USecurD

Auswertung der Online-Studie

Deliverable E 1.3

Projekt	USecureD – Usable Security by Design
Förderinitiative	Einfach intuitiv – Usability für den Mittelstand
Förderkennzeichen	01MU14002
Arbeitspaket	AP 1.3
Fälligkeit	-
Autoren	Hoai Viet Nguyen und Luigi Lo Iacono (Technische Hochschule Köln)
Status	Final
Klassifikation	Öffentlich

HKBS

HK Business Solutions GmbH
Hartmut Schmitt
Mellinweg 20
66280 Sulzbach
schmitt@hk-bs.de

KMU
(Konsortialführer)

Technology
Arts Sciences
TH Köln

Technische Hochschule Köln
Prof. Dr.-Ing. Luigi Lo Iacono
Betzdorfer Straße 2
50679 Köln
luigi.lo_iacono@th-koeln.de

Hochschule
(Konsortialpartner)

Mittelstand-Digital

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Abstract

Im Projekt USecureD werden Musterlösungen und praxistaugliche Werkzeuge entwickelt, die kleine und mittlere Unternehmen (KMU) bei der Entwicklung bzw. bei der Auswahl betrieblicher Anwendungssoftware mit dem Qualitätsmerkmal „Usable Security“ unterstützen. Im Rahmen der methodischen Vorbereitung (Arbeitspaket 1.2: Anforderungen an Usable Security) wurde eine breit angelegte Online-Studie durchgeführt, um das Verständnis von und die Bedürfnisse an Usable Security in Softwareentwickler- und Softwareanwender-Unternehmen sowie KMU und Großunternehmen (GU) zu ermitteln.

In der Studie, die vom 30.10.2015 bis 20.12.2015 durchgeführt wurde, sind 118 vollständig beantwortete Fragebögen erfasst worden. 55% der Rückmeldungen stammen von Teilnehmern, die in einem KMU beschäftigt sind. 45% der Umfrage sind von Personen beantwortet worden, die eine berufliche Tätigkeit in einem Softwareentwickler-KMU ausüben und 17% sind in einem Softwareanwender-KMU angestellt.

Schlagworte

Usable Security, Usability, IT-Sicherheit, Online-Studie, Limesurvey

Executive Summary

Das Projekt USecureD entwickelt und evaluiert methodische Grundlagen, Musterlösungen und Werkzeuge mit dem Ziel, das Qualitätsmerkmal Usable Security stärker in den deutschen IT-Sektor zu verankern. Im Rahmen der methodischen Vorbereitung wurde eine Online-Studie durchgeführt, um das Verständnis, die Anforderungen und die Bedürfnisse an Usable Security zu erheben.

Die Online-Studie startete am 30.10.2015 und endete am 20.12.2015. Die Umfragen der Studie beinhalteten 42 Fragen. Für die Bekanntmachung der Online-Studie wurden die Webseiten von USecureD, Mittelstand-Digital, dem German UPA Arbeitspreis „Usable Security and Privacy“, HK Business Solutions, saar.is und eBusinessLoste-OWL genutzt. Zudem sind Ankündigungen auf der Usable-Security-Gruppe bei Xing, der Facebook- als auch der Google-Plus-Seite des Fraunhofer SIT platziert worden. Des Weiteren wurde versucht potenzielle Teilnehmer über die Mailinglisten der GI Fachgruppe SICHERHEIT und die Vorlesung Daten- und Anwendungssicherheit des Master-Studiengangs Medientechnologie an der TH Köln zu akquirieren.

Insgesamt wurden 118 vollständig beantwortete Umfragen erfasst. 55% der Rückmeldungen stammen von Befragten aus KMU. 45% sind von Teilnehmern beantwortet worden, die eine berufliche Tätigkeit in einem GU ausüben. 71% der Teilnehmer sind in einem Unternehmen angestellt, das Software entwickelt. 29% der Befragten arbeiten in Unternehmen, die Software nur anwenden.

