) beinahe durchgängig vorhanden sind, während kaum andere Maßnahmen hinsichtlich deren Verbreitung so offensichtlich wie gewisse technische Maßnahmen hervorstechen. Zwar werden auch „Physische Sicherheit", „Patch & Update Management“, „Medien-/ Datenvernichtung“, „Dokumentation“ und „Change Management“ häufig genannt, doch gibt es auch Beantwortungen, dass diese „in Planung“ oder „nicht vorhanden“ sind. Einige organisatorische Maßnahmen wie „Versicherung gegen Cyber/IT-Angriffe“, „Firmeneigenes CERT“, „Durchführung/Teilnahme an Cyber Übungen“ oder der „Betrieb eines IKS inklusive IT-Kontrollen“ sind nur bei einer Minderheit der Unternehmen umgesetzt (siehe Diagramm 4.46).

Generell wird der Implementierungsgrad der zusätzlich zu den beinahe in allen Unternehmen vorhandenen technischen und organisatorischen Maßnahmen von Faktoren wie der Unternehmensgröße (Behandlung des Zusammenhangs siehe Tabellen 4.6 und 4.7), dem allgemeinen Bewusstsein für Informationssicherheit, dem Stellenwert bzw. der Notwendigkeit dieser im Unternehmenskontext sowie der Nutzung von Standards etc. abhängig sein.

In einigen Fragen wie zum Beispiel der Nutzung von Standards, in den Unternehmen umgesetzten Richtlinien, Informationssicherheits-Überprüfungsaktivitäten, dem Einsatz von mobilen Geräten, der Nutzung von Cloud und Outsourcing sowie der technischen und organisatorischen Aufstellung gibt es durchaus länderspezifische Unterschiede in den Antworten der Teilnehmerinnen und Teilnehmern aus der Schweiz, Deutschland und Österreich. Hierbei erscheinen die Antworten von Unternehmen aus Deutschland und

der Schweiz meist etwas „sicherheitsbewusster bzw. stärker in diverse Informationssicherheitsaktivitäten involviert“ (siehe div. länderspezifische Diagramme in Kapitel 4.2).
Es ist jedoch anzumerken, dass einige dieser Unterschiede auch teilweise darauf zurückzuführen sein können, dass in Österreich im Vergleich zu Deutschland und der Schweiz relativ viele kleine Unternehmen an der Umfrage teilnahmen, während in der Schweiz sehr viele Unternehmen mit mehr als 1000 Abgestellten antworteten. Auch auf Grund der Tatsache, dass bei den kleinen Unternehmen Informationssicherheitsmanagementsysteme viel weniger weit verbreitet sind (siehe Tabelle 4.6 können verschieden Unterschiede in der länderspezifischen Auswertung erklärbar sein.
Anmerkung: Aufgrund diverser Faktoren und Einschränkungen bei der Verteilung und Durchführung der Umfrage ist eine gewisse Verzerrung der Ergebnisse (Über-/Unterrepräsentation von Unternehmen gewisser Größe/Branche bzw. IT-Affinität & Sicherheitsbewusstsein etc.) möglich und wahrscheinlich (siehe Kapitel 4.5). Es ist davon auszugehen, dass die meisten Teilnehmerinnen und Teilnehmer dieser Umfrage ein höheres Bewusstsein und Interesse für das Thema der Informationssicherheit aufweisen und hierin besser aufgestellt sind als ein „typisches durchschnittliches Unternehmen“ dies ist.
Daher erhebt diese Studie keinen Anspruch auf Repräsentativität und die Gesamtsituation der Informationssicherheit in Deutschland, Österreich und der Schweiz könnte, verglichen mit den in dieser Studie angeführten Ergebnissen und Schlüssen „anders“ bzw. „schlechter“ sein, als hier nahegelegt wird.

5.2. Eigene Erfahrungen und Überlegungen

Grundsätzlich stellte die Verteilung der Umfrage eine große Herausforderung dar, und ohne die Unterstützung und Hilfe von verschiedenen Distributionspartnern mit vielen Kontakten kann nur schwer ein einigermaßen aussagekräftiger Stichprobenumfang erreicht werden. Meiner Erfahrung nach sollte schon möglichst früh im Design der Studie Kontakt zu möglichen Partnern aufgenommen werden, da auch bei diesen gewisse Vorlaufzeiten notwendig sind und auch die Abstimmung relativ arbeits- und zeitintensiv sein kann. Außerdem können durch eine frühe Kontaktaufnahme auch Fragebogen und Inhalte mit den Partnern abgesprochen und bei Bedarf angepasst werden.
Natürlich besteht auch die Möglichkeit selbst bzw. über private Kontakte zu einzelnen Unternehmen Kontakt aufzunehmen, wodurch relativ sicher Beantwortungen erzielt werden können. Dieses Vorgehen erfordert jedoch einen gewissen Aufwand und ist nur in geringem Umfang praktikabel.
Abermals wurden die Fragen zu den „Trendthemen“ Cloud, mobile Geräte und BYOD sowie APTs und der NSA Affäre bewusst sehr kurz gehalten, um ein Ausufern des Umfanges der Umfrage zu vermeiden. Hier wäre es sicherlich interessant nachzuforschen, welche spezifische Sicherheitsmaßnahmen bei diesen Themen in Unternehmen umgesetzt werden [1, S. 45].

Eventuell könnte eine noch detailliertere statistische Analyse der Ergebnisse (Korrelation, Bildung von Gruppen mit ähnlichen Merkmalen etc.), etwa mit SPSS, zusätzlich interessante Informationen und Details liefern.

Es gibt diverse Studien [66, o. S.], [28, o. S.], [18, o. S.], laut denen Insider (Ex-Mitarbeiter, Mitarbeiter, Partner, Dienstleister mit Systemzugriff) eine der Hauptquellen von Angriffen (vorsätzlich) und Risiken bzw. Lecks (durch Fahrlässigkeit) für Unternehmen sind. Eine vertiefende Untersuchung dieses (heiklen) Themas in der Umfrage könnte durchaus interessant sein.

Wie auch schon in meiner letzten Umfrage beschrieben [1, S. 46] könnte versucht werden über in die Umfrage eingebaute „Verifikationsfragen"/Detailfragen zu erkennen, ob sich Unternehmen etwa in Bezug auf technische/organisatorische Maßnahmen korrekt eingeschätzt haben. Es könnte versucht werden bei einigen Themen den Reifegrad bzw. die Qualität der Maßnahme im jeweiligen Unternehmen zu bewerten, da auch ein hoher Implementierungsgrad von Maßnahmen nicht unbedingt bedeutet, dass die jeweiligen technischen und organisatorischen Maßnahmen sauber/in hoher Qualität umgesetzt sind (diese Problematik ist auch in den Kapiteln 4.2.5 und 4.2.5 beschrieben). Um ein umfangmäßiges Ausufern der Umfrage zu vermeiden könnte - sofern die Studie regelmäßig durchgeführt wird - etwa jedes Jahr ein anderes Themengebiet detailliert abgefragt bzw. behandelt werden (z.B. im ersten Jahr Fokus auf Change & Patchmanagement, danach Fokus auf Netzwerksicherheit und Identitäts- und Zugriffsmanagement etc.).

Wie schon in meiner letzten Umfrage beschrieben [1, S. 46] und auch in Kapitel 5.3 überlegt, könnte am Beginn der Umfrage versucht werden über einige Fragen bzw. per Selbsteinschätzung eine Einteilung der befragten Unternehmen nach Engagement und Fähigkeit im Informationssicherheitsbereich (Security-Affinität) durchzuführen. In der Umfrage könnten dann zwei in ihrer Detailtiefe verschiedene Fragebögen hinterlegt werden, um weniger IT/Informationssicherheits-affine Unternehmen zu einem „einfacheren" bzw. weniger detaillierten Fragebogen zu verweisen und besser aufgestellte Unternehmen detaillierteren Fragen zu stellen, die bei gewissen Themen und Maßnahmen mehr in die Tiefe gehen. Somit würde besser auf sehr kleine (EPU) bzw. Informationssicherheits-„fremdere" Unternehmen eingegangen, für die viele organisatorische und technische Fragen zu genau (bzw. nicht relevant) sind, wodurch sie nicht sinnvoll beantwortet werden können.

Eine weitere denkbare Verbesserungsmöglichkeit wäre es zu versuchen, die Umfrage über große Wirtschaftsverteiler oder -vereine zu verteilen, um auch Unternehmen mit weniger Bezug zur Informationssicherheit zu erreichen und ein „realistischeres" bzw. für die Gesamtsituation in Deutschland, Österreich und der Schweiz eher repräsentatives Lagebild zu erreichen (hierzu wäre jedoch, wie zuvor erwähnte, die Entwicklung einer weniger detaillierten Version des Fragebogens empfehlenswert).

5.3. Rückmeldungen von Teilnehmerinnen und Teilnehmern

Den Teilnehmerinnen und Teilnehmern wurde es am Ende der Umfrage ermöglicht Rückmeldungen zu geben. Ein sehr wichtiges Ergebnis hierbei war, dass die Umfrage und der Fragebogen in einigen Rückmeldungen sehr positiv aufgenommen und gelobt wurde.

Weitere Rückmeldungen waren, dass bei manchen Fragen eine feinere Granulierung wünschenswert wäre z.B. „Vorhanden, aber verbesserungsfähig“ (bzw. „ja, mehrere Maßnahmen getroffen“, „ja Security-Aspekte nur in geringem Ausmaß berücksichtigt“) und bei den Matrix Fragen zu technischen und organisatorischen Maßnahmen auch eine Option „teilweise implementiert“ für nicht vollständig implementierte Maßnahmen gut gewesen wäre.

Zu der Frage, welcher Aufgabenbereich im Unternehmen durch die teilnehmende Person erfüllt wird wurde angemerkt, dass es hier sinnvoll wäre mehrere Antworten zuzulassen (Multiple Choice statt Single Choice), da sich diese Aufgabenbereiche mitunter überschneiden.

Ein weiterer Tipp war das Thema der „externen Datensicherung, bzw. der Wiederherstellbarkeit für mehrere Versionen in der Vergangenheit“ gezielt in einer Frage zu behandeln, da hier oft Schwächen bestehen. Generell wäre es eine Idee in der Umfrage gezielt mehr Fragen zu spezifischen Teilgebieten zu stellen, von denen etwa aus Audits bzw. allgemeinen Erfahrungen etc. bekannt ist, das Unternehmen hier oft eher schwach aufgestellt sind.

Zwei weitere Rückmeldungen bezogen sich auf die generelle Ausrichtung des Fragebogens und auf die Problematik, dass der Fragebogen bei vielen Fragen für Ein Personen Unternehmen (EPUs) nicht sinnvoll zu beantworten ist, da viele der IT-Security Maßnahmen hier mangels Publikum keinen Sinn machen. Es wurde geraten, dass „in Anbetracht der großen Anzahl an EPUs gerade im IT-Bereich in Österreich der Fragebogen entsprechend erweitert werden sollte“. Dieser Anmerkung kann nur zugestimmt werden. Eine Möglichkeit wäre es eine zweite Version des Fragebogens, welche auf EPU bzw. „nicht Security-affine“ Unternehmen angepasst ist, zu erstellen und den Teilnehmerinnen und Teilnehmern nach der Angabe gewisser Grunddaten die jeweils besser passende Version des Fragebogens zuzuweisen (beziehungsweise die Unternehmen selbst vor die Wahl zu stellen).

Eine weitere interessante Anregung, welche in einer Rückmeldung gemacht wurde, war die Frage, wie sichergestellt werden kann, dass die Anonymität der Teilnehmerinnen und Teilnehmer tatsächlich gewährleistet wird. Es wurde angemerkt, dass es diesbezüglich durch die Nutzung des Online-Umfragetools surveymonkey zu Problemen kommen kann. Dies ist grundsätzlich natürlich ein valider Einwand, da die Umfragedaten und Ergebnisse bei surveymonkey liegen.

Es muss jedoch angemerkt werden, dass bewusst nicht nach Firmennamen oder spezifischen Informationen gefragt wurde, über die sich einzelne Unternehmen leicht identifizieren lassen würden (bei der

E-Mail konnte eine beliebige bzw. keine Adresse angegeben werden). Außerdem wurden die Daten nach Beendigung der Auswertung aus surveymonkey gelöscht und somit eventuell zusätzlich mitgespeicherte Metadaten vernichtet. Weiters ist surveymonkey ein sehr großes und weltweit sehr stark verbreitetes Umfragetool, welches von vielen großen Firmen genutzt wird. Daher sollte es hoffentlich angebrachte sein, dass surveymonkey in gewissen Rahmen Vertrauen entgegengebracht wird. Natürlich besteht die Möglichkeit die Umfrage zukünftig mit einem eigens gehostetem Tool durchführen. Hierzu könnte etwa die frei Open Source Software LimeSurvey verwendet werden.

5.4. Ausblick

Die Arbeit und der Fragebogen bieten eine meiner Meinung nach sehr gute Ausgangsbasis sowie Hinweise und eigene Erfahrungen, um die Informationssicherheitssituation in Deutschland, Österreich und der Schweiz in Form einer noch größeren und umfangreicheren Studie in darauffolgenden Jahren zu untersuchen.
Ein schönes Ziel wäre es eine solche Studie regelmäßig durchzuführen, um vergleichende Ergebnisse zu erhalten und eine breitere Basis an teilnehmenden Unternehmen zu erreichen. Somit könnte die Studie und deren Aussagekraft kontinuierlich verbessert, auf aktuelle Entwicklungen eingegangen und jährlich verschiedene Themenschwerpunkte gesetzt werden. Längerfristig könnte versucht werden sich mit dieser Studie im deutschsprachigen Raum, neben diversen anderen Studien und Untersuchungen im Bereich der Informationssicherheit (bzw. Cybersicherheit), zu etablieren.
Die Ergebnisse könnten genutzt werden, um Entwicklungen und Trends im Feld der Informationssicherheit zu erkennen, Bewusstsein und Interesse an dem Thema zu wecken und um Unternehmen dazu zu bringen bzw. dabei zu unterstützen, sich mit den verschiedensten Aspekten des unbestreitbar sehr wichtigen Themas der Informationssicherheit auseinanderzusetzen.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

[1] P. Reisinger, “Informationssicherheit in Österreich - Eine Studie zur Informationssicherheit in österreichischen Unternehmen 2013,” Master’s thesis, Fachhochschul St. Pölten - Studiengang IT-Security, 2013.

[2] M. Pilz , A. Obereder, P. Schaumann. Informationssicherheit und Recht. [Online]. Available: http://sicherheitskultur.at/Eisberg_jus.htm[letzterZugriff:25.07.2013]

[3] SBA, “SBA CyberSecurity Incident Aggregation,” Not Published.

[4] SBA Research, “Whitepaper: Heartbleed,” April 2014.

[5] F. Niemann, M. Poujol, M. Flug, “Cyber Security - Investitionspläne, Chancen und Herausforderungen in deutschen Unternehmen,” 2014.

[6] KPMG, “Cloud-monitor,” 2014.

[7] Corporate Trust, “Studie: Industriespionage 2014 - Cybergeddon der deutschen Wirtschaft durch NSA & Co.?” 2014.

[8] BSI, “Ergebnisse der Cyber-Sicherheits-Umfrage 2014,” Oktober 2014.

[9] Kaspersky lab, “IT Security Risks Survey 2014: A Business approach to managing Data Security Threats,” 2014.

[10] techconsult, “2. Bericht zur Studie „Security-Bilanz Deutschland“ - Pain-Points der Umsetzung von IT-Sicherheitsmaßnahmen,” 2014.

[11] *Information technology - Security techniques - Information security management systems - Overview and vocabulary ISO/IEC 27000:2013*, International Organization for Standardization Std.

[12] *Leitfaden für das Management der Informationssicherheit ISO/IEC 27002:2008*, International Organization for Standardization Std.

[13] DI H. Geyer, “Vorlesungsunterlagen Sicherheitsnormen und Standards,” WS 2011/12.

[14] M. Barzilay. (2013, Mai) A simple definition of cybersecurity. ISACA. [Online]. Available: http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296[letzterZugriff:06.07.2013]

[15] grecs. (2014, Mai) Cyber Security versus Information Security. [Online]. Available: https://www.novainfosec.com/2014/05/05/cyber-security-versus-information-security/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+novainfosecportalblog+%28NovaInfosec.com+Blog%29[letzterZugriff:13.04.2015]

[16] M. A. Davis, "InformationWeek 2014 Strategic Security Survey," 2014.

[17] Ernst & Young, "Get ahead of cybercrime - EY's Global Information Security Survey 2014," 2014.

[18] PWC, "Managing cyber risks in an interconnected world - The Global State of Information Security Survey 2015," 2014.

[19] ——. (2015) Global State of Information Security Survey: Explore the data. [Online]. Available: http://www.pwc.com/gx/en/consulting-services/information-security-survey/giss.jhtml[letzterZugriff:15.04.2015]

[20] R. Richardson, "2010/11 CSI Computer Crime and Security Survey," 2011.

[21] Deloitte Touche Tohmatsu Limited (DTTL) TMT Industry Group, "Blurring the lines 2013 TMT Global Security Study - Key Findings," 2013.

[22] Ponemon Institute LLC, "2015 Cost of Data Breach Study," 2015.

[23] Verizon, "2015 Data Breach Investigations Report," 2015.

[24] L. I. Kurki, "Informationssicherheit in österreichischen klein- und mittelständischen Unternehmen," Master's thesis, Fachhochschul Eisenstadt -Studiengang Informationsberufe, 2006.

[25] Dr. S. Fenz et. al, "Monitoring zur Datensicherheit in Österreich," 2013.

[26] Austrian Security Forum, "IT-Security in Österreich 2012," 2012.

[27] E. B. et. al, "Cyber Security Fitness Index Austria - Führungsinstrument zur Bewertung der unternehmerischen Sicherheitsvorsorge im Cyberspace," 2015.

[28] BITKOM. Digitale Angriffe auf jedes zweite Unternehmen. [Online]. Available: http://www.bitkom.org/de/presse/8477_82074.aspx[letzterZugriff:17.04.2015]

[29] NIFIS - Nationale Initiative für Informations- und Internet-Sicherheit, "IT-Sicherheit und Datenschutz 2015," 2015.

[30] techconsult, "1. Bericht zur Studie „Security-Bilanz Deutschland" - Der Status Quo der IT-Sicherheit im deutschen Mittelstand," 2014.

[31] N. Luckhardt. kes - Ergebnisse der kes/Microsoft-Sicherheits-Studie. [Online]. Available: http://www.techcast.com/events/it-sa-2014/mittwoch-gruen-1600-luckhardt/?q=mittwoch-gruen-1600-luckhardt[letzterZugriff:03.05.2015]

[32] ——. Rückschlag in der Malware-Abwehr - Ergebnisse der <kes>/Microsoft-Sicherheitsstudie 2014. [Online]. Available: http://www.pressebox.de/pressemitteilung/secumedia-verlags-gmbh/Rueckschlag-in-der-Malware-Abwehr/boxid/704967[letzterZugriff:03.05.2015]

[33] o. A. Heartbleed Entdeckung. wipipedia.org. [Online]. Available: https://de.wikipedia.org/wiki/Heartbleed#Entdeckung[letzterZugriff:22.04.2015]

[34] SBA Research. Heartbleed Bedrohungslage in Österreich. SBA Research. [Online]. Available: https://www.sba-research.org/2014/04/15/heartbleed-bedrohungslage-in-osterreich/[letzterZugriff:22.04.2015]

[35] ——, "Whitepaper: Shellshock a.k.a. Bashbleed," September 2014.

[36] o. A. Shellshock: Yahoo, WinZip und Lycos fallen Angriffen zum Opfer. heise.de. [Online]. Available: http://www.heise.de/security/meldung/Shellshock-Yahoo-WinZip-und-Lycos-fallen-Angriffen-zum-Opfer-2412822.html[letzterZugriff:22.04.2015]

[37] Open Source Software Security - Coverity Scan. wikipedia.org. [Online]. Available: https://en.wikipedia.org/wiki/Open-source_software_security#Coverity_scan[letzterZugriff:18.07.2015]

[38] F. Scherschel. NSA-Affäre: Generatoren für Zufallszahlen unter der Lupe. heise.de. [Online]. Available: http://www.heise.de/security/meldung/NSA-Affaere-Generatoren-fuer-Zufallszahlen-unter-der-Lupe-1953716.html[letzterZugriff:22.04.2015]

[39] B. Schneier. Exploit of the day. schneier.com. [Online]. Available: https://www.schneier.com/cgi-bin/mt/mt-search.cgi?search=exploit%20of%20the%20day&__mode=tag&IncludeBlogs=2&limit=20&page=2[letzterZugriff:22.04.2015]

[40] J. Appelbaum et. al. Neue Dokumente: Der geheime Werkzeugkasten der NSA. Der Spiegel. [Online]. Available: http://www.spiegel.de/netzwelt/netzpolitik/neue-dokumente-der-geheime-werkzeugkasten-der-nsa-a-941153.html[letzterZugriff:22.04.2015]

[41] ——, "Die Klempner aus San Antonio," *Der Spiegel*, vol. 1, pp. 100–105, 2014.

[42] ——, "Otto-Katalog für Spione," *Der Spiegel*, vol. 1, pp. 102–103, 2014.

[43] o. A. Bullrun (decryption program). wikipedia.org. [Online]. Available: https://en.wikipedia.org/wiki/Bullrun_%28decryption_program%29[letzterZugriff:22.04.2015]

[44] A. Kannenberg. Bruce Schneier zum NSA-Skandal: Die US-Regierung hat das Internet verraten. heise.de. [Online]. Available: http://www.heise.de/security/meldung/Bruce-Schneier-zum-NSA-Skandal-Die-US-Regierung-hat-das-Internet-verraten-1951318.html[letzterZugriff:22.04.2015]

[45] S. S. Nicole Perloth, Jeff larson. Secret Documents Reveal N.S.A. Campaign Against Encryption. The New York Times. [Online]. Available: http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?_r=2&[letzterZugriff:22.04.2015]

[46] M. Holland. NSA sabotiert offenbar auch direkt in Deutschland. heise.de. [Online]. Available: http://www.heise.de/newsticker/meldung/NSA-sabotiert-offenbar-auch-direkt-in-Deutschland-2415559.html[letzterZugriff:22.04.2015]

[47] R. Höwelkrlöger. NSA zahlte 10 Millionen US-Dollar für Krypto-Backdoor. heise.de. [Online]. Available: http://www.heise.de/newsticker/meldung/NSA-zahlte-10-Millionen-US-Dollar-fuer-Krypto-Backdoor-2071567.html[letzterZugriff:22.04.2015]

[48] J. Schmidt. Todesurteil für Verschlüsselung in den USA. heise.de. [Online]. Available: http://www.heise.de/security/artikel/Todesurteil-fuer-Verschluesselung-in-den-USA-1972561.html[letzterZugriff:22.04.2015]

[49] o. A. Snowden-Dokumente: NSA-Mitarbeiter sabotieren möglicherweise auch in Deutschland. Speigel Online. [Online]. Available: http://www.spiegel.de/netzwelt/netzpolitik/nsa-snowden-dokumente-bei-the-intercept-tarex-basis-in-deutschland-a-996667.html[letzterZugriff:22.04.2015]

[50] M. Baumgärtner, H. Gude, M. Rosenbach, J. Schindler. (2015, April) Überwachung: Neue Spionageaffäre erschüttert BND. Spiegel Online. [Online]. Available: http://www.spiegel.de/politik/deutschland/ueberwachung-neue-spionageaffaere-erschuettert-bnd-a-1030191.html[letzterZugriff:03.05.2015]

[51] BSI, ISACA Chapter Germany, "Leitfaden Cyber-Sicherheits-Check -Ein Leitfaden zur Durchführung von Cyber-Sicherheits-Checks in Unternehmen und Behörden," Februar 2014.

[52] T. Terpandjian. Advanced Persistent Threats (APT): Operation Aurora, its Perpetrators, Incentives and Administrative Responses to Alleviate Dangers. [Online]. Available: https://www.academia.edu/10247992/Advanced_Persistent_Threats-_Operation_Aurora[letzterZugriff:13.04.2015]

[53] R. Richmond. (2011, April) The RSA Hack: How They Did It. The New York Times. [Online]. Available: http://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/[letzterZugriff: 13.04.2015]

[54] F. Scherschel. (2014, Dezember) BSI-Sicherheitsbericht: Erfolgreiche Cyber-Attacke auf deutsches Stahlwerk. heise.de. [Online]. Available: http://www.heise.de/security/meldung/BSI-Sicherheitsbericht-Erfolgreiche-Cyber-Attacke-auf-deutsches-Stahlwerk-2498990.html[letzterZugriff:13.04.2015]

[55] A. Pratzner. Fragebogen, Internet Umfrage, Online Survey - einfach Umfragen durchführen - fragebogen.de. [Online]. Available: http://www.fragebogen.de[letzterZugriff:20.07.2013]

[56] o. A. Fragebögen. Wirtschaftspsychologische Gesellschaft. [Online]. Available: http://www.wpgs.de/content/blogcategory/87/355/l[letzterZugriff:24.04.2015]

[57] B. Aschemann-Pilshofer, "Wie erstelle ich einen Fragebogen - Ein Leitfaden für die Praxis," Jänner 2001.

[58] R. Felser. (2015, März) Aufruf zur Teilnahme an Studie zur Informationssicherheit in Deutschland und Österreich. Computerwelt. [Online]. Available: http://www.computerwelt.at/news/technologie-strategie/security/detail/artikel/110328-aufruf-zur-teilnahme-an-studie-zur-informationssicherheit-in-deutschland-und-oesterreich/[letzterZugriff: 21.04.2015]

[59] o. A. (2015, März) Informationssicherheitsstudie: Betriebe gesucht . onlinesicherheit.at. [Online]. Available: https://www.onlinesicherheit.gv.at/mitarbeiterinnen/news/158970.html[letzterZugriff: 21.04.2015]

[60] ——. Selbstselektion. wikipedia.org. [Online]. Available: https://de.wikipedia.org/wiki/Selbstselektion[letzterZugriff:29.04.2015]

[61] R. K. Bidmon. (2010, März) Mythos: Sind Studien mit hoher Teilnehmerzahl wirklich repräsentativ? [Online]. Available: http://www.bidmon.de/blog/2010/03/studien-hohe_teilnehmerzahl-repraesentativ-html/[letzterZugriff:29.04.2015]

[62] M. Suter, "Informationssicherheit in Schweizer Unternehmen," August 2006.

[63] D. Florencio, C. Herley, "Sex, Lies and Cyber-crime Surveys," 2011.

[64] o. A. Repräsentativität. [Online]. Available: https://de.wikipedia.org/wiki/Repr%C3%A4sentativit%C3%A4t[letzterZugriff:29.04.2015]

[65] o. A. Kapitel Repräsentativität sowie Stichproben und Repräsentativität . Wirtschaftspsychologische Gesellschaft. [Online]. Available: http://www.wpgs.de/content/blogcategory/83/348/ [letzterZugriff:29.04.2015]

[66] J. Diercks. IBM-Sicherheitsstudien: Cyberattacken aus den eigenen Reihen am häufigsten. heise.de. [Online]. Available: http://www.heise.de/ix/meldung/IBM-Sicherheitsstudien-Cyberattacken-aus-den-eigenen-Reihen-am-haeufigsten-2715977.html[letzterZugriff:21.06.2015]

A. Anhang

A.1. Gesamter Fragebogen

Im Folgenden ist der gesamte Fragebogen der Umfrage inklusive aller Fragen und Begleittexte ersichtlich.

Studie Informationssicherheit in Deutschland, Schweiz und Österreich

1. Einleitung

Sehr geehrte Teilnehmerin, sehr geehrter Teilnehmer!

Vielen Dank dafür, dass Sie sich entschieden haben, an der folgenden wissenschaftlichen Umfrage teilzunehmen!

Mein Name ist Philipp Reisinger und ich führe diese Umfrage im Rahmen meiner Diplomarbeit an der FH St. Pölten durch. In ihr untersuche ich, inwiefern IT-/Informationssicherheit in deutschen, Schweizer und österreichischen Unternehmen und Organisationen ein Thema ist und wie diese aufgestellt sind.

Aufgrund Ihrer Teilnahme an der Studie können Sie dadurch profitieren, dass verschiedene organisatorische und technische Maßnahmen angesprochen werden, deren Umsetzung die Informationssicherheit in Ihrem Unternehmen erheblich verbessern kann. Diese Maßnahmen könne als Anregung verstanden werden, sich mit gewissen Themen zu befassen. Außerdem erhalten Sie präzise Ergebnisse zur aktuellen Situation in Deutschland, Österreich und der Schweiz.

Der Fragebogen umfasst 21 fachspezifische Fragen und sollte in einem Zeitrahmen von 15-20 Minuten gut auszufüllen sein.

Alle Fragen können übersprungen werden. Lediglich bei den demographischen Fragen würde ich Sie aus Auswertungsgründen um Angabe der Mitarbeiteranzahl und des Standortes (Land) bitten.

Natürlich werden alle Angaben vertraulich behandelt und lediglich im Rahmen der Studie selbst, der darauf aufbauenden Diplomarbeit und einem Artikel hierzu in anonymisierter Form (in Statistiken, Grafiken) verwendet.

Ich möchte mich nochmals dafür bedanken, dass Sie sich die Zeit nehmen, den folgenden Fragebogen auszufüllen und somit einen wertvollen Beitrag zu meiner Studie leisten.

Mit freundlichen Grüßen
Philipp Reisinger

Philipp Reisinger BSc.
Master Student im Studiengang Information Security
e-mail: is131510@fhstp.ac.at
Fachhochschule St. Pölten GmbH
Matthias Corvinus-Straße. 15, A-3100 St. Pölten

Schlussendlich möchte ich mich bei dem ADV, bei Computerwelt, bei Cyber Security Austria, der IT-Security Experts Group der WKÖ, dem IKT-Sicherheitsportal, ISACA Austria, der SBA Research, der FH St. Pölten sowie den vielen anderen Helfern für die Unterstützung bei der Durchführung und Verteilung dieser Umfrage bedanken!

2. Wichtigkeit von eigener IT und Daten

1. Denken Sie an die wichtigsten IT-Systeme/Services/Ressourcen (*) in Ihrem Unternehmen. Wie lange dürfte diese ausfallen, ohne Ihr Kerngeschäft stark negativ zu beeinträchtigen oder unmöglich zu machen?

- ○ Wenige Stunden: sehr starke Abhängigkeit von IT
- ○ 1 Tag: starke Abhängigkeit von IT
- ○ 2 Tage: Abhängigkeit von IT lediglich in Teilbereichen
- ○ > 2 Tage: geringe Abhängigkeit von IT

* Beispielsweise Firmenapplikationen, SAP/ERP, CRM, Internet, e-mail, SharePoint, Website, Fileserver & Fileshares, Datenbanken, Netzwerk, Server etc.

2. Denken Sie an die wichtigsten Daten und Informationen(*) in Ihrem Unternehmen. Als wie schwerwiegend schätzen Sie die Auswirkungen bei deren Verlust, Nichtverfügbarkeit oder Verfälschung bzw. bei einer Veröffentlichung - etwa an Mitbewerber - ein?

- Niedrig: Das Geschäft des Unternehmens wird kaum beeinträchtig und es ist nur mit sehr geringen Konsequenzen zu rechnen.
- Mittel: Das Kerngeschäft wird spürbar beeinträchtigt und es ist mit gewissen Geldverlusten, Know-How-Verlusten, Imageschäden oder rechtlichen Konsequenzen zu rechnen.
- Hoch: Das Kerngeschäft wird stark beeinträchtigt und es ist mit Geldverlusten, Know-How-Verlusten, Imageschäden und rechtlichen Konsequenzen zu rechnen.
- Sehr hoch: Das Kerngeschäft des Unternehmens wird sehr stark negativ beeinträchtigt. Es ist mit schwerwiegenden Imageschäden, Know-How Verlusten, Geldverlusten und rechtlichen Konsequenzen zu rechnen. Außerdem werden langfristige Auswirkungen auf die Neukunden- bzw. Auftragsgewinnung erwartet.

* Beispielsweise Personenbezogene Daten, Mitarbeiterdaten, Geschäftsdaten, E-Mails, Verträge, Buchhaltungs-/ Finanzdaten, Projektdaten, Kundendaten etc.

3. Als wie wichtig wird das Thema Informationssicherheit in Ihrem Unternehmen angesehen (*) und wie sehr ist die Informationssicherheit in unternehmerische Tätigkeiten integriert und berücksichtigt?