Aus den Ergebnissen der Online-Studie kann entnommen werden, dass über 85% der Befragten in der Lage sind die Qualitätseigenschaften hinter den Begriffen Usability und IT-Sicherheit zu verstehen und zu erläutern. Zudem erachten ebenfalls über 85% der Befragten die Relevanz von Usability und IT-Sicherheit in Software-Produkten als hoch bis sehr hoch. Hieraus lässt sich erschließen, dass Usability und IT-Sicherheit sowohl bei den Befragten aus Softwareanwender- als auch Softwareentwickler-Unternehmen und aus KMU sowie GU bekannte und wichtige Qualitätsmerkmale sind.

Untermauert wird diese Feststellung dadurch, dass über 90% der Befragten aus Softwareentwickler-Unternehmen angeben, dass bei ihrem Unternehmen Usability- und Security-Engineering Bestandteil des Softwareentwicklungsprozesses ist. Als adäquate Methoden und Werkzeuge für Usability- und Security-Engineering nennen die Befragten am häufigsten Vorgehensmodelle, Patterns, Guidelines, Checklisten und Tools. Die Entwicklung und Evaluierung dieser Hilfsmittel entspricht genau den Zielen des Projekts USecureD, das beabsichtigt diese Methoden und Werkzeuge in einer Plattform zu bündeln. Die USecureD-Plattform soll zum einen als Grundlage für Softwareentwickler-KMU dienen, um die Disziplinen Usability-Engineering, User-Experience-Engineering und Security-Engineering zu vereinen. Zum anderen bietet die USecureD-Plattform für Softwareanwender-KMU die Möglichkeit, ihre verwendeten Software-Produkte fundiert nach dem Qualitätsmerkmal Usable Security zu evaluieren.

Die Bereitschaft solche Methoden und Werkzeuge einzusetzen besteht ebenfalls. 76% der Befragten geben an, dass ihr Unternehmen bereit ist spezialisierte Werkzeuge für die

Qualitätsthemen Usability und/oder IT-Sicherheit einzusetzen, 54% sogar für beide Themen. Eine ähnlich hohe Investitionsbereitschaft herrscht auch bei Schulungen. 71% der Teilnehmer geben an, dass ihr Unternehmen bereit ist ihr eigenes Personal in Usability und/oder IT-Sicherheit zu schulen, 45% sogar für beide Themen.

Trotz der hohen Relevanz und Investitionsbereitschaft in Usability und IT-Sicherheit, stehen beide Qualitätsmerkmale bei der Auswahl von Software nicht im Vordergrund. Als erstes Auswahlkriterium für Software geben 74% der Befragten Funktionalität an. Nur jeweils 5% stufen Usability und IT-Sicherheit als erstes Auswahlkriterium ein. Als zweites Kriterium stimmten 26% für Usability und 21% für Sicherheit.

Des Weiteren kann der Online-Studie entnommen werden, dass in vielen Bereichen noch Handlungsbedarf für Usable Security besteht. Hierbei stechen insbesondere die Bereiche E-Mail-Sicherheit und Mobile Security hervor. Für diese Bereiche haben über 70% der Befragten abgestimmt. Der Handlungsbedarf dieser vielen Bereiche geht vermutlich mit der Feststellung einher, dass 65% der Teilnehmer bis 1 Stunde pro Tag, 4% sogar bis 2 Stunden pro Tag für die Verwendung von Sicherheitsmechanismen aufwenden müssen. Bei den Befragten aus Softwareanwender-Unternehmen benötigten sogar 9% bis 2 Stunden pro Tag.

Diese Kosten gilt es im Projekt USecureD zu reduzieren, indem die entwickelten und evaluierten Werkzeuge KMU darin unterstützen, Geschäftsprozesse effizienter und zugleich sicherer zu gestalten.

Als Anforderungen wie gebrauchtstaugliche Sicherheitsmechanismen in den Augen der Teilnehmer gestaltet sein sollen, geben 65% der Befragten Transparenz und 75% Nachvollziehbarkeit an. Die meist gewählte Anforderung für die Gestaltung gebrauchstauglicher Sicherheitsmechanismen ist mit 83% die einfache Anwendbarkeit.

Inhaltsverzeichnis

1 Einleitung

Ein Hauptziel des Arbeitspakets 1.2 ist die Analyse der Anforderungen und Bedürfnisse an Usable Security. Um die Anforderungen und Bedürfnisse von Stakeholdern und Endanwendern in Softwareanwender- sowie Softentwickler-Unternehmen und KMU[1] sowie GU zu erheben, wurde eine breit angelegte Online-Studie durchgeführt.