- Unwichtig/nebensächlich, Keine besondere Berücksichtigung von Informationssicherheit in wesentlichen Geschäftsprozessen.
- Weniger wichtig, Informationssicherheit ist mehrheitlich IT Thema und dort angesiedelt
- Wichtig, Es gibt eine dedizierte Rolle, die für Informationssicherheit verantwortlich ist. Diese übernimmt auch die Kommunikation und Abstimmung mit den Fachbereichen/Geschäftsprozessen.
- Sehr wichtig, Informationssicherheit ist in allen wesentlichen Geschäftsprozessen ein definierter, integraler Bestandteil, mit festgelegten Sicherheitsmaßnahmen und Verantwortlichkeiten

* unter Berücksichtigung der eigenen Abhängigkeit von IT Technologien im alltäglichen Betrieb und dem Schutzbedarf/Sensibilität von verarbeiteten Daten und Informationen

3. Gründe/Motivation für Informationssicherheit, Bedrohungen

Studie Informationssicherheit in Deutschland, Schweiz und Österreich

4. Welches sind die (Top 5) Gründe Ihres Unternehmens sich mit dem Thema Informationssicherheit auseinanderzusetzen?

- [ ] Gesetzliche Vorgaben (Datenschutz, EU-Richtlinien)/Compliance
- [ ] Vermeidung von (Geld/Image)Verlusten durch Sicherheitsvorfälle oder Datenpannen
- [ ] Datenverlusten/Verfälschung vorbeugen
- [ ] Stabilität des Betriebs sicherstellen
- [ ] Haftung gegenüber Dritten
- [ ] Forderung von Kunden/Partnern
- [ ] Als Wettbewerbsvorteil/zum Marketing (Zertifizierungen)
- [ ] Vorfälle in der Vergangenheit (Ausfälle von IT-Systemen, Einbrüche in IT-Systeme, Hacking, Datenverluste etc.)
- [ ] Starke Abhängigkeit von eigener IT in gewissen Geschäftsprozessen
- [ ] Wirtschaftsprüfung, Jahresabschluss, Due Diligence
- [ ] Vorfälle, über die in Medien berichtet wurde
- [ ] NSA-Überwachungsskandal
- [ ] Sonstiges (bitte angeben)

5. - Setzt sich Ihr Unternehmen mit Standards/Empfehlungen im Bereich der Informationssicherheit auseinander?

- [ ] keine Verwendung von speziellen Standards/Empfehlungen
- [ ] ISO 27001
- [ ] BSI - IT-Grundschutz
- [ ] ITIL
- [ ] COBIT
- [ ] BSI - Leitfaden Informationssicherheit - IT-Grundschutz kompakt
- [ ] IT-Beauftragter der Bayerischen Staatsregierung - Leitfaden zur Informationssicherheit in kleinen und mittleren Unternehmen
- [ ] BITKOM - Sicherheit für Systeme und Netze in Unternehmen - Einführung in die IT-Sicherheit und Leitfaden für erste Maßnahmen
- [ ] Österreichische Informationssicherheitshandbuch
- [ ] WKÖ - IT Sicherheitshandbuch
- [ ] SANS CSC - Critical Security Controls
- [ ] PCI DSS
- [ ] OWASP Top 10
- [ ] Sonstiges (bitte angeben)

Studie Informationssicherheit in Deutschland, Schweiz und Österreich

6. Was sind Ihrer Meinung nach die (Top 5) Hauptrisiken/Bedrohung in Bezug zur Informationssicherheit, denen Ihr Unternehmen ausgesetzt ist?

- ☐ Malware (Viren, Trojaner, Spyware etc.)
- ☐ Hacking
- ☐ (D)DoS Angriffe
- ☐ APTs (zielgerichtete, komplexe, fortgeschrittene Angriffe)
- ☐ Angriffe auf Website und Datenbanken
- ☐ Abhören/Spionage
- ☐ Betrug
- ☐ Social Engineering
- ☐ (Spear)Phishing
- ☐ Spam
- ☐ Einbrüche bzw. Diebstahl Systeme/mobile Geräte
- ☐ Hardware- oder Software-Fehler
- ☐ Datenverluste (Daten gelöscht/verloren, nicht mehr wiederherstellbar)
- ☐ Datendiebstahl (unautorisierte Person erlangt Daten)
- ☐ (unbemerkte) Datenmanipulation
- ☐ Katastrophen/Höhere Gewalt
- ☐ Stromausfälle
- ☐ Insider-Missbrauch von Rechten/Systemen
- ☐ Fahrlässigkeit eigener Mitarbeiter
- ☐ bewusstes schadhaftes Verhalten eigener Mitarbeitern
- ☐ Ausfälle oder Fehler von externen Partnern/Cloud
- ☐ Einsatz mobiler Geräte (BYOD)
- ☐ Social Media
- ☐ Sonstiges (bitte angeben)

7. Welches sind Ihrer Meinung nach die (Top 5) Hauptprobleme/hemmende Faktoren bei der Aufrechterhaltung/Verbesserung der Informationssicherheit in Ihrem Unternehmen?

- ☐ Fehlendes Budget
- ☐ Fehlende Unterstützung und Bewusstsein (z.B. zu Risiken und Gefahren) im (Top)Management
- ☐ Fehlendes Bewusstsein der Mitarbeiter
- ☐ Mangelndes Detail/Spezialwissen (zu Gefahren/Angriffsvektoren und notwendigen Maßnahmen)
- ☐ Mangelnde Beratungsmöglichkeiten
- ☐ Fehlende (technische) Lösungen
- ☐ Fehlende Mitarbeiter-Akzeptanz für Sicherheitsmaßnahmen, die die Usability/Benutzbarkeit einschränken
- ☐ Datenschutzbedenken
- ☐ Sich schnell ändernde Systemumgebung und Angriffsarten
- ☐ Sonstiges (bitte angeben)

4. Aktuelle Situation im Unternehmen

Studie Informationssicherheit in Deutschland, Schweiz und Österreich

8. Gibt es in dem Unternehmen einen IT-/Informationssicherheits-Verantwortlichen (*) und gibt es eine Informationssicherheits-Policy?

- ○ Ja, Verantwortlicher und Informationssicherheits-Policy
- ○ Verantwortlicher, aber keine Informationssicherheits-Policy
- ○ Kein Verantwortlicher und keine Informationssicherheits-Policy

* für die Steuerung, Koordinierung und Umsetzung von Informationssicherheits-bezogenen Maßnahmen und Themen

9. Gibt es in Ihrem Unternehmen Richtlinien/Vorgaben in Bezug zur Informationssicherheit?

- ☐ Keine Richtlinien/Vorgaben
- ☐ Nutzung Mail, Internet & Social Media
- ☐ Nutzung mobiler Geräte (etwa auch BYOD) und Speichermedien
- ☐ Clear Desk/ Clear Screen
- ☐ Akzeptable/Zulässige Verwendung Endbenutzer-IT
- ☐ Datenvernichtung und Geräteentsorgung
- ☐ Passwortrichtlinien
- ☐ Informationsklassifikation & Verarbeitung
- ☐ Dokumentationsvorgaben/-anforderungen
- ☐ Sicherheitsvorgaben für Partner und Dienstleister
- ☐ Sonstiges (bitte angeben)

10. Führen Sie in regelmäßigen Abständen interne/externe Audits, Penetration Tests oder Vulnerability Scans durch, um die Informationssicherheit bewerten zu können?

- ☐ Durchführung von internen Audits
- ☐ Durchführung von externen Audits
- ☐ Durchführung von Penetration Tests
- ☐ Durchführung von Vulnerability Scans
- ☐ Keine regelmäßigen Überprüfungsaktivitäten

11. Wurden im letzten Jahr Beratungstätigkeiten zu Informationssicherheits-Themen durch externe Unternehmen wahrgenommen?

- ☐ Keine externe Beratung
- ☐ Informationssicherheits-Strategie- und Managementberatung
- ☐ Durchführung von Schulungen
- ☐ Durchführung von Audits, Penetration Tests
- ☐ Durchführung von Risikoanalysen
- ☐ Beratung bei Produkterwerb und Implementierung
- ☐ Entwicklung von Informationssicherheits-Prozessen und -Maßnahmen sowie Optimierung dieser
- ☐ Incident Response
- ☐ Forensik
- ☐ Sonstiges (bitte angeben)

Studie Informationssicherheit in Deutschland, Schweiz und Österreich

12. Gab es in Ihrem Unternehmen im letzten Jahr Vorfälle im Bereich der Informationssicherheit und wenn ja, in welchem Teilgebiet?

- ☐ Keine Vorfälle
- ☐ Malware (Viren, Trojaner, Spyware etc.)
- ☐ Hacking
- ☐ (D)DoS Angriffe
- ☐ APTs (zielgerichtete, komplexe, fortgeschrittene Angriffe)
- ☐ Angriffe auf Website und Datenbanken
- ☐ Abhören/Spionage
- ☐ Betrug
- ☐ Social Engineering
- ☐ (Spear)Phishing
- ☐ Spam
- ☐ Einbrüche bzw. Diebstahl Systeme/mobile Geräte
- ☐ Hardware- oder Software-Fehler
- ☐ Datenverluste (Daten gelöscht/verloren, nicht mehr wiederherstellbar)
- ☐ Datendiebstahl (unautorisierte Person erlangt Daten)
- ☐ (unbemerkte) Datenmanipulation
- ☐ Katastrophen/Höhere Gewalt
- ☐ Stromausfälle
- ☐ Insider Missbrauch von Rechten/Systemen
- ☐ Fahrlässigkeit Mitarbeiter
- ☐ bewusstes schadhaftes Verhalten eigener Mitarbeitern
- ☐ Ausfälle oder Fehler von externen Partnern/Cloud
- ☐ Einsatz mobiler Geräte (BYOD)
- ☐ Social Media
- ☐ Sonstiges (bitte angeben)

5. Trendthemen

13. Werden mobile Geräte (Laptop, Tablets, Smartphones), etwa auch in Form von BYOD, in Ihrem Unternehmen eingesetzt?

- ○ Ja. Einsatz mobiler Geräte auch in Form von BYOD. Außerdem werden spezielle Sicherheitsmaßnahmen ergriffen (Mobile Device Management, Remote Access und Wipe, Verschlüsselung, interne Regelungen etc.)
- ○ Ja es werden mobile Geräte und BYOD eingesetzt, jedoch ohne gesonderte Sicherheitsmaßnahmen.
- ○ Ja Einsatz mobiler Geräte jedoch kein BYOD
- ○ Nein

14. Nutzt Ihr Unternehmen Cloud Dienstleistungen oder wird Outsourcing von IT Services (*) betrieben?

- ○ Ja. Außerdem werden spezifische Sicherheitsmaßnahmen ergriffen (heimische/europäische Service Provider, Notfallplanung für den Fall der Nichtverfügbarkeit des Dienstleisters, Verschlüsselung, SLAs, Überprüfungen des Partners und von Zugriffsrechten/-möglichkeiten, Fordern von Zertifizierungen etc.)
- ○ Ja, jedoch ohne Informationssicherheitsaspekte speziell zu berücksichtigen
- ○ Nein aufgrund von Sicherheitsbedenken und diverser Vorkommnisse (NSA-Skandal etc.)
- ○ Nein

* Beispielsweise externes Webhosting, externe Datenbanken, Speicher in Cloud, externe oder Cloud Maillösungen, Cloud CRM, Office 365 etc.

15. Gibt es in Ihrem Unternehmen Mitarbeiter-Awareness-Aktivitäten zum Thema Informationssicherheit und der korrekten Nutzung von informationsverarbeitenden Systemen und wenn ja, in welcher Form werden diese durchgeführt?

- ☐ Keine Durchführung von Awareness Aktivitäten
- ☐ Formale Vorgaben in diversen Dokumenten/Richtlinien
- ☐ Intranet Portal
- ☐ Schulungen
- ☐ Sonstiges (bitte angeben)
- ☐ Newsletter und Infomaterial
- ☐ Workshops
- ☐ Kampagnen

16. Wird in Ihrem Unternehmen Open Source Software (*) eingesetzt und wenn ja, treffen Sie Maßnahmen um diese auf Fehlerfreiheit/Korrektheit und Qualität zu überprüfen?

- ○ Kein Einsatz von Open Source Software
- ○ Kein Einsatz von Open Source Software aufgrund von Sicherheitsbedenken
- ○ Ja, jedoch keine Überprüfung der Open Source Software
- ○ Ja, Durchführung von Code Reviews und Recherche zu Auditergebnissen, Sicherheitsanalysen und dem Entwicklerkreis
- ○ Weiß nicht

* Beispielsweise Appache http Server, Linux und diverse Unix Betriebssysteme, MySQL Datenbanken, PHP, OpenVPN, OpenSSL, Firefox, Chrom, OpenOffice etc.

17. War Ihr Unternehmen von schwerwiegenden Sicherheitslücken in Open Source Software wie Heartbleed oder Shellshock betroffen?

- ○ Nein, nicht betroffen
- ○ Ja, jedoch keine Beeinträchtigung der Geschäftstätigkeiten
- ○ Ja, Geschäftstätigkeit wurde beeinträchtigt (*)
- ○ Ja, diese Lücken wurden aktiv für Angriffe auf das Unternehmen ausgenutzt
- ○ Weiß nicht

* durch Nichtverfügbarkeit wichtiger Dienste und außerplanmäßige Wartungsfenster für notwendige Notfall-Patches

18. War Ihr Unternehmen im letzten Jahr Ziel eines komplexen, fortgeschrittenen, direkt auf sie gezielten IT-Angriffs (APT-Advanced Persistent Threat) und wenn ja, richtete dieser Schaden an?

- ○ Nein
- ○ Ja, dieser richtete Schaden an
- ○ Ja, jedoch kein Schaden da erfolgreich abgewehrt
- ○ Es besteht der Verdacht
- ○ Weiß nicht

19. Waren die NSA-Enthüllungen bezüglich Überwachung und Spionage sowie der gezielten Manipulation von (amerikanischen) Soft- und Hardware-Produkten für Ihr Unternehmen ein Thema bzw. haben Sie darauffolgend spezielle Sicherheitsmaßnahmen ergriffen?

- ☐ Nein
- ☐ Ja, jedoch keine gezielten Maßnahmen ergriffen
- ☐ Ja, wachsende Beachtung des Themas der Informationssicherheit
- ☐ Ja, Erhöhung des IT Sicherheitsbudgets
- ☐ Ja, sonstige Maßnahmen bitte nennen

  _____

- ☐ Ja, verstärkter Einsatz von Verschlüsselung
- ☐ Ja, im Fall von Cloud oder Outsourcing wird verstärkt auf heimische/europäische Anbieter gesetzt
- ☐ Ja, Planung zur verstärkten Beschaffung von „IT Made in Swiss/Austria/Germany“ bzw. Europa

6. Technische und organisatorische Aufstellung des Unternehmens 1

Vielen Dank, dass Sie bis hierher teilgenommen haben. Die Umfrage ist fast fertig.

Es folgen nun noch zwei Fragen zu technischen und organisatorischen Maßnahmen in Ihrem Unternehmen, bevor ich Sie am Ende um demographische Angaben ersuche.

Die in folgender Frage angeführten technischen Systeme und Maßnahmen werden unter der Frage kurz beschrieben.

Studie Informationssicherheit in Deutschland, Schweiz und Österreich

20. Welche technischen Systeme, Tools etc. werde im Bereich der Informationssicherheit im Unternehmen eingesetzt bzw. sollen in Zukunft implementiert werden?

	Implementiert	Implementierung in Planung/ in Zukunft vorgesehen	Nicht vorhanden
Firewall(s)	○	○	○
Virenschutz/Malware Scanner	○	○	○
IDS/IPS	○	○	○
Web Content Inspection/ - Filtering /Monitoring	○	○	○
Monitoring Software	○	○	○
SIEM	○	○	○
E-Mail Verschlüsselung & Signatur	○	○	○
E-Mail Malware Scans	○	○	○
Spamschutz	○	○	○
DLP	○	○	○
VPNs	○	○	○
Netzwerk Segmentierung	○	○	○
Layer 2 Netzwerksicherheit	○	○	○
Web Application Firewalls	○	○	○
DDOS Protection	○	○	○
Vulnerability Mgmt. Tools	○	○	○
Verschlüsselungstechnologien	○	○	○
Backupsoftware	○	○	○
Patch Mgmt Software	○	○	○
Log Management Software	○	○	○
(Security) Configuration Management Software	○	○	○
Mobile Device Management Software	○	○	○
OS und Server Hardening	○	○	○
Client Sicherheit	○	○	○
Zwei Faktor Authentifizierung	○	○	○
PKI – Public Key Infrastruktur	○	○	○
MSSP -Managed Security Service Provider	○	○	○

Sonstige im Unternehmen vorhandene Systeme/Tools bitte angeben

Firewall(s): Soft- bzw. Hardware um Zugriffen und Verbindungen auf ein Netz zu kontrollieren

Virenschutz/Malware Scanner: Software, die bekannte Computer-Viren, Computer-Würmer und Trojanische Pferde aufspürt, blockiert und gegebenenfalls beseitigt.

IDS/IPS: Intrusion Detection/Prevention Systeme dienen der Erkennung von Angriffen auf ein Rechnersystem oder Rechnernetz und dem Setzen von Gegenmaßnahmen.

Web Content Inspection/ -Filtering /Monitoring: Systeme um den Web-Verkehr, der etwa über einen Proxy geleitet wird, zu überwachen.

Monitoring Software: Software zur Überwachung (der Performance, Auslastung, Systemzustandes) von IT-Infrastruktur, Netzwerk, Systemen etc. (etwa Nagios, Microsoft System Center Operations Manager, Big Brother, Tivoli etc.)