1.1 Aufbau und Durchführung der Online-Studie

Die Online-Studie startete am 30.10.2015 und endete am 20.12.2015. Erstellt wurde sie mit der Software Limesurvey, einer frei verfügbaren und quelloffenen Webanwendung für Online-Umfragen. Für den Betrieb der Online-Studie wurde ein Server von HK Business Solutions bereitgestellt. Die Installation und Konfiguration übernahm ebenfalls HK Business Solutions. Die Implementierung, Durchführung und Auswertung der Online-Umfrage wurde von der TH Köln durchgeführt.

Die Umfragen wurden als strukturiertes Interview ausgelegt und bestanden aus insgesamt 42 Fragen. In Abhängigkeit der gegebenen Antworten mussten die Teilnehmer eine unterschiedliche Anzahl und ggf. auch unterschiedliche Fragen beantworten.

Der Umfragekatalog der Online-Studie bestand aus 6 Fragegruppen. In der ersten Fragegruppe wurden demographische Fragen gestellt. Die zweite Fragegruppe bestand aus allgemeinen Fragen zum Thema Usability. In der dritten Fragegruppen mussten die Teilnehmer allgemeine Fragen zum Thema IT-Sicherheit beantworten. Die vierte Fragegruppe beinhaltete allgemeine Fragen über die Einordnung und Relevanz von Usable Security. Die letzten beiden Fragengruppen enthalten jeweils Fragen über den aktuellen Umsetzungsgrad und die Investitionsbereitschaft für Usability und IT-Sicherheit in Softwareentwickler- bzw. Softwareanwenderunternehmen.

Als Distributionskanäle für die Bekanntmachung der Online-Studie wurden verschiedene Plattformen gewählt. Ankündigungen wurden auf den Webseiten von USecureD, Mittelstand-Digital, dem German UPA Arbeitskreis „Usable Security und Privacy“, HK Business Solutions, saar.is und eBusinessLoste-OWL platziert. Im Bereich der sozialen Medien wurde die Usable-Security-Gruppe bei Xing und sowohl die Facebook- als auch die Google-Plus-Seite des Fraunhofer SIT genutzt. Zudem wurde versucht potenzielle Teilnehmer über die Mailinglisten der GI Fachgruppe SICHERHEIT und die Vorlesung Daten- und Anwendungssicherheit des Master-Studiengangs Medientechnologie an der TH Köln zu akquirieren.

1.2 Studienteilnehmer

Insgesamt wurden 154 Fragebögen erfasst, von denen 118 vollständig und 36 unvollständig beantwortet wurden. Berücksichtigung in der Auswertung fanden ausschließlich vollständig

[1] In diesem Deliverable werden alle Unternehmen, die weniger als 250 Personen beschäftigen, als KMU definiert. Nach der Empfehlung der Europäischen Kommission beinhaltet die Definition eines KMU nicht nur die Anzahl der Beschäftigten, sondern auch den Jahresumsatz bzw. die Jahresbilanzsumme [EU-Kommission 2003]. Die Angabe dieser beiden Zahlen wurde in der Online-Studie allerdings nicht berücksichtigt.

beantwortete Fragebögen, auf die sich folglich die prozentualen Angaben im weiteren Verlauf dieses Deliverables beziehen.

85% der Teilnehmer sind Männer und 15% der Umfrage wurden von Frauen beantwortet (siehe Abbildung 1).