SIEM: Security Information and Event Management Software sammelt Log Informationen und Security Warnungen aus verschiedenen Quellen, um diese zu korrelieren und Angriffsmuster entdecken zu können.

E-Mail Verschlüsselung & Signatur: Signierung und Verschlüsselung von vertraulichen Mails

E-Mail Malware Scans: Virenscans von Anhängen, bevor diese Mail in die Mailbox des Mitarbeiters gelangt

Spamschutz: Maßnahmen wie Spam Filter, Greylisting, SPF etc., um Spam zu verhindern.

DLP: Systeme zur Data Loss/Leakage Prevention, die die Vertraulichkeit von Informationen schützen und Datendiebstähle verhindern sollen.

VPNs: Virtual private Networks dienen der sicheren Verbindung von Rechnern oder Netzen mit einem interne Firmennetz über (unsichere) öffentliche Netze (Internet).

Layer 2 Netzwerksicherheit: Maßnahmen im Bereich der LAN und WLAN Sicherheit. Einige Punkte sind Netzwerksegmentierung, VLANs (Virtual Local Area Networks), 802.1x, NAC (Network Admission Control),NAP (Network Access Protection), Arp Protection, BPDUGuard etc.

Netzwerk Segmentierung: Logische Trennung der Netzwerke eines Unternehmens. Etwa Schaffung eines eigenen Netzes für Server, Clients, Produktion und Administration sowie Regelung der Zugriffsmöglichkeiten zwischen diesen Netzen (per Firewall oder ACLs)

Web Application Firewalls: Software welche dem Schutz von Webapplikationen vor Angriffen wie SQL Injection, XSS etc. dient, indem Webkommunikation auf der Anwendungsebene untersucht wird.

DDOS Protection: Diverse Anbieter welche die Webkommunikation, welche auf die Firmen-Website zielt, überwachen und bei DDOS Angriffen Gegenmaßnahmen durchführen können.

Vulnerability Mgmt. Tools: Programme die durch regelmäßige (interne und externe) Netzwerkscans dem Auffinden von Schwachstellen auf in Unternehmen eingesetzten Rechnern und Servern dienen sollen.

Verschlüsselungstechnologien: Software um Daten zu verschlüsseln, damit deren Vertraulichkeit gewährleistet und diese nur noch unter Bereitstellung des entsprechenden Schlüssels gelesen werden können. Neben der Verschlüsselung selbst ist das Schlüsselmanagement (Erzeugen, Speichern, Sichern, Archivieren, Löschen) von sehr großer Bedeutung.

Backupsoftware: Software zum Erstellen und Wiedereinspielen von Sicherungen.

Patch Mgmt Software: Software, die dem Verteilen und Installieren von Updates auf im Unternehmen eingesetzten Systemen dient (etwa WSUS und SCCM für Windows selbst und z.B. Secunia CSI, SolarWinds Patch Manager oder Shavlik Patch für Third Party Updates).

Log Management Software: Software zum Sammeln (auf einem zentralen Syslog Server) und Analysieren (für die Analyse/Korrelation insbesondere SIEM Produkte) von Logs/Aufzeichnungen von im Unternehmen eingesetzten Systemen.

(Security) Configuration Management Software: Software zur Verwaltung der Konfiguration von Endgeräten und Server wie z.B.Tripwire, NetIQ, IBM Endpoint Manager etc.

Mobile Device Management Tools: Tools welche die zentrale Verwaltung und den sicheren Einsatz von mobile Geräten in einem Unternehmen ermöglichen sollen.
OS Hardening: Prozess zur Absicherung eines Systems durch Reduktion der Angriffsfläche und möglicher Schwachstellen. Etwa durch die Befolgung von in Hardening Guides vorgeschlagenen Maßnahmen wie der Deinstallation unnötiger Services, der sicheren Konfiguration einzelner Dienste, der Änderung von Default Passwörtern und Usernamen, Application Whitelisting. etc.
Client Sicherheit: eingeschränkte Rechte, Schutz vor Installation ungewollter Software, Schnittstellen-Sicherung (USB, DVD etc.)
Zwei Faktor Authentifizierung: Verwendung von mehreren unabhängigen Faktoren bei der Authentifikation und dem Einsatz von Smart Cards, Tokens oder Biometrie bei der Authentifizierung von Mitarbeitern
PKI - Public Key Infrastruktur: Sicherheitsinfrastruktur, die es ermöglicht, in nicht gesicherten Netzen (z. B. Internet) auf der Basis eines von einer vertrauenswürdigen Stelle (CA) ausgegebenen Schlüsselpaares (für die asymmetrische Verschlüsselung) verschlüsselt Daten auszutauschen, Signaturen zu erzeugen und zu prüfen bzw. zur Authentifizierung mittels (Client)Zertifikaten genutzt werden kann.
MSSP -Managed Security Service Provider: Outsourcing diverser Security Aufgaben wie regelmäßige System Scans, Firewall Maintenance, Intrusion Detection und Prevention, Patch und Update Management etc. an einen spezialisierten Security Service Provider.
Quellen: BSI Cyber Sicherheit Glossar, wikipedia

7. Technische und organisatorische Aufstellung des Unternehmens 2

Die in folgender Frage angeführten organisatorischen Prozesse und Maßnahmen werden unter der Frage kurz beschrieben.

Studie Informationssicherheit in Deutschland, Schweiz und Österreich

21. Welche organisatorische Maßnahmen/Prozesse sind im Bereich der Informationssicherheit im Unternehmen umgesetzt bzw. sollen in Zukunft eingeführt werden?

	Implementiert	Implementierung in Planung /in Zukunft vorgesehen	Nicht vorhanden
Betrieb eines ISMS	○	○	○
Betrieb eines IKS inklusive IT Kontrollen	○	○	○
Audits/Penetration Tests/Vulnerability Scans	○	○	○
Risikomanagement	○	○	○
BCM und BIA/ Notfallplanung/-vorsorge	○	○	○
Personal Management	○	○	○
Awareness Aktivitäten	○	○	○
Vulnerability Management	○	○	○
Change Management	○	○	○
Configuration/ Capacity Management	○	○	○
Physische Sicherheit	○	○	○
Asset Management	○	○	○
Informationsklassifikation und –Verarbeitung	○	○	○
Identitäts- und Zugriffsmanagement	○	○	○
Vorfallmanagement	○	○	○
Patch & Update Management	○	○	○
Backup & Wiederherstellung	○	○	○
Logging & (Performance) Monitoring	○	○	○
Spam & Antivirus	○	○	○
Medien-/Datenvernichtung	○	○	○
Management der Leistungserbringung/Verträge Externe IT Dienstleister	○	○	○
Dokumentation (Systeme, Konfigurationen, Organisatorische Prozesse etc.)	○	○	○
Sichere Software-	○	○	○

/Webapplikationsentwicklung			
Versicherung gegen Cyber/IT-Angriffe	○	○	○
Firmeneigenes CERT	○	○	○
Durchführung/Teilnahme an Cyber Übungen	○	○	○

a. Sonstige im Unternehmen vorhandene Maßnahmen/Prozesse bitte angeben

Betrieb eines ISMS: Organisatorische Vorgehensweise bezüglich der Aufstellung von Verfahren und Regeln innerhalb eines Unternehmens, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Der bekannteste Ansatz hierfür ist eine Vorgehensweise nach ISO 27001 oder BSI Grundschutz.
Betrieb eines IKS inklusive IT Kontrollen: Systematisch gestaltete technische und organisatorische Maßnahmen und Kontrollen im Unternehmen zur Einhaltung von Richtlinien und zur Abwehr von Schäden, die durch das eigene Personal oder böswillige Dritte verursacht werden können. In Bezug auf IT Kontrollen ist hierfür insbesondere COBIT eine häufig genutzte Ausgangsbasis.
Audits/Penetration Tests/Vulnerability Scans: Durchführung von Audits/Penetration Tests/Vulnerability Scans, um die Informationssicherheit bzw. die Sicherheit einzelner Systeme erheben zu können und auf Basis dessen Maßnahmen zur kontinuierlichen Verbesserung zu ergreifen.
Risikomanagement: Prozess um Risiken, die die Informationssicherheit betreffen, zu identifizieren, zu analysieren und zu bewerten und durch entsprechende Maßnahmen zu steuern.
BCM und BIA/Notfallvorsorge/-planung: Prozess der sich mit den möglichen Auswirkungen von Vorfällen und Katastrophen auf den Geschäftsbetrieb mit Schwerpunkt auf die IT auseinandersetzt (BIA) und in dem Notfallpläne für verschiedene Szenarien erstellt und getestet werden, um in Ausnahmesituationen eine geregelte Fortführung der Geschäftstätigkeiten zu ermöglichen.
Personal Management: Tätigkeiten im Bereich der personellen Sicherheit. Insbesondere in Bezug zum Mitarbeiter-Ein- und Austrittsprozess, zu Rechte- und Assetvergabe/-entzug und zu Vorgaben zur korrekten/zulässigen Verwendung von (IT-) Systemen.
Awareness Schulungen: Schulungen der Mitarbeiter zu Informationssicherheits-Relevanten Themen (wie etwa E-Mail-Sicherheit, Phishing, Spam & Viren, mobile Sicherheit, interne Regelungen etc.), um deren Sicherheitsbewusstsein zu verbessern und eine sichere Benutzung von IT-Systemen zu ermöglichen.
Vulnerability Management: Prozess der sich mit der Identifikation, Analyse, Bewertung und dem Beheben/der Behandlung von Schwachstellen (etwa durch Patches) in Systemen des Unternehmens auseinandersetzt.
Change Management: Prozess der sich mit der kontrollierten Durchführung von Änderungen an IT Assets auseinandersetzt und der Themen wie die Freigabe, Autorisierung, Tests und Dokumentation von Änderungen umfasst.
Configuration/Capacity Management: Prozess zum Management der (sicheren) Konfiguration von Assets sowie zur Analyse von derzeitigen und Planung von zukünftigen Kapazitätsanforderungen, der eng mit dem Change Management verbunden ist.
Physische Sicherheit: Prozess der sich mit Maßnahmen im Bereich der physischen Sicherheit des Standortes, des Serverraums und von Geräten beschäftigt und Themen wie Zugangs-/Zugriffsschutz, Überwachung, USV, Kühlung/Klima, Brandschutz, Wassereinbruchschutz etc. behandelt.
Asset Management: Prozess der sich mit der Verwaltung und Inventarisierung aller Assets einer Organisation beschäftigt. Für Assets werden unter anderem Verantwortliche und zulässige Nutzungsmöglichkeiten festgelegt.
Informationsklassifikation und –Verarbeitung: Prozess der Vorgaben zur Klassifikation und Kennzeichnung aller im Unternehmen vorhandenen Informationen jeglicher Art und Form (elektronisch, auf Papier etc.) festlegt und in dem je Klassifikationslevel die zulässige Nutzung, Verarbeitung, Vervielfältigung und der zulässigen Transport von Daten geregelt wird.

Identitäts- und Zugriffsmanagement: Prozess der für eine geregelte Verwaltung von Benutzerkonten auf allen Systemen und die Vergabe und regelmäßige Überprüfung von Zugriffsrechten (nach dem Need to Know und Least Privileged Prinzip) zuständig ist.
Vorfallmanagement: Prozess der sich mit der Meldung, Klassifikation, Eskalation und Behandlung (sowie Dokumentation) von IT-Sicherheitsvorfällen auseinandersetzt, um eine zeitgerechte Reaktion auf solche zu ermöglichen und mögliche Problemursachen zu beheben.
Patch & Update Management: Prozess der sich mit der Identifikation, dem Test und der Ausrollung von Patches & Updates auf Systemen des Unternehmens beschäftigt.
Backup & Wiederherstellung: Prozess der der Steuerung von Maßnahmen im Bereich des Sicherung & Wiederherstellung von Daten und Konfigurationen von allen Systemen dient. Er umfasst die regelmäßige Erstellung von Backups, deren korrekte und sichere Verwahrung und die Durchführung von Wiederherstellungstests.
Logging & (Performance) Monitoring: Prozess der sich mit dem Sammeln und Analysieren (um eventuelle Probleme oder Angriffe zu erkennen) von Log Informationen und Performance Daten befasst.
Spam & Antivirus: Steuerung von Maßnahmen, die im Bereich des Spam und Virenschutz ergriffen werden.
Medien-/Datenvernichtung: Prozess der sich um die korrekte Vernichtung von Daten auf Medien, die aus dem Unternehmen ausgeschieden oder extern repariert/gewartet werden, kümmert. Es soll sichergestellt werden, dass von entsorgten Medien (Papier, Festplatten, USB Sticks, DVDs etc.) keine vertraulichen Informationen wiederhergestellt werden können.
Management der Leistungserbringung/Verträge Externe IT Dienstleister: Prozess der die Leistungserbringung der externe Partner kontrolliert. Er umfasst unter anderem die Festlegung und Verwaltung von SLAs, Berücksichtigung von Security Aspekten in den Verträgen, Forderung einer Zertifizierung und Sicherheitsmaßnahmen des Dienstleistern, die Kontrolle der gewährten Zugriffsrechte und -Möglichkeiten auf eigene Daten und Systeme sowie die Planung für mögliche Ausfälle des Dienstleisters.
Dokumentation: Dokumentation zu eingesetzten Systemen, Konfigurationen, organisatorische Prozessen etc., um Übersichtlichkeit und Nachvollziehbarkeit zu gewährleisten und sicherzustellen, dass es zu keinen kritischen Wissens-/Know-How-Verlusten beim Abgang von Schlüsselpersonal kommt.
Sichere Software-/Webapplikationsentwicklung: Prozess zur sicheren Entwicklung von Software und Webapplikationen, welcher Maßnahmen wie etwa einen SDLC, Sicherheitstest und Source Code Reviews etc. umfasst.
Versicherung gegen Cyber/IT-Angriffe: Zusatzversicherung für Unternehmen, die Schäden im Zusammenhang mit Hacker-Angriffen oder sonstigen Akten von Cyberkriminalität absichert. Cyber-Versicherungen gleichen nicht nur den direkten Schaden aus, den der Angriff verursacht hat, sondern decken vor allem auch die Kosten, die mit der vollständigen Wiederherstellung der Geschäftstätigkeit verbunden sind (System-Wiederherstellung, Beratung, Forensik, Rechtskosten etc.).
Firmeneigenes CERT: Sicherheitsexperten die sich speziell mit der Reaktion auf IT Sicherheitsvorfälle und allgemein mit Computersicherheit befassen. Außerdem erfolgt Kommunikation und Koordination mit nationalen und internationalen bzw. branchenspezifischen CERTs.
Durchführung/Teilnahme an Cyber Übungen: Durchführung von internen Notfall-/Cyber-Übungen sowie Teilnahme an nationalen oder internationalen Cyber-Übungen.
Quellen: BSI Cyber Sicherheit Glossar, wikipedia

8. Demographische Daten

Vielen Dank, dass Sie die Fragen beantwortet haben!

Nun möchte ich Sie für die Auswertung noch um einige demographische Angaben ersuchen, wobei zumindest die Angabe der Mitarbeiteranzahl und des Hauptstandortes erforderlich ist.

Studie Informationssicherheit in Deutschland, Schweiz und Österreich

*22. Wie viele Mitarbeiter beschäftigt Ihr Unternehmen?

- 1-49
- 50-249
- 250-999
- >1000
- keine Angabe

*23. Wo ist der Hauptstandort Ihres Unternehmens?

- Deutschland
- Österreich
- Schweiz
- keine Angabe
- Anderer bitte nennen

24. In welcher Branche ist Ihr Unternehmen tätig?

- Land- und Forstwirtschaft, Fischerei
- Bergbau und Gewinnung von Steinen und Erden
- Herstellung von Waren
- Energieversorgung
- Wasserversorgung, Abwasser und Abfallentsorgung und Beseitigung von Umweltverschmutzungen
- Bau
- Handel, Instandhaltung und Reparatur von Kraftfahrzeugen
- Verkehr und Lagerei
- Beherbergung und Gastronomie
- Information und Kommunikation
- Erbringung von Finanz- und Versicherungsdienstleistungen
- Grundstücks- und Wohnungswesen
- Erbringung von freiberuflichen, wissenschaftlichen und technischen Dienstleistungen
- Erbringung von sonstigen wirtschaftlichen Dienstleistungen
- Öffentliche Verwaltung, Verteidigung, Sozialversicherung
- Erziehung und Unterricht
- Gesundheits- und Sozialwesen
- Kunst, Unterhaltung und Erholung
- Erbringung von sonstigen Dienstleistungen
- Private Haushalte mit Hauspersonal, Herstellung von Waren und Erbringung von Dienstleistungen durch private Haushalte für den Eigenbedarf ohne ausgeprägten Schwerpunkt
- Exterritoriale Organisationen und Körperschaften

Studie Informationssicherheit in Deutschland, Schweiz und Österreich

25. Welchen Aufgabenbereich erfüllen Sie in Ihrem Unternehmen?

- ○ Geschäftsführer
- ○ Aufsichtsrat
- ○ IT-Leiter/IT-Sicherheitsmanager
- ○ CISO/Informationssicherheits-Beauftragter
- ○ Datenschutzbeauftragter
- ○ Systemadministrator
- ○ Netzwerkadministrator
- ○ Risikomanager
- ○ Sonstiges (bitte angeben)

9. Ende & Dank

Vielen Dank, dass Sie sich die Zeit genommen haben, die Umfrage auszufüllen und somit einen wertvollen Beitrag zu meiner Studie geleistet haben.