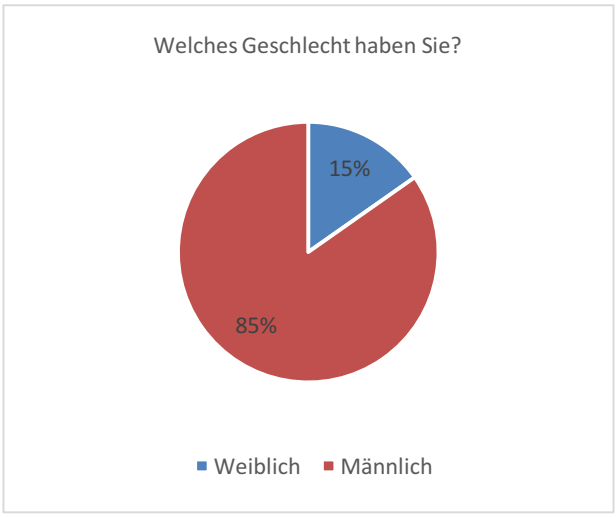

Abbildung 1: Geschlecht der Befragten

4% der teilnehmenden Personen sind unter 26 Jahren oder über 55 Jahre alt. Zwischen 26 und 35 Jahre alt sind 41% der Teilnehmer. 27 % aller Teilnehmer sind zwischen 36 und 45. Teilnehmer in der Altersgruppe von 46 bis 55 Jahre haben 24% der Umfragen beantwortet (siehe Abbildung 2).

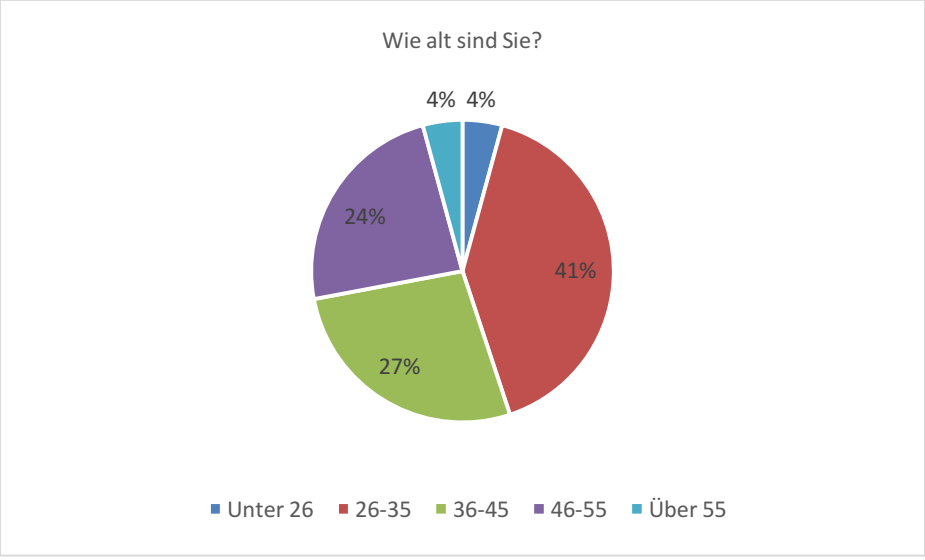

Abbildung 2: Altersgruppen der Befragten

74% der Befragten haben einen fachlichen Hintergrund im Bereich Informatik oder Ingenieurwissenschaften. Bei 7% liegt der fachliche Hintergrund im Bereich

Betriebswirtschaft und bei 6% im Bereich Design. 13% geben Sonstiges an (siehe Abbildung 3). Hierunter fielen u. a. die Antworten Soziologie, Architektur, Volkswirtschaft, Datenschutz/Informationssicherheit, PR/Kommunikation, User Experience, Geisteswissenschaften, Sozialwissenschaften, Psychologie, Kommunikationswissenschaften, Physik und Usability.

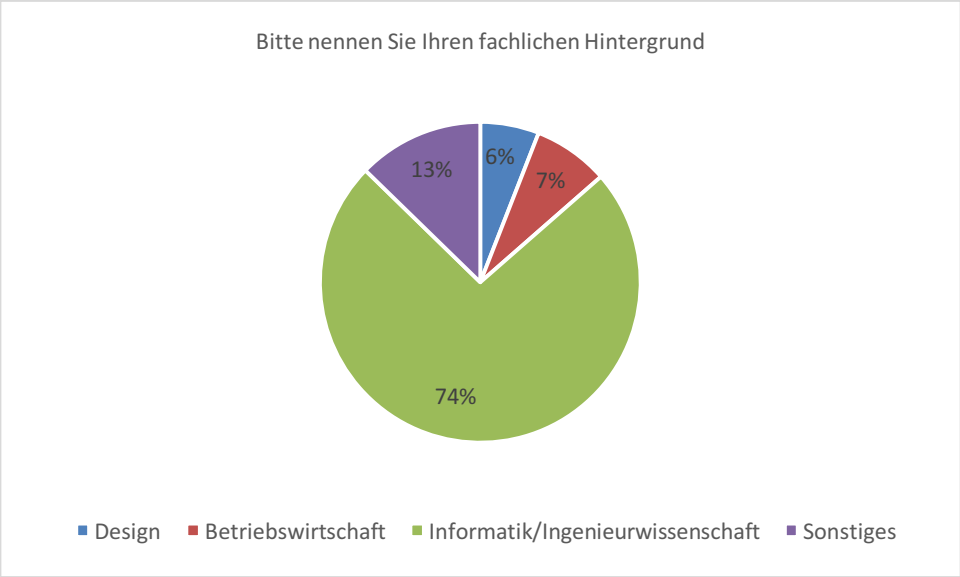

Abbildung 3: Fachlicher Hintergrund der Befragten

53% der Befragten besitzen über 10 Jahre Berufserfahrung. 20% haben eine Berufserfahrung von 6-10 Jahren, 13% von 4-5 Jahren, 11% von unter 2 Jahren und 3% von 2-3 Jahren (siehe Abbildung 4).

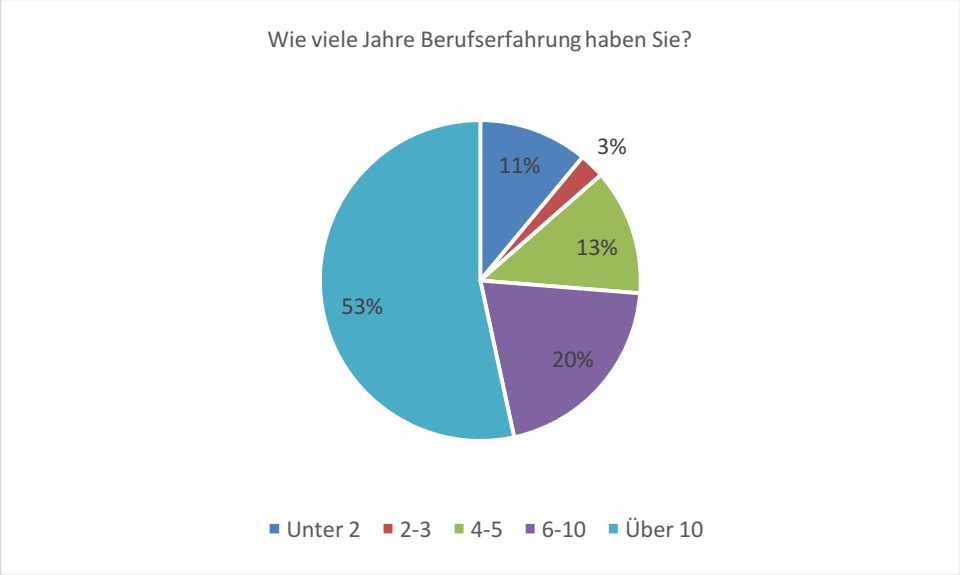

Abbildung 4: Berufserfahrung der Befragten

53% der Befragten geben an, dass das Unternehmen, in dem sie arbeiten, im IT-Sektor tätig ist. Bei 24% sind die Unternehmen im Bereich Wissenschaft und Bildung tätig. 11% geben an, dass ihr Unternehmen im Bereich Medien tätig ist. Alle anderen Bereiche blieben bei dieser Frage unter 10%. Keiner der Befragten gab an, dass sein Unternehmen im Bereich Verteidigung oder Luft- und Raumfahrt tätig ist (siehe Abbildung 5). Unter Sonstiges geben 11% der Befragten u. a. Wirtschaftsförderung, Heizung und Klima, Beratung, Unterhaltung, Dienstleistung, Lehre, Forschung und Entwicklung, erneuerbare Energien, Sozialwesen, E-Commerce und Soziallotterie an.