Falls Ihnen die Umfrage gefallen hat freue ich mich sehr, wenn Sie mich bei der Verteilung unterstützen und den Link zu dieser Studie an Unternehmenskontakte oder Partner weiterleiten.

https://de.surveymonkey.com/r/Studie-Informationssicherheit

26. Falls Sie Einsicht in die Ergebnisse der Umfrage erwünschen, ersuche ich Sie um eine E-Mail-Adresse, an die Ihnen meine Zusammenfassung geschickt wird, sobald die Auswertung abgeschlossen ist.

E-Mail-Adresse:

27. Kommentare und Anregungen zu der Umfrage (Inhalt, Umfang, Verbesserungspotential) können Sie gerne hier abgeben. Für Ihre Rückmeldungen bin ich Ihnen sehr dankbar!

Philipp Reisinger BSc.
Master Student im Studiengang Information Security
e-mail: is131510@fhstp.ac.at
Fachhochschule St. Pölten GmbH
Matthias Corvinus-Straße. 15, A-3100 St. Pölten

Schlussendlich möchte ich mich abermals bei dem ADV, bei Computerwelt, bei Cyber Security Austria, der IT-Security Experts Group der WKÖ, dem IKT-Sicherheitsportal, ISACA Austria, der SBA Research, der FH St. Pölten sowie den vielen anderen Helfern für die Unterstützung bei der Durchführung und Verteilung dieser Umfrage bedanken!

A.2. Weitere Abbildungen

Im Folgenden ist ein Vergleich der technischen und organisatorischen Aufstellung von Unternehmen, welchen von bzw. nicht von Informationssicherheits Vorfällen betroffen waren.

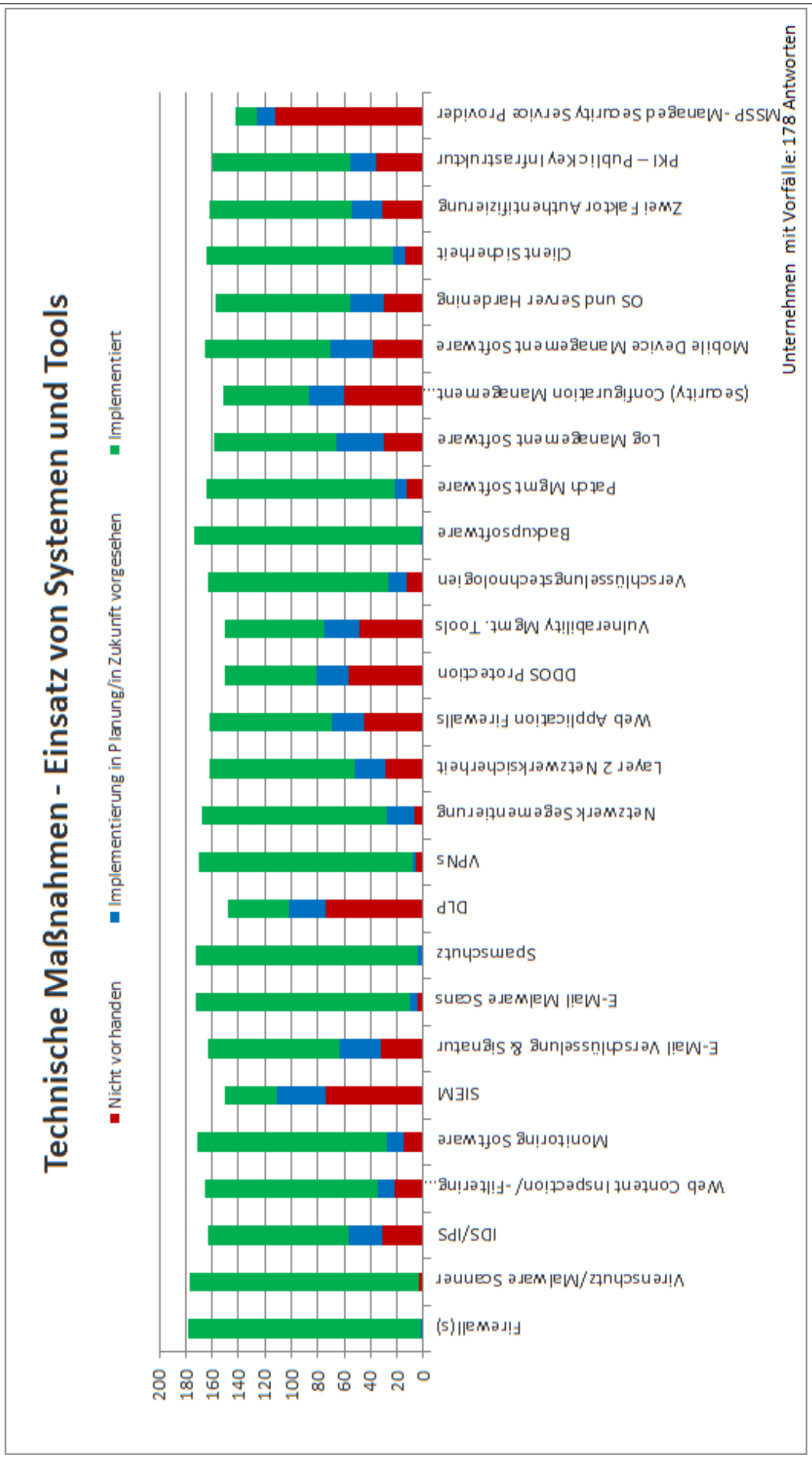

Abbildung A.1.: Technische Maßnahmen - Einsatz technischer Systeme und Tools - Unternehmen mit Vorfällen

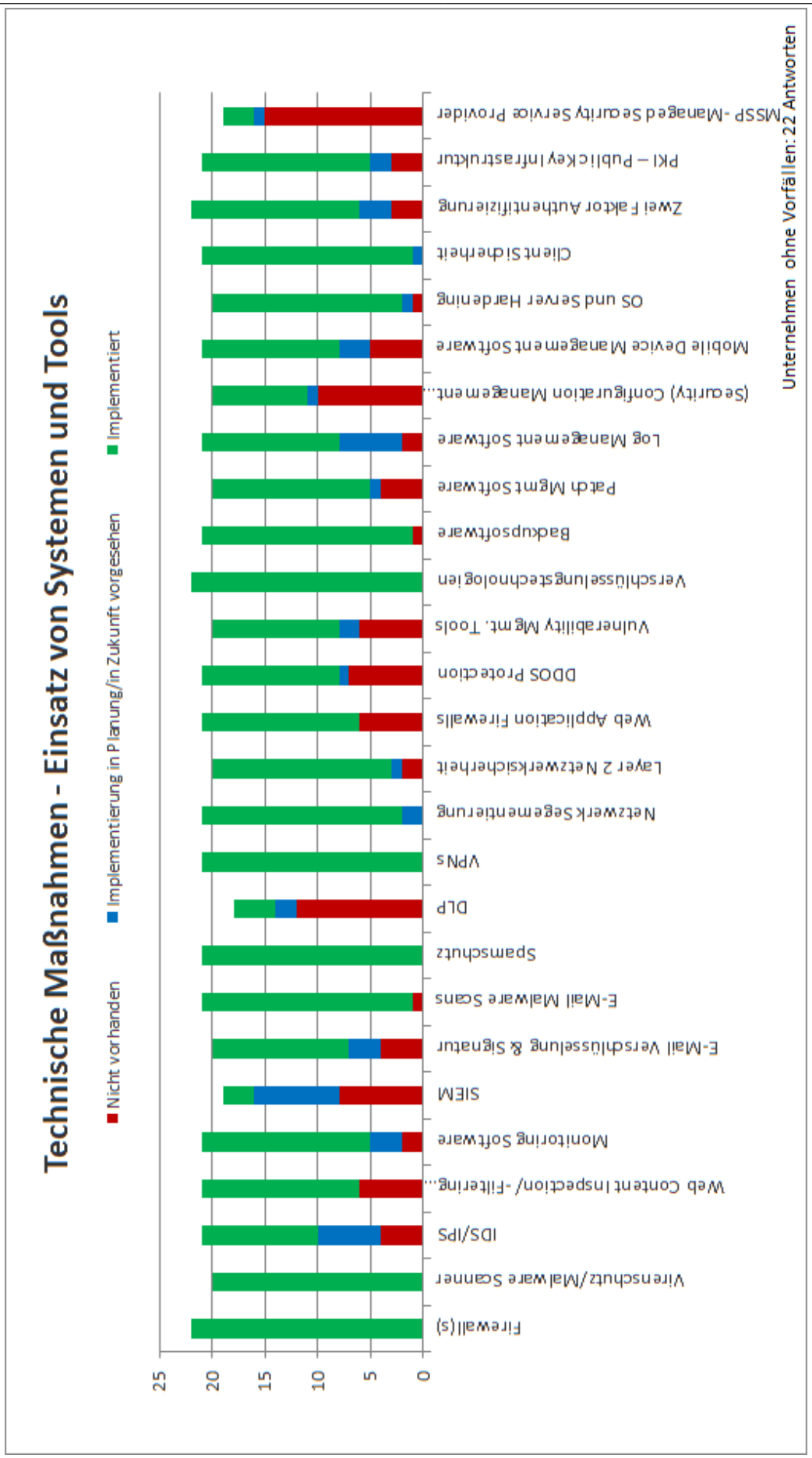

Abbildung A.2.: Technische Maßnahmen - Einsatz technischer Systeme und Tools - Unternehmen ohne Vorfälle

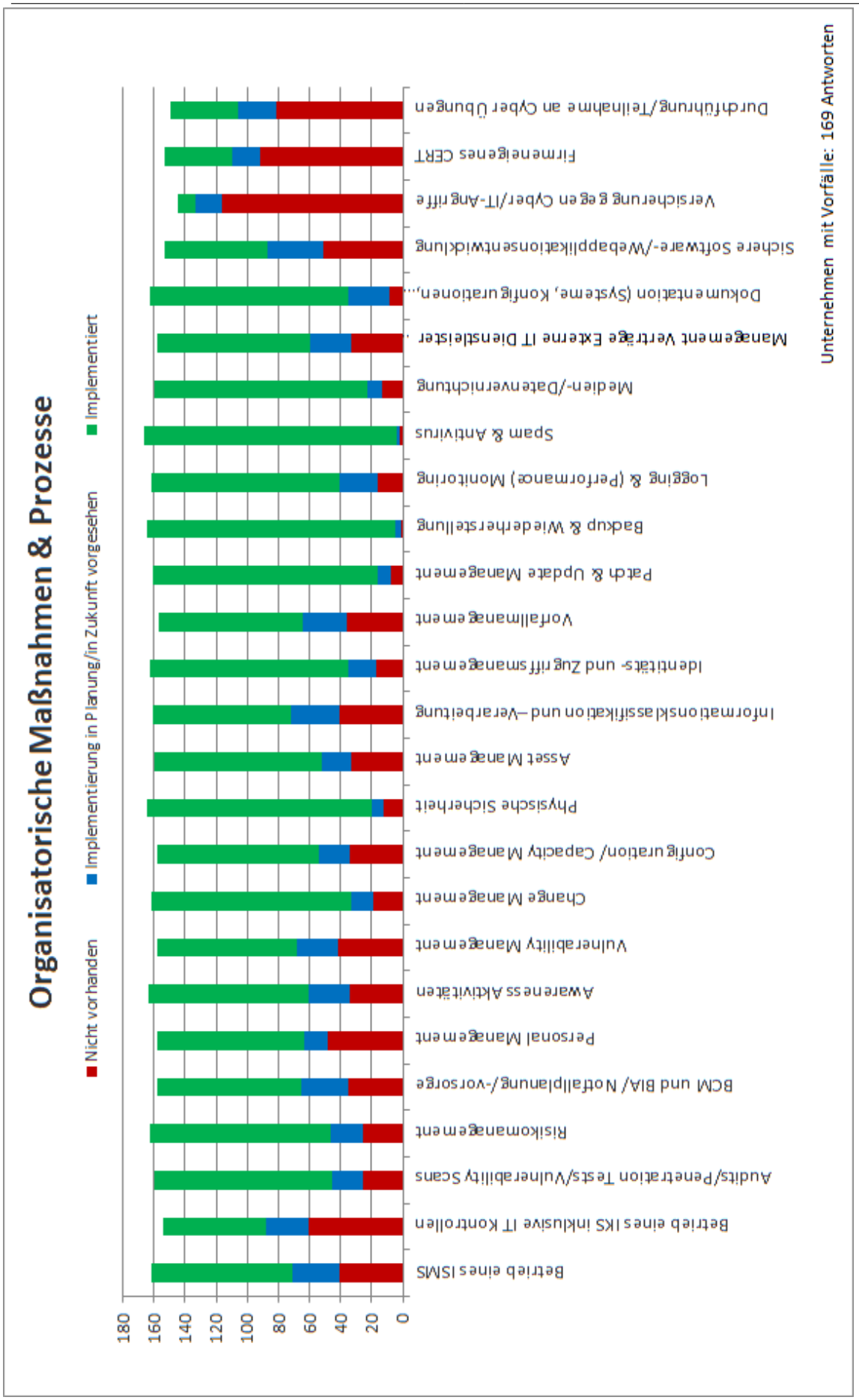

Abbildung A.3.: Organisatorische Maßnahmen & Prozesse - Unternehmen mit Vorfällen

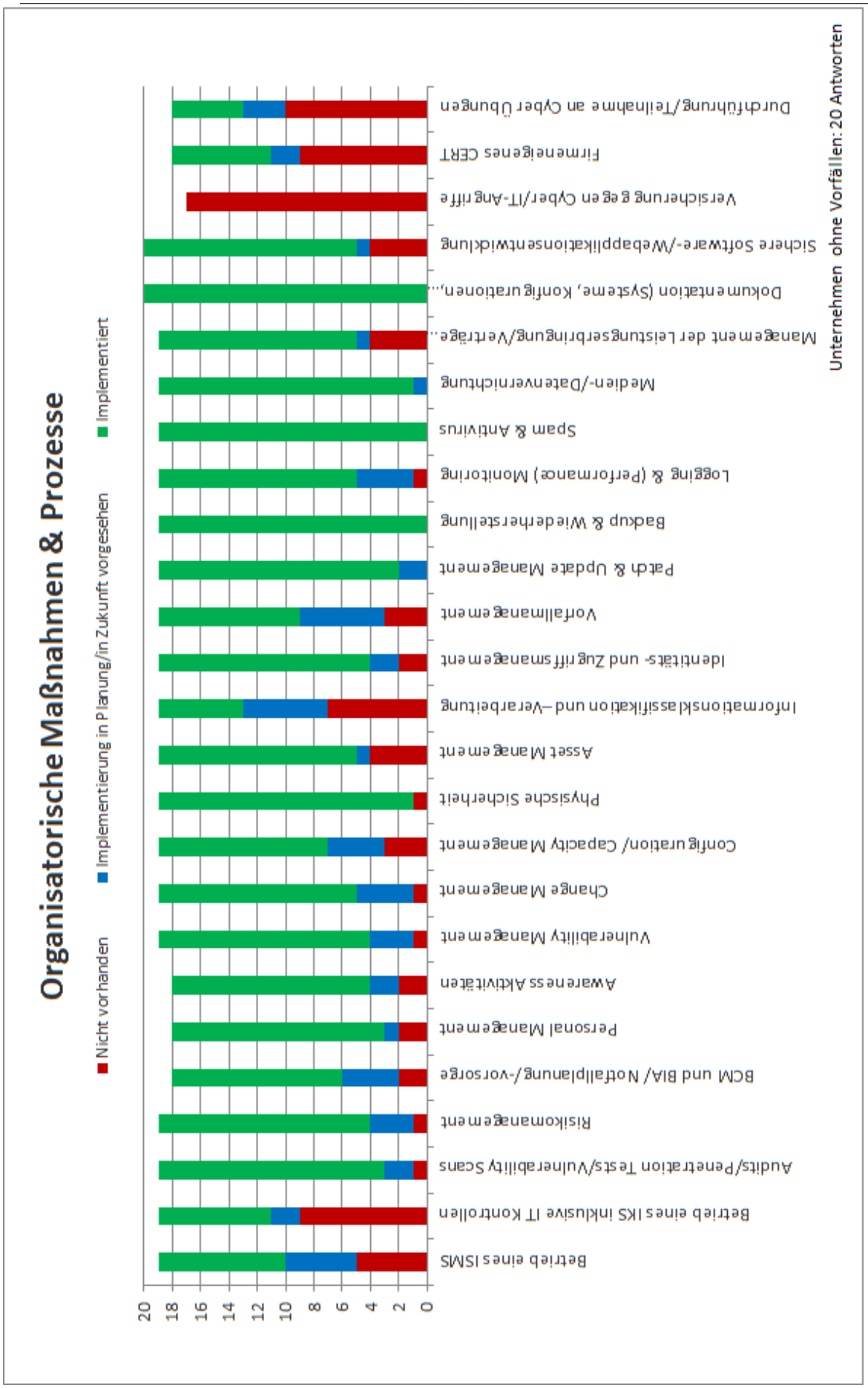

Abbildung A.4.: Organisatorische Maßnahmen & Prozesse - Unternehmen ohne Vorfälle

A.3. Alle Detailergebnisse

Im Folgenden sind alle Detailergebnisse der einzelnen Fragen ersichtlich. Je Fragen werden sowohl die gesamten, als auch die länderspezifischen Beantwortungen aufgeführt.

Frage 1: Denken Sie an die wichtigsten IT-Systeme/Services/Ressourcen in Ihrem Unternehmen. Wie lange dürfte diese ausfallen, ohne Ihr Kerngeschäft stark negativ zu beeinträchtigen oder unmöglich zu machen?	**D**	**Ö**	**Ch**	**Ges**
Wenige Stunden: sehr starke Abhängigkeit von IT	46,4%	65,9%	50,8%	57,6%
1 Tag: starke Abhängigkeit von IT	37,5%	22,0%	40,0%	31,4%
2 Tage: Abhängigkeit von IT lediglich in Teilbereichen	8,9%	9,8%	7,7%	7,9%
> 2 Tage: geringe Abhängigkeit von IT	7,1%	2,4%	1,5%	3,1%
Anzahl Beantwortungen	***56***	***82***	***65***	***229***
Legende: Hell-/Dunkelgrau Min/Max der Zeilen, bei Ges Min/Max der Spalte				

Tabelle A.1.: Frage 1, Abhängigkeit von IT

Frage 2: Denken Sie an die wichtigsten Daten und Informationen in Ihrem Unternehmen. Als wie schwerwiegend schätzen Sie die Auswirkungen bei deren Verlust, Nichtverfügbarkeit oder Verfälschung bzw. bei einer Veröffentlichung - etwa an Mitbewerber - ein?	**D**	**Ö**	**Ch**	**Ges**
Niedrig: Das Geschäft des Unternehmens wird kaum beeinträchtig und es ist nur mit sehr geringen Konsequenzen zu rechnen.	3,6%	7,3%	1,6%	4,0%
Mittel: Das Kerngeschäft wird spürbar beeinträchtigt und es ist mit gewissen Geldverlusten, Know-How-Verlusten, Imageschäden oder rechtlichen Konsequenzen zu rechnen.	19,6%	14,6%	23,8%	17,6%
Hoch: Das Kerngeschäft wird stark beeinträchtigt und es ist mit Geldverlusten, Know-How-Verlusten, Imageschäden und rechtlichen Konsequenzen zu rechnen.	26,8%	25,6%	25,4%	26,0%
Sehr hoch: Das Kerngeschäft des Unternehmens wird sehr stark negativ beeinträchtigt. Es ist mit schwerwiegenden Imageschäden, Know-How-Verlusten, Geldverlusten und rechtlichen Konsequenzen zu rechnen. Außerdem werden langfristige Auswirkungen auf die Neukunden- bzw. Auftragsgewinnung erwartet.	50,0%	52,4%	49,2%	52,4%
Anzahl Beantwortungen	***56***	***82***	***63***	***227***
Legende: Hell-/Dunkelgrau Min/Max der Zeilen, bei Ges Min/Max der Spalte				

Tabelle A.2.: Frage 2, Wichtigkeit von Daten und Informationen

Frage 3: Als wie wichtig wird das Thema Informationssicherheit in Ihrem Unternehmen angesehen und wie sehr ist die Informationssicherheit in unternehmerische Tätigkeiten integriert und berücksichtigt?	**D**	**Ö**	**Ch**	**Ges**
Unwichtig/nebensächlich, Keine besondere Berücksichtigung von Informationssicherheit in wesentlichen Geschäftsprozessen.	0,0%	1,2%	0,0%	0,4%
Weniger wichtig, Informationssicherheit ist mehrheitlich IT Thema und dort angesiedelt	17,9%	23,2%	27,7%	21,8%
Wichtig, Es gibt eine dedizierte Rolle, die für Informationssicherheit verantwortlich ist. Diese übernimmt auch die Kommunikation und Abstimmung mit den Fachbereichen/Geschäftsprozessen.	44,6%	40,2%	38,5%	40,2%
Sehr wichtig, Informationssicherheit ist in allen wesentlichen Geschäftsprozessen ein definierter, integraler Bestandteil, mit festgelegten Sicherheitsmaßnahmen und Verantwortlichkeiten	37,5%	35,4%	33,8%	37,6%
Anzahl Beantwortungen	***56***	***82***	***65***	***229***
Legende: Hell-/Dunkelgrau Min/Max der Zeilen, bei Ges Min/Max der Spalte				

Tabelle A.3.: Frage 3, Wichtigkeit der Informationssicherheit

Frage 4: Welches sind die (Top 5) Gründe Ihres Unternehmens sich mit dem Thema Informationssicherheit auseinanderzusetzen?	**D**	**Ö**	**Ch**	**Ges**
Gesetzliche Vorgaben (Datenschutz, EU-Richtlinien)/Compliance	87,3%	73,2%	81,5%	80,3%
Vermeidung von (Geld/Image)Verlusten durch Sicherheitsvorfälle oder Datenpannen	67,3%	69,5%	72,3%	71,5%
Datenverlusten/Verfälschung vorbeugen	63,6%	68,3%	70,8%	68,9%
Stabilität des Betriebs sicherstellen	56,4%	57,3%	50,8%	53,5%
Haftung gegenüber Dritten	36,4%	26,8%	27,7%	30,7%
Forderung von Kunden/Partnern	38,2%	22,0%	38,5%	32,0%
Als Wettbewerbsvorteil/zum Marketing (Zertifizierungen)	23,6%	17,1%	12,3%	16,2%
Vorfälle in der Vergangenheit (Ausfälle von IT-Systemen, Einbrüche in IT-Systeme, Hacking, Datenverluste etc.)	5,5%	23,2%	24,6%	18,4%
Starke Abhängigkeit von eigener IT in gewissen Geschäftsprozessen	50,9%	59,8%	60,0%	55,7%
Wirtschaftsprüfung, Jahresabschluss, Due Diligence	14,5%	23,2%	23,1%	22,4%
Vorfälle, über die in Medien berichtet wurde	7,3%	15,9%	12,3%	12,7%
NSA-Überwachungsskandal	3,6%	4,9%	1,5%	3,1%
Sonstiges (bitte angeben)	1,8%	3,7%	3,1%	3,5%
Anzahl Beantwortungen	***55***	***82***	***65***	***228***
Legende: Hell-/Dunkelgrau auffällige Min/Max der Zeilen, bei Ges Min/Max der Spalte				

Tabelle A.4.: Frage 4, Gründe und Motivation für Informationssicherheit

Frage 5: Setzt sich Ihr Unternehmen mit Standards/Empfehlungen im Bereich der Informationssicherheit auseinander?	**D**	**Ö**	**Ch**	**Ges**
keine Verwendung von speziellen Standards/Empfehlungen	5,7%	21,0%	12,7%	12,7%
ISO 27001	62,3%	60,5%	84,1%	69,1%
BSI - IT-Grundschutz	64,2%	42,0%	57,1%	52,3%
ITIL	35,8%	50,6%	57,1%	49,1%
COBIT	13,2%	27,2%	36,5%	26,4%
BSI - Leitfaden Informationssicherheit - IT-Grundschutz kompakt	37,7%	32,1%	30,2%	31,8%
IT-Beauftragter der Bayerischen Staatsregierung - Leitfaden zur Informationssicherheit in kleinen und mittleren Unternehmen	7,5%	1,2%	0,0%	2,3%
BITKOM - Sicherheit für Systeme und Netze in Unternehmen - Einführung in die IT-Sicherheit, Leitfaden für erste Maßnahmen	17,0%	1,2%	0,0%	5,5%
Österreichische Informationssicherheitshandbuch	0,0%	25,9%	0,0%	10,9%
WKÖ - IT Sicherheitshandbuch	0,0%	12,3%	1,6%	5,0%
SANS CSC - Critical Security Controls	11,3%	11,1%	9,5%	10,9%
PCI DSS	9,4%	11,1%	9,5%	11,8%
OWASP Top 10	24,5%	33,3%	44,4%	32,7%
Sonstiges (bitte angeben)	7,5%	12,3%	22,2%	14,1%
Anzahl Beantwortungen	***53***	***81***	***63***	***220***
Legende: Hell-/Dunkelgrau auffällige Min/Max der Zeilen, bei Ges Min/Max der Spalte				

Tabelle A.5.: Frage 5, Nutzung von Standards & Empfehlungen im Bereich der Informationssicherheit

Frage 6: Was sind Ihrer Meinung nach die (Top 5) Hauptrisiken/Bedrohung in Bezug zur Informationssicherheit, denen Ihr Unternehmen ausgesetzt ist?	D	Ö	Ch	Ges
Malware (Viren, Trojaner, Spyware etc.)	63,0%	56,1%	49,2%	57,3%
Hacking	24,1%	32,9%	20,0%	26,9%
(D)DoS Angriffe	22,2%	15,9%	16,9%	18,5%
APTs (zielgerichtete, komplexe, fortgeschrittene Angriffe)	27,8%	30,5%	32,3%	30,8%
Angriffe auf Website und Datenbanken	27,8%	19,5%	12,3%	22,9%
Abhören/Spionage	13,0%	12,2%	9,2%	11,9%
Betrug	9,3%	7,3%	15,4%	10,1%
Social Engineering	35,2%	24,4%	33,8%	30,0%
(Spear)Phishing	20,4%	18,3%	18,5%	21,1%
Spam	16,7%	22,0%	13,8%	17,6%
Einbrüche bzw. Diebstahl Systeme/mobile Geräte	9,3%	15,9%	10,8%	11,9%
Hardware- oder Software-Fehler	25,9%	28,0%	24,6%	24,7%
Datenverluste (Daten gelöscht/verloren, nicht mehr wiederherstellbar)	22,2%	41,5%	36,9%	34,4%
Datendiebstahl (unautorisierte Person erlangt Daten)	51,9%	43,9%	56,9%	49,3%
(unbemerkte) Datenmanipulation	11,1%	30,5%	21,5%	21,1%
Katastrophen/Höhere Gewalt	14,8%	11,0%	9,2%	10,6%
Stromausfälle	9,3%	9,8%	1,5%	6,6%
Insider-Missbrauch von Rechten/Systemen	22,2%	28,0%	30,8%	26,0%
Fahrlässigkeit eigener Mitarbeiter	38,9%	46,3%	32,3%	39,6%
bewusstes schadhaftes Verhalten eigener Mitarbeitern	9,3%	22,0%	15,4%	16,3%
Ausfälle oder Fehler von externen Partnern/Cloud	5,6%	13,4%	6,2%	9,3%
Einsatz mobiler Geräte (BYOD)	11,1%	13,4%	15,4%	13,7%
Social Media	0,0%	2,4%	3,1%	1,8%
Sonstiges (bitte angeben)	1,9%	3,7%	0,0%	1,8%
Anzahl Beantwortungen	***54***	***82***	***65***	***227***
Legende: Hell-/Dunkelgrau auffällige Min/Max der Zeilen, bei Ges Min/Max der Spalte				

Tabelle A.6.: Frage 6, Hauptrisiken & Bedrohung in Bezug zur Informationssicherheit

Frage 7: Welches sind Ihrer Meinung nach die (Top 5) Hauptprobleme/hemmende Faktoren bei der Aufrechterhaltung/Verbesserung der Informationssicherheit in Ihrem Unternehmen?	**D**	**Ö**	**Ch**	**Ges**
Fehlendes Budget	48,1%	62,5%	47,7%	54,0%
Fehlende Unterstützung und Bewusstsein (z.B. zu Risiken und Gefahren) im (Top)Management	51,9%	53,8%	58,5%	54,5%
Fehlendes Bewusstsein der Mitarbeiter	59,3%	67,5%	67,7%	66,1%
Mangelndes Detail/Spezialwissen (zu Gefahren/Angriffsvektoren und notwendigen Maßnahmen)	29,6%	27,5%	33,8%	29,5%
Mangelnde Beratungsmöglichkeiten	3,7%	5,0%	3,1%	3,6%
Fehlende (technische) Lösungen	13,0%	22,5%	15,4%	19,6%
Fehlende Mitarbeiter-Akzeptanz für Sicherheitsmaßnahmen, die die Usability/Benutzbarkeit einschränken	68,5%	63,8%	64,6%	65,2%
Datenschutzbedenken	14,8%	18,8%	7,7%	14,7%
Sich schnell ändernde Systemumgebung und Angriffsarten	42,6%	47,5%	35,4%	42,0%
Sonstiges (bitte angeben)	7,4%	12,5%	3,1%	7,6%
Anzahl Beantwortungen	***54***	***80***	***65***	***224***
Legende: Hell-/Dunkelgrau auffällige Min/Max der Zeilen, bei Ges Min/Max der Spalte				

Tabelle A.7.: Frage 7, Hauptprobleme bei der Aufrechterhaltung & Verbesserung der Informationssicherheit

Frage 8: Gibt es in dem Unternehmen einen IT-/Informationssicherheits-Verantwortlichen (*) und gibt es eine Informationssicherheits-Policy?	**D**	**Ö**	**Ch**	**Ges**
Ja, Verantwortlicher und Informationssicherheits-Policy	83,6%	66,7%	80,0%	76,2%
Verantwortlicher, aber keine Informationssicherheits-Policy	12,7%	22,2%	7,7%	14,3%
Kein Verantwortlicher und keine Informationssicherheits-Policy	3,6%	11,1%	12,3%	9,4%
Anzahl Beantwortungen	***55***	***81***	***65***	***223***
Legende: Hell-/Dunkelgrau auffällige Min/Max der Zeilen, bei Ges Min/Max der Spalte				

Tabelle A.8.: Frage 8, Informationssicherheits-Verantwortliche und Informationssicherheits-Policy

Frage 9: Gibt es in Ihrem Unternehmen Richtlinien/Vorgaben in Bezug zur Informationssicherheit?	D	Ö	Ch	Ges
Keine Richtlinien/Vorgaben	1,8%	9,9%	9,2%	6,7%
Nutzung Mail, Internet & Social Media	94,5%	70,4%	87,7%	84,3%
Nutzung mobiler Geräte (etwa auch BYOD) und Speichermedien	76,4%	54,3%	76,9%	68,2%
Clear Desk/ Clear Screen	54,5%	45,7%	61,5%	54,3%
Akzeptable/Zulässige Verwendung Endbenutzer-IT	61,8%	54,3%	53,8%	55,6%
Datenvernichtung und Geräteentsorgung	78,2%	69,1%	69,2%	71,7%
Passwortrichtlinien	96,4%	79,0%	86,2%	86,5%
Informationsklassifikation & Verarbeitung	54,5%	45,7%	64,6%	56,1%
Dokumentationsvorgaben/-anforderungen	54,5%	43,2%	36,9%	43,9%
Sicherheitsvorgaben für Partner und Dienstleister	61,8%	56,8%	53,8%	57,4%
Sonstiges (bitte angeben)	1,8%	3,7%	1,5%	3,1%
Anzahl Beantwortungen	***55***	***81***	***65***	***223***
Legende: Hell-/Dunkelgrau auffällige Min/Max der Zeilen, bei Ges Min/Max der Spalte				

Tabelle A.9.: Frage 9, Richtlinien & Vorgaben in Bezug zur Informationssicherheit

Frage 10: Führen Sie in regelmäßigen Abständen interne/externe Audits, Penetration Tests oder Vulnerability Scans durch, um die Informationssicherheit bewerten zu können?	D	Ö	Ch	Ges
Durchführung von internen Audits	74,5%	66,7%	69,2%	70,4%
Durchführung von externen Audits	52,7%	46,9%	75,4%	58,7%
Durchführung von Penetration Tests	52,7%	59,3%	55,4%	57,8%
Durchführung von Vulnerability Scans	40,0%	59,3%	61,5%	56,5%
Keine regelmäßigen Überprüfungsaktivitäten	10,9%	21,0%	15,4%	14,8%
Anzahl Beantwortungen	***55***	***81***	***65***	***223***
Legende: Hell-/Dunkelgrau auffällige Min/Max der Zeilen, bei Ges Min/Max der Spalte				