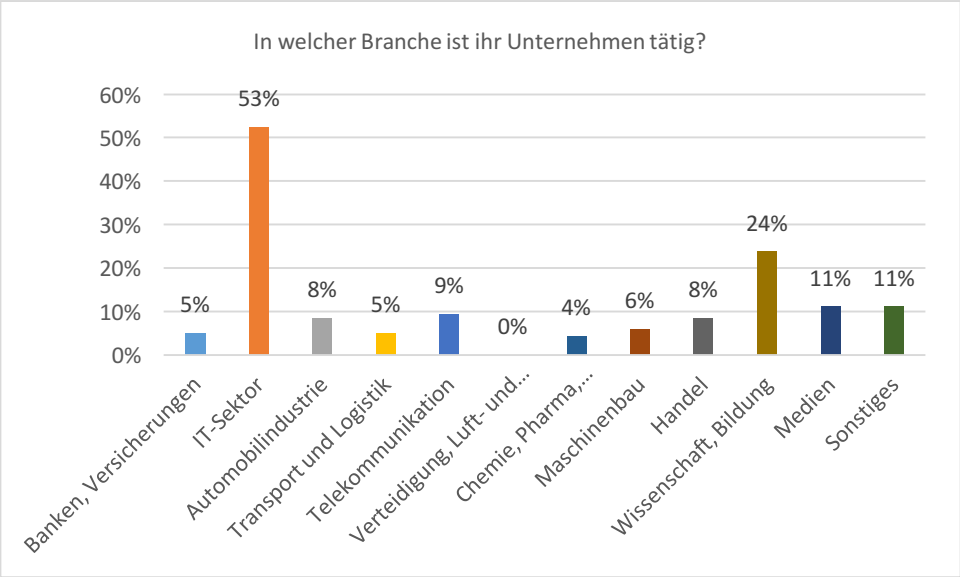

Abbildung 5: Unternehmensbranche der Befragten

45% der Teilnehmer sind in einem GU mit über 250 Mitarbeitern beschäftigt. Jeweils 21% arbeiten in einem Unternehmen mit unter 10 oder zwischen 10 und 25 Mitarbeitern. 13% aller Teilnehmer sind in Unternehmen eingestellt, in denen 50 bis 249 Mitarbeiter angestellt sind (siehe Abbildung 6). Folglich gehen 55% der Teilnehmer ihrer Beschäftigung in einem KMU nach.

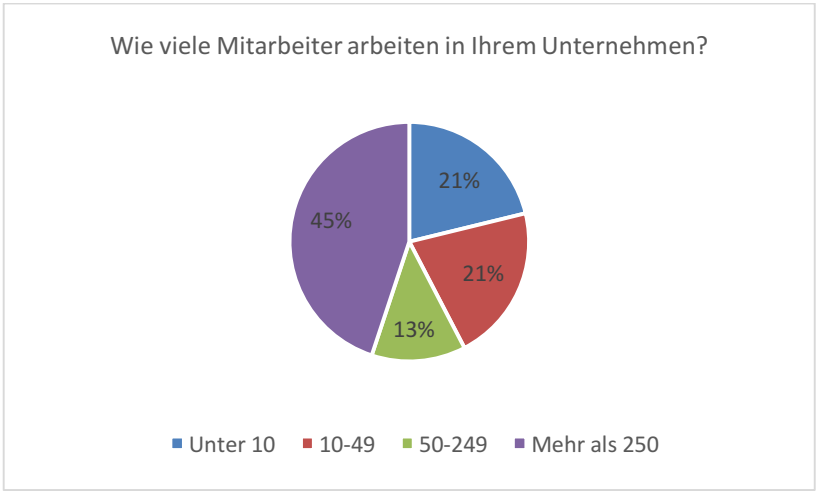

Abbildung 6: Unternehmensgrößen der Befragten

26% der Befragten arbeiten in ihrem Unternehmen in der Abteilung Forschung/Entwicklung. 23% sind in der IT-Abteilung tätig. Jeweils 15% arbeiten in der Geschäftsführung oder Projektleitung. 9% leiten eine Abteilung. 4% arbeiten im Marketing/Vertrieb. Keiner der Befragten ist im Einkauf, in der Logistik, im Personalwesen, im Finanzwesen oder in der Verwaltung tätig (siehe Abbildung 7). 8% der Befragten geben unter Sonstiges u. a. Student, UX Research, PR, Compliance, Selbständig/IT-Freelancer, Pre-Sales, Systemarchitekt und Business Development an.