Tabelle A.10.: Frage 10, Aktivitäten zur Überprüfung der Informationssicherheit

Frage 11: Wurden im letzten Jahr Beratungstätigkeiten zu Informationssicherheits-Themen durch externe Unternehmen wahrgenommen?	**D**	**Ö**	**Ch**	**Ges**
Keine externe Beratung	29,6%	33,3%	23,4%	28,3%
Informationssicherheits-Strategie- und Managementberatung	24,1%	19,8%	28,1%	21,9%
Durchführung von Schulungen	29,6%	22,2%	25,0%	25,6%
Durchführung von Audits, Penetration Tests	51,9%	53,1%	70,3%	58,9%
Durchführung von Risikoanalysen	18,5%	22,2%	32,8%	23,3%
Beratung bei Produkterwerb und Implementierung	25,9%	21,0%	15,6%	21,9%
Entwicklung von Informationssicherheits-Prozessen und -Maßnahmen sowie Optimierung dieser	22,2%	19,8%	14,1%	19,2%
Incident Response	9,3%	11,1%	3,1%	7,3%
Forensik	9,3%	11,1%	6,3%	9,1%
Sonstiges (bitte angeben)	1,9%	3,7%	0,0%	1,8%
Anzahl Beantwortungen	***54***	***81***	***64***	***219***
Legende: Hell-/Dunkelgrau auffällige Min/Max der Zeilen, bei Ges Min/Max der Spalte				

Tabelle A.11.: Frage 11, Beratungstätigkeiten zu Informationssicherheits-Themen durch Externe

Frage 12: Gab es in Ihrem Unternehmen im letzten Jahr Vorfälle im Bereich der Informationssicherheit und wenn ja, in welchem Teilgebiet?	**D**	**Ö**	**Ch**	**Ges**
Keine Vorfälle	7,4%	12,7%	12,5%	11,1%
Malware (Viren, Trojaner, Spyware etc.)	57,4%	55,7%	46,9%	53,5%
Hacking	7,4%	7,6%	9,4%	9,7%
(D)DoS Angriffe	11,1%	19,0%	12,5%	15,2%
APTs (zielgerichtete, komplexe, fortgeschrittene Angriffe)	5,6%	7,6%	4,7%	5,5%
Angriffe auf Website und Datenbanken	14,8%	19,0%	12,5%	17,1%
Abhören/Spionage	1,9%	2,5%	1,6%	2,3%
Betrug	9,3%	5,1%	7,8%	6,5%
Social Engineering	13,0%	11,4%	17,2%	14,7%
(Spear)Phishing	13,0%	19,0%	26,6%	21,2%
Spam	51,9%	48,1%	39,1%	46,5%
Einbrüche bzw. Diebstahl Systeme/mobile Geräte	18,5%	12,7%	9,4%	13,4%
Hardware- oder Software-Fehler	27,8%	32,9%	21,9%	28,6%
Datenverluste (Daten gelöscht/verloren, nicht mehr wiederherstellbar)	14,8%	17,7%	14,1%	15,7%
Datendiebstahl (unautorisierte Person erlangt Daten)	1,9%	0,0%	6,3%	3,2%
(unbemerkte) Datenmanipulation	5,6%	0,0%	0,0%	1,4%
Katastrophen/Höhere Gewalt	0,0%	0,0%	1,6%	0,9%
Stromausfälle	25,9%	26,6%	21,9%	25,3%
Insider Missbrauch von Rechten/Systemen	13,0%	6,3%	6,3%	7,4%
Fahrlässigkeit Mitarbeiter	33,3%	27,8%	26,6%	28,6%
bewusstes schadhaftes Verhalten eigener Mitarbeitern	7,4%	2,5%	3,1%	3,7%
Ausfälle oder Fehler von externen Partnern/Cloud	13,0%	7,6%	7,8%	8,3%
Einsatz mobiler Geräte (BYOD)	5,6%	5,1%	9,4%	6,5%
Social Media	1,9%	2,5%	3,1%	2,3%
Sonstiges (bitte angeben)	1,9%	6,3%	12,5%	7,4%
Anzahl Beantwortungen	***54***	***79***	***64***	***217***
Legende: Hell-/Dunkelgrau auffällige Min/Max der Zeilen, bei Ges Min/Max der Spalte				

Tabelle A.12.: Frage 12, Vorfälle im Bereich der Informationssicherheit

Frage 13: Werden mobile Geräte (Laptop, Tablets, Smartphones), etwa auch in Form von BYOD, in Ihrem Unternehmen eingesetzt?	D	Ö	Ch	Ges
Ja. Einsatz mobiler Geräte auch in Form von BYOD. Außerdem werden spezielle Sicherheitsmaßnahmen ergriffen (Mobile Device Management, Remote Access und Wipe, Verschlüsselung, interne Regelungen etc.)	27,3%	27,2%	55,4%	37,7%
Ja es werden mobile Geräte und BYOD eingesetzt, jedoch ohne gesonderte Sicherheitsmaßnahmen.	7,3%	18,5%	9,2%	12,3%
Ja Einsatz mobiler Geräte jedoch kein BYOD	47,3%	34,6%	23,1%	33,6%
Nein	18,2%	19,8%	12,3%	16,4%
Anzahl Beantwortungen	***55***	***81***	***65***	***220***
Legende: Hell-/Dunkelgrau auffällige Min/Max der Zeilen, bei Ges Min/Max der Spalte				

Tabelle A.13.: Frage 13, Einsatz von mobilen Geräten und BYOD

Frage 14: Nutzt Ihr Unternehmen Cloud Dienstleistungen oder wird Outsourcing von IT Services betrieben?	**D**	**Ö**	**Ch**	**Ges**
Ja. Außerdem werden spezifische Sicherheitsmaßnahmen ergriffen (heimische/europäische Service Provider, Notfallplanung für den Fall der Nichtverfügbarkeit des Dienstleisters, Verschlüsselung, SLAs, Überprüfungen des Partners und von Zugriffsrechten/-möglichkeiten, Fordern von Zertifizierungen etc.)	52,7%	30,9%	43,1%	43,4%
Ja, jedoch ohne Informationssicherheitsaspekte speziell zu berücksichtigen	5,5%	16,0%	10,8%	10,9%
Nein aufgrund von Sicherheitsbedenken und diverser Vorkommnisse (NSA-Skandal etc.)	7,3%	21,0%	15,4%	14,9%
Nein	34,5%	32,1%	30,8%	30,8%
Anzahl Beantwortungen	***55***	***81***	***65***	***221***
Legende: Hell-/Dunkelgrau auffällige Min/Max der Zeilen, bei Ges Min/Max der Spalte				

Tabelle A.14.: Frage 14, Nutzung Cloud und/oder Outsourcing von IT

Frage 15: Gibt es in Ihrem Unternehmen Mitarbeiter-Awareness-Aktivitäten zum Thema Informationssicherheit und der korrekten Nutzung von informationsverarbeitenden Systemen und wenn ja, in welcher Form werden diese durchgeführt?	**D**	**Ö**	**Ch**	**Ges**
Keine Durchführung von Awareness Aktivitäten	11,1%	23,5%	16,9%	16,8%
Formale Vorgaben in diversen Dokumenten/Richtlinien	70,4%	45,7%	47,7%	53,6%
Intranet Portal	63,0%	44,4%	52,3%	52,3%
Schulungen	53,7%	54,3%	49,2%	53,6%
Newsletter und Infomaterial	48,1%	29,6%	40,0%	38,2%
Workshops	18,5%	18,5%	12,3%	18,2%
Kampagnen	29,6%	18,5%	41,5%	30,5%
Sonstiges (bitte angeben)	7,4%	11,1%	4,6%	7,3%
Anzahl Beantwortungen	***54***	***81***	***65***	***220***
Legende: Hell-/Dunkelgrau auffällige Min/Max der Zeilen, bei Ges Min/Max der Spalte				

Tabelle A.15.: Frage 15, Mitarbeiter-Awareness-Aktivitäten

Frage 16: Wird in Ihrem Unternehmen Open Source Software eingesetzt und wenn ja, treffen Sie Maßnahmen um diese auf Fehlerfreiheit/Korrektheit und Qualität zu überprüfen?	**D**	**Ö**	**Ch**	**Ges**
Kein Einsatz von Open Source Software	12,7%	8,6%	20,6%	12,4%
Kein Einsatz von Open Source Software aufgrund von Sicherheitsbedenken	0,0%	0,0%	1,6%	0,5%
Ja, jedoch keine Überprüfung der Open Source Software	58,2%	61,7%	55,6%	58,1%
Ja, Durchführung von Code Reviews und Recherche zu Auditergebnissen, Sicherheitsanalysen und dem Entwicklerkreis	23,6%	29,6%	19,0%	25,8%
Weiß nicht	5,5%	0,0%	3,2%	3,2%
Anzahl Beantwortungen	***55***	***81***	***63***	***217***
Legende: Hell-/Dunkelgrau auffällige Min/Max der Zeilen, bei Ges Min/Max der Spalte				

Tabelle A.16.: Frage 16, Einsatz von Open Source Software

Frage 17: War Ihr Unternehmen von schwerwiegenden Sicherheitslücken in Open Source Software wie Heartbleed oder Shellshock betroffen?	D	Ö	Ch	Ges
Nein, nicht betroffen	32,7%	22,5%	32,8%	29,0%
Ja, jedoch keine Beeinträchtigung der Geschäftstätigkeiten	60,0%	62,5%	57,8%	59,4%
Ja, Geschäftstätigkeit wurde beeinträchtigt	5,5%	6,3%	3,1%	4,6%
Ja, diese Lücken wurden aktiv für Angriffe auf das Unternehmen ausgenutzt	0,0%	0,0%	1,6%	0,5%
Weiß nicht	1,8%	8,8%	4,7%	6,5%
Anzahl Beantwortungen	***55***	***80***	***64***	***217***
Legende: Hell-/Dunkelgrau auffällige Min/Max der Zeilen, bei Ges Min/Max der Spalte				

Tabelle A.17.: Frage 17, Betroffenheit von Heartbleed und Shellshock

Frage 18: War Ihr Unternehmen im letzten Jahr Ziel eines komplexen, fortgeschrittenen, direkt auf sie gezielten IT-Angriffs (APT-Advanced Persistent Threat) und wenn ja, richtete dieser Schaden an?	D	Ö	Ch	Ges
Nein	53,7%	59,5%	59,4%	56,5%
Ja, dieser richtete Schaden an	1,9%	1,3%	6,3%	2,8%
Ja, jedoch kein Schaden da erfolgreich abgewehrt	9,3%	10,1%	6,3%	9,3%
Es besteht der Verdacht	3,7%	5,1%	4,7%	5,6%
Weiß nicht	31,5%	24,1%	23,4%	25,9%
Anzahl Beantwortungen	***54***	***79***	***64***	***216***
Legende: Hell-/Dunkelgrau auffällige Min/Max der Zeilen, bei Ges Min/Max der Spalte				

Tabelle A.18.: Frage 18, Ziel eines komplexen, fortgeschrittenen, gezielten IT-Angriffs - APT

Frage 19: Waren die NSA-Enthüllungen bezüglich Überwachung und Spionage sowie der gezielten Manipulation von (amerikanischen) Soft- und Hardware-Produkten für Ihr Unternehmen ein Thema bzw. haben Sie darauffolgend spezielle Sicherheitsmaßnahmen ergriffen?	**D**	**Ö**	**Ch**	**Ges**
Nein	46,3%	41,8%	36,5%	39,1%
Ja, jedoch keine gezielten Maßnahmen ergriffen	11,1%	11,4%	28,6%	17,2%
Ja, wachsende Beachtung des Themas der Informationssicherheit	38,9%	35,4%	31,7%	36,7%
Ja, Erhöhung des IT Sicherheitsbudgets	0,0%	3,8%	1,6%	1,9%
Ja, verstärkter Einsatz von Verschlüsselung	13,0%	20,3%	11,1%	16,7%
Ja, im Fall von Cloud oder Outsourcing wird verstärkt auf heimische/europäische Anbieter gesetzt	22,2%	11,4%	15,9%	16,3%
Ja, Planung zur verstärkten Beschaffung von „IT Made in Austria/Germany/Switzerland“ bzw. Europa	9,3%	10,1%	7,9%	9,3%
Ja, sonstige Maßnahmen bitte nennen	5,6%	5,1%	3,2%	5,1%
Anzahl Beantwortungen	***54***	***79***	***63***	***215***
Legende: Hell-/Dunkelgrau auffällige Min/Max der Zeilen, bei Ges Min/Max der Spalte				

Tabelle A.19.: Frage 19, Bedeutung der NSA-Enthüllungen bezüglich Überwachung und Spionage

Frage 20: Welche technischen Systeme, Tools etc. werde im Bereich der Informationssicherheit im Unternehmen eingesetzt bzw. sollen in Zukunft implementiert werden?
Deutschland

Imp: Implementiert, ***Pl***: in Planung bzw. in Zukunft vorgesehen, ***NA***: Nicht vorhanden

Technische Maßnahmen	*Imp*	*Pl*	*NA*	*Ges*
Firewall(s)	54	0	0	54
Virenschutz/Malware Scanner	52	0	0	52
IDS/IPS	28	12	9	49
Web Content Inspection/ -Filtering /Monitoring	40	3	7	50
Monitoring Software	42	5	3	50
SIEM	11	14	22	47
E-Mail Verschlüsselung & Signatur	32	9	7	48
E-Mail Malware Scans	47	3	2	52
Spamschutz	50	2	0	52
DLP	14	9	23	46
VPNs	51	0	1	52
Netzwerk Segmentierung	42	6	1	49
Layer 2 Netzwerksicherheit	37	9	3	49
Web Application Firewalls	26	8	16	50
DDOS Protection	23	5	19	47
Vulnerability Mgmt. Tools	18	10	18	46
Verschlüsselungstechnologien	44	5	1	50
Backupsoftware	51	0	1	52
Patch Mgmt Software	43	1	5	49
Log Management Software	22	17	9	48
(Security) Configuration Management Software	19	6	22	47
Mobile Device Management Software	33	4	12	49
OS und Server Hardening	36	7	6	49
Client Sicherheit	48	2	2	52
Zwei Faktor Authentifizierung	30	11	8	49
PKI-Public Key Infrastruktur	28	9	10	47
MSSP-Managed Security Service Provider	6	3	35	44
Anzahl Beantwortungen				**54**

Legende: Hell-/Dunkelgrau Min/Max der Spalten

Tabelle A.20.: Frage 20, Technische Aufstellung - Deutschland

Frage 20: Welche technischen Systeme, Tools etc. werde im Bereich der Informationssicherheit im Unternehmen eingesetzt bzw. sollen in Zukunft implementiert werden?
Österreich

Imp: Implementiert, ***Pl***: in Planung bzw. in Zukunft vorgesehen, ***NA***: Nicht vorhanden

Technische Maßnahmen	*Imp*	*Pl*	*NA*	*Ges*
Firewall(s)	78	1	1	80
Virenschutz/Malware Scanner	78	0	2	80
IDS/IPS	49	11	17	77
Web Content Inspection/ -Filtering /Monitoring	53	8	17	78
Monitoring Software	63	6	7	76
SIEM	14	19	36	69
E-Mail Verschlüsselung & Signatur	32	19	23	74
E-Mail Malware Scans	74	2	2	78
Spamschutz	76	2	0	78
DLP	18	11	39	68
VPNs	68	2	5	75
Netzwerk Segmentierung	61	12	4	77
Layer 2 Netzwerksicherheit	45	11	19	75
Web Application Firewalls	35	14	24	73
DDOS Protection	32	10	30	72
Vulnerability Mgmt. Tools	36	11	27	74
Verschlüsselungstechnologien	62	7	8	77
Backupsoftware	78	1	0	79
Patch Mgmt Software	63	6	6	75
Log Management Software	42	18	17	77
(Security) Configuration Management Software	27	12	32	71
Mobile Device Management Software	34	20	23	77
OS und Server Hardening	43	13	15	71
Client Sicherheit	62	6	8	76
Zwei Faktor Authentifizierung	45	12	18	75
PKI-Public Key Infrastruktur	46	9	18	73
MSSP-Managed Security Service Provider	8	4	56	68
Anzahl Beantwortungen				**80**

Legende: Hell-/Dunkelgrau Min/Max der Spalten

Tabelle A.21.: Frage 20, Technische Aufstellung - Österreich

Frage 20: Welche technischen Systeme, Tools etc. werde im Bereich der Informationssicherheit im Unternehmen eingesetzt bzw. sollen in Zukunft implementiert werden?

Schweiz

Imp: Implementiert, ***Pl***: in Planung bzw. in Zukunft vorgesehen, ***NA***: Nicht vorhanden

Technische Maßnahmen	*Imp*	*Pl*	*NA*	*Ges*
Firewall(s)	64	0	0	64
Virenschutz/Malware Scanner	62	0	1	63
IDS/IPS	41	7	10	58
Web Content Inspection/ -Filtering /Monitoring	53	3	3	59
Monitoring Software	52	4	7	63
SIEM	19	13	22	54
E-Mail Verschlüsselung & Signatur	45	8	6	59
E-Mail Malware Scans	60	1	1	62
Spamschutz	61	0	0	61
DLP	21	10	24	55
VPNs	61	0	1	62
Netzwerk Segmentierung	54	6	2	62
Layer 2 Netzwerksicherheit	43	5	10	58
Web Application Firewalls	46	2	12	60
DDOS Protection	28	11	16	55
Vulnerability Mgmt. Tools	33	10	11	54
Verschlüsselungstechnologien	53	2	4	59
Backupsoftware	61	1	0	62
Patch Mgmt Software	51	4	4	59
Log Management Software	38	8	8	54
(Security) Configuration Management Software	28	9	18	55
Mobile Device Management Software	39	12	9	60
OS und Server Hardening	42	6	9	57
Client Sicherheit	53	2	4	59
Zwei Faktor Authentifizierung	50	3	7	60
PKI-Public Key Infrastruktur	44	4	11	59
MSSP-Managed Security Service Provider	5	7	38	50
Anzahl Beantwortungen				**64**

Legende: Hell-/Dunkelgrau Min/Max der Spalten

Tabelle A.22.: Frage 20, Technische Aufstellung - Schweiz

Frage 20: Welche technischen Systeme, Tools etc. werde im Bereich der Informationssicherheit im Unternehmen eingesetzt bzw. sollen in Zukunft implementiert werden?

Gesamt

Imp: Implementiert, ***Pl***: in Planung bzw. in Zukunft vorgesehen, ***NA***: Nicht vorhanden

Technische Maßnahmen	*Imp*	*Pl*	*NA*	*Ges*
Firewall(s)	211	1	1	213
Virenschutz/Malware Scanner	207	0	3	210
IDS/IPS	129	31	37	197
Web Content Inspection/ -Filtering /Monitoring	159	14	27	200
Monitoring Software	170	17	17	204
SIEM	48	47	85	180
E-Mail Verschlüsselung & Signatur	122	37	36	195
E-Mail Malware Scans	196	6	5	207
Spamschutz	202	4	0	206
DLP	57	31	89	177
VPNs	195	2	7	204
Netzwerk Segmentierung	171	24	7	202
Layer 2 Netzwerksicherheit	135	25	33	193
Web Application Firewalls	118	24	53	195
DDOS Protection	90	27	66	183
Vulnerability Mgmt. Tools	97	31	56	184
Verschlüsselungstechnologien	171	14	13	198
Backupsoftware	205	2	1	208
Patch Mgmt Software	170	11	16	197
Log Management Software	115	43	34	192
(Security) Configuration Management Software	84	28	72	184
Mobile Device Management Software	118	37	44	199
OS und Server Hardening	131	27	32	190
Client Sicherheit	173	10	14	197
Zwei Faktor Authentifizierung	134	28	35	197
PKI-Public Key Infrastruktur	130	23	40	193
MSSP-Managed Security Service Provider	23	15	134	172
Anzahl Beantwortungen				**213**

Legende: Hell-/Dunkelgrau Min/Max der Spalten

Tabelle A.23.: Frage 20, Technische Aufstellung - Gesamt

Frage 21: Welche organisatorische Maßnahmen/Prozesse sind im Bereich der Informationssicherheit im Unternehmen umgesetzt bzw. sollen in Zukunft eingeführt werden?
Deutschland

Imp: Implementiert, ***Pl***: in Planung bzw. in Zukunft vorgesehen, ***NA***: Nicht vorhanden

Organisatorische Maßnahmen	***Imp***	***Pl***	***NA***	***Ges***
Betrieb eines ISMS	33	10	9	52
Betrieb eines IKS inklusive IT Kontrollen	15	8	25	48
Audits/Penetration Tests/Vulnerability Scans	36	11	5	52
Risikomanagement	34	11	7	52
BCM und BIA/ Notfallplanung/-vorsorge	27	11	13	51
Personal Management	32	5	13	50
Awareness Aktivitäten	37	8	7	52
Vulnerability Management	27	9	14	50
Change Management	35	8	6	49
Configuration/ Capacity Management	35	4	11	50
Physische Sicherheit	50	1	2	53
Asset Management	36	5	9	50
Informationsklassifikation und -Verarbeitung	30	6	14	50
Identitäts- und Zugriffsmanagement	45	5	3	53
Vorfallmanagement	37	8	6	51
Patch & Update Management	48	1	2	51
Backup & Wiederherstellung	53	0	0	53
Logging & (Performance) Monitoring	39	8	4	51
Spam & Antivirus	54	0	0	54
Medien-/Datenvernichtung	46	3	2	51
Management der Leistungserbringung/Verträge Externe IT Dienstleister	32	9	10	51
Dokumentation (Systeme, Konfigurationen, org. Prozesse etc.)	41	10	1	52
Sichere Software-/Webapplikationsentwicklung	20	16	14	50
Versicherung gegen Cyber/IT-Angriffe	6	4	37	47
Firmeneigenes CERT	16	2	31	49
Durchführung/Teilnahme an Cyber Übungen	15	9	23	47
Anzahl Beantwortungen				**54**

Legende: Hell-/Dunkelgrau Min/Max der Spalten

Tabelle A.24.: Frage 21, Organisatorische Aufstellung - Deutschland

Frage 21: Welche organisatorische Maßnahmen/Prozesse sind im Bereich der Informationssicherheit im Unternehmen umgesetzt bzw. sollen in Zukunft eingeführt werden?
Österreich

Imp: Implementiert, ***Pl***: in Planung bzw. in Zukunft vorgesehen, ***NA***: Nicht vorhanden

Organisatorische Maßnahmen	*Imp*	*Pl*	*NA*	*Ges*
Betrieb eines ISMS	33	12	26	71
Betrieb eines IKS inklusive IT Kontrollen	23	14	34	71
Audits/Penetration Tests/Vulnerability Scans	54	2	17	73
Risikomanagement	52	7	13	72
BCM und BIA/ Notfallplanung/-vorsorge	38	16	16	70
Personal Management	43	7	24	74
Awareness Aktivitäten	43	13	19	75
Vulnerability Management	44	9	19	72
Change Management	57	7	11	75
Configuration/ Capacity Management	45	12	17	74
Physische Sicherheit	60	6	8	74
Asset Management	46	9	20	75
Informationsklassifikation und -Verarbeitung	31	19	23	73
Identitäts- und Zugriffsmanagement	52	14	7	73
Vorfallmanagement	35	15	20	70
Patch & Update Management	65	5	3	73
Backup & Wiederherstellung	72	2	1	75
Logging & (Performance) Monitoring	55	10	9	74
Spam & Antivirus	72	1	1	74
Medien-/Datenvernichtung	62	5	7	74
Management der Leistungserbringung/Verträge Externe IT Dienstleister	45	9	18	72
Dokumentation (Systeme, Konfigurationen, org. Prozesse etc.)	61	9	4	74
Sichere Software-/Webapplikationsentwicklung	35	13	24	72
Versicherung gegen Cyber/IT-Angriffe	4	7	60	71
Firmeneigenes CERT	24	9	40	73
Durchführung/Teilnahme an Cyber Übungen	25	8	36	69
Anzahl Beantwortungen				**76**

Legende: Hell-/Dunkelgrau Min/Max der Spalten

Tabelle A.25.: Frage 21, Organisatorische Aufstellung - Österreich

Frage 21: Welche organisatorische Maßnahmen/Prozesse sind im Bereich der Informationssicherheit im Unternehmen umgesetzt bzw. sollen in Zukunft eingeführt werden?
Schweiz

Imp: Implementiert, ***Pl***: in Planung bzw. in Zukunft vorgesehen, ***NA***: Nicht vorhanden

Organisatorische Maßnahmen	*Imp*	*Pl*	*NA*	*Ges*
Betrieb eines ISMS	37	14	12	63
Betrieb eines IKS inklusive IT Kontrollen	42	7	12	61
Audits/Penetration Tests/Vulnerability Scans	45	8	6	59
Risikomanagement	50	5	7	62
BCM und BIA/ Notfallplanung/-vorsorge	43	8	8	59
Personal Management	42	4	12	58
Awareness Aktivitäten	42	7	10	59
Vulnerability Management	37	12	11	60
Change Management	53	3	5	61
Configuration/ Capacity Management	40	7	10	57
Physische Sicherheit	57	1	3	61
Asset Management	43	7	9	59
Informationsklassifikation und -Verarbeitung	39	12	10	61
Identitäts- und Zugriffsmanagement	48	2	10	60
Vorfallmanagement	35	11	13	59
Patch & Update Management	52	5	3	60
Backup & Wiederherstellung	60	1	0	61
Logging & (Performance) Monitoring	43	12	5	60
Spam & Antivirus	59	1	1	61
Medien-/Datenvernichtung	52	3	4	59
Management der Leistungserbringung/Verträge Externe IT Dienstleister	40	9	9	58
Dokumentation (Systeme, Konfigurationen, org. Prozesse etc.)	51	6	4	61
Sichere Software-/Webapplikationsentwicklung	28	9	18	55
Versicherung gegen Cyber/IT-Angriffe	4	7	40	51
Firmeneigenes CERT	15	9	30	54
Durchführung/Teilnahme an Cyber Übungen	12	10	32	54
Anzahl Beantwortungen				**63**

Legende: Hell-/Dunkelgrau Min/Max der Spalten

Tabelle A.26.: Frage 21, Organisatorische Aufstellung - Schweiz

Frage 21: Welche organisatorische Maßnahmen/Prozesse sind im Bereich der Informationssicherheit im Unternehmen umgesetzt bzw. sollen in Zukunft eingeführt werden?

Gesamt

Imp: Implementiert, ***Pl***: in Planung bzw. in Zukunft vorgesehen, ***NA***: Nicht vorhanden

Organisatorische Maßnahmen	***Imp***	***Pl***	***NA***	***Ges***
Betrieb eines ISMS	108	38	47	193
Betrieb eines IKS inklusive IT Kontrollen	85	29	71	185
Audits/Penetration Tests/Vulnerability Scans	142	21	28	191
Risikomanagement	143	24	27	194
BCM und BIA/ Notfallplanung/-vorsorge	116	35	37	188
Personal Management	122	16	50	188
Awareness Aktivitäten	129	29	36	194
Vulnerability Management	115	30	44	189
Change Management	153	18	22	193
Configuration/ Capacity Management	127	24	38	189
Physische Sicherheit	175	8	13	196
Asset Management	132	21	38	191
Informationsklassifikation und -Verarbeitung	108	37	47	192
Identitäts- und Zugriffsmanagement	153	21	20	194
Vorfallmanagement	114	35	39	188
Patch & Update Management	173	11	8	192
Backup & Wiederherstellung	191	4	1	196
Logging & (Performance) Monitoring	144	31	18	193
Spam & Antivirus	193	2	2	197
Medien-/Datenvernichtung	167	11	13	191
Management der Leistungserbringung/Verträge Externe IT Dienstleister	124	28	37	189
Dokumentation (Systeme, Konfigurationen, org. Prozesse etc.)	160	26	9	195
Sichere Software-/Webapplikationsentwicklung	89	40	56	185
Versicherung gegen Cyber/IT-Angriffe	16	18	140	174
Firmeneigenes CERT	60	21	102	183
Durchführung/Teilnahme an Cyber Übungen	55	29	93	177
Anzahl Beantwortungen				**201**

Legende: Hell-/Dunkelgrau Min/Max der Spalten

Tabelle A.27.: Frage 21, Organisatorische Aufstellung - Gesamt

Demografie 1: Wie viele Mitarbeiter beschäftigt Ihr Unternehmen?	D	Ö	Ch	Ges
1-49	21,4%	36,6%	10,8%	21,4%
50-249	17,9%	9,8%	13,8%	12,2%
250-999	21,4%	18,3%	24,6%	18,8%
>1000	39,3%	35,4%	50,8%	39,3%
keine Angabe	0,0%	0,0%	0,0%	8,3%
Anzahl Beantwortungen	***56***	***82***	***65***	***229***
Legende: Hell-/Dunkelgrau auffällige Min/Max der Zeilen, bei Ges Min/Max der Spalte				

Tabelle A.28.: Demografie 1, Unternehmensgröße

Demografie 2: Wo ist der Hauptstandort Ihres Unternehmens?	Ges	Ges
Deutschland	24,5%	56
Österreich	35,8%	82
Schweiz	28,4%	65
keine Angabe	8,3%	19
Anderer bitte nennen	3,1%	7
Anzahl Beantwortungen		***229***
Legende: Hell-/Dunkelgrau auffällige Min/Max der Spalte		

Tabelle A.29.: Demografie 2, Hauptstandort

Demografie 3: In welcher Branche ist Ihr Unternehmen tätig?	D	Ö	Ch	Ges
Land- und Forstwirtschaft, Fischerei	1,9%	0,0%	0,0%	0,5%
Bergbau und Gewinnung von Steinen und Erden	0,0%	0,0%	0,0%	0,0%
Herstellung von Waren	9,6%	3,9%	8,1%	6,6%
Energieversorgung	7,7%	1,3%	1,6%	4,0%
Wasserversorgung, Abwasser und Abfallentsorgung und Beseitigung von Umweltverschmutzungen	1,9%	2,6%	0,0%	1,5%
Bau	0,0%	1,3%	1,6%	1,0%
Handel, Instandhaltung und Reparatur von Kraftfahrzeugen	5,8%	1,3%	1,6%	2,5%
Verkehr und Lagerei	3,8%	1,3%	0,0%	1,5%
Beherbergung und Gastronomie	0,0%	0,0%	0,0%	0,0%
Information und Kommunikation	26,9%	37,7%	17,7%	28,3%
Erbringung von Finanz- und Versicherungsdienstleistungen	7,7%	7,8%	21,0%	13,1%
Grundstücks- und Wohnungswesen	0,0%	1,3%	0,0%	0,5%
Erbringung von freiberuflichen, wissenschaftlichen und technischen Dienstleistungen	0,0%	1,3%	4,8%	2,0%
Erbringung von sonstigen wirtschaftlichen Dienstleistungen	7,7%	6,5%	3,2%	5,6%
Öffentliche Verwaltung, Verteidigung, Sozialversicherung	23,1%	18,2%	25,8%	21,2%
Erziehung und Unterricht	0,0%	1,3%	0,0%	0,5%
Gesundheits- und Sozialwesen	0,0%	3,9%	9,7%	4,5%
Kunst, Unterhaltung und Erholung	0,0%	2,6%	0,0%	1,0%
Erbringung von sonstigen Dienstleistungen	1,9%	7,8%	4,8%	5,1%
Private Haushalte mit Hauspersonal, Herstellung von Waren und Erbringung von Dienstleistungen durch private Haushalte für den Eigenbedarf ohne ausgeprägten Schwerpunkt	0,0%	0,0%	0,0%	0,0%
Exterritoriale Organisationen und Körperschaften	1,9%	0,0%	0,0%	0,5%
Anzahl Beantwortungen	***52***	***77***	***62***	***198***
Legende: Hell-/Dunkelgrau auffällige Min/Max der Zeilen, bei Ges Min/Max der Spalte				

Tabelle A.30.: Demografie 3, Branche

Demografie 4: Welchen Aufgabenbereich erfüllen Sie in Ihrem Unternehmen?	D	Ö	Ch	Ges
Geschäftsführer	13,0%	19,7%	4,6%	12,4%
Aufsichtsrat	0,0%	0,0%	0,0%	0,0%
IT-Leiter/IT-Sicherheitsmanager	25,9%	26,3%	23,1%	25,4%
CISO/Informationssicherheits-Beauftragter	46,3%	15,8%	35,4%	29,9%
Datenschutzbeauftragter	3,7%	0,0%	0,0%	1,0%
Systemadministrator	1,9%	6,6%	10,8%	6,5%
Netzwerkadministrator	5,6%	9,2%	4,6%	6,5%
Risikomanager	0,0%	2,6%	1,5%	2,0%
Sonstiges (bitte angeben)	3,7%	19,7%	20,0%	16,4%
Anzahl Beantwortungen	***54***	***76***	***65***	***201***
Legende: Hell-/Dunkelgrau auffällige Min/Max der Zeilen, bei Ges Min/Max der Spalte				

Tabelle A.31.: Demografie 4, Funktion