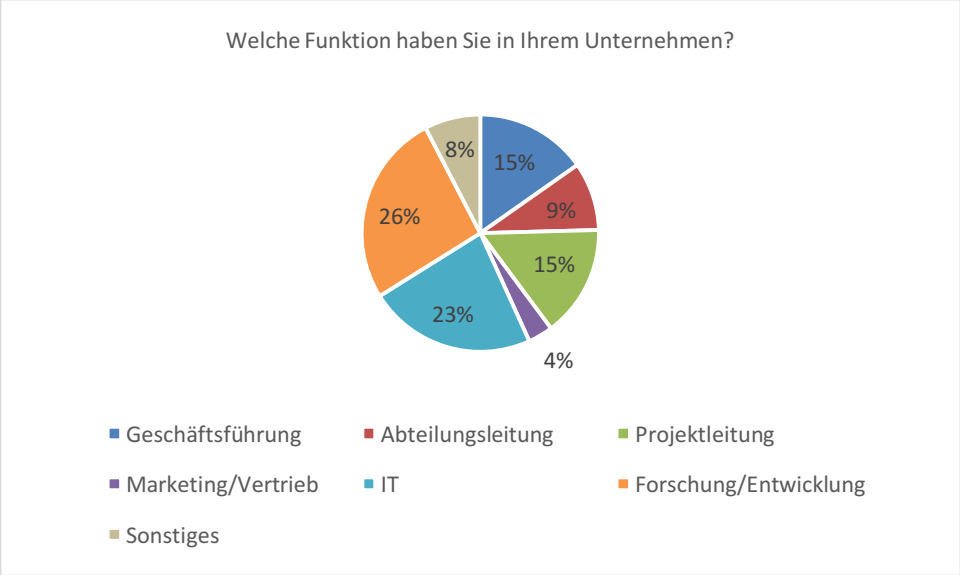

Abbildung 7: Unternehmensfunktion der Befragten

71% aller Teilnehmer sind in einem Unternehmen angestellt, das Software entwickelt. 29% der Teilnehmer sind dagegen in einem Unternehmen beschäftigt sind, welches Software nur anwendet (siehe Abbildung 8).

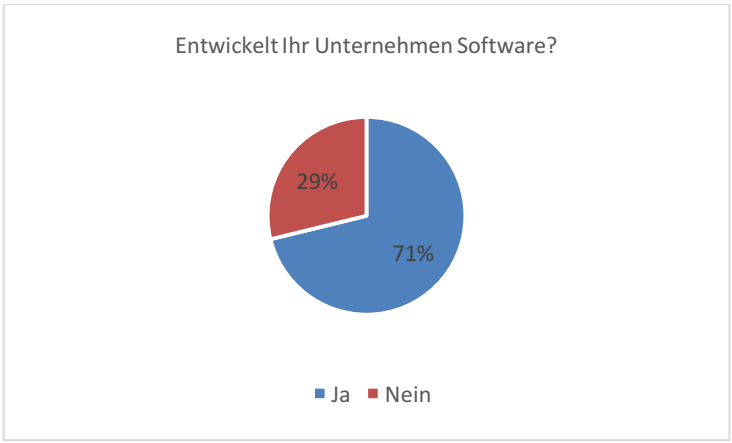

Abbildung 8: Befragte aus Softwareentwicklungs- und Softwareanwenderunternehmen

Aus dieser Frage und der Frage nach der Unternehmensgröße kann abgeleitet werden, dass 45% der Befragten in einem Softwareentwickler-KMU angestellt sind. 17% gehen einer

beruflichen Tätigkeit in einem Softwareanwender-KMU nach. 33% sind in einem Softwareentwickler-GU beschäftigt. 12% üben eine berufliche Tätigkeit in einem Softwareanwender-GU aus.

85% der Befragten, die in einem Softwareentwickler-Unternehmen tätig sind, geben an, dass ihr Unternehmen Individualsoftware entwickelt. 43% entwickeln Apps und 23% Standardsoftware. 10% geben Sonstiges an (siehe Abbildung 9). Hierunter fielen u. a. die Antworten Games, ECM, SaaS, Prototypen, Webangebote, Websites und Webanwendungen.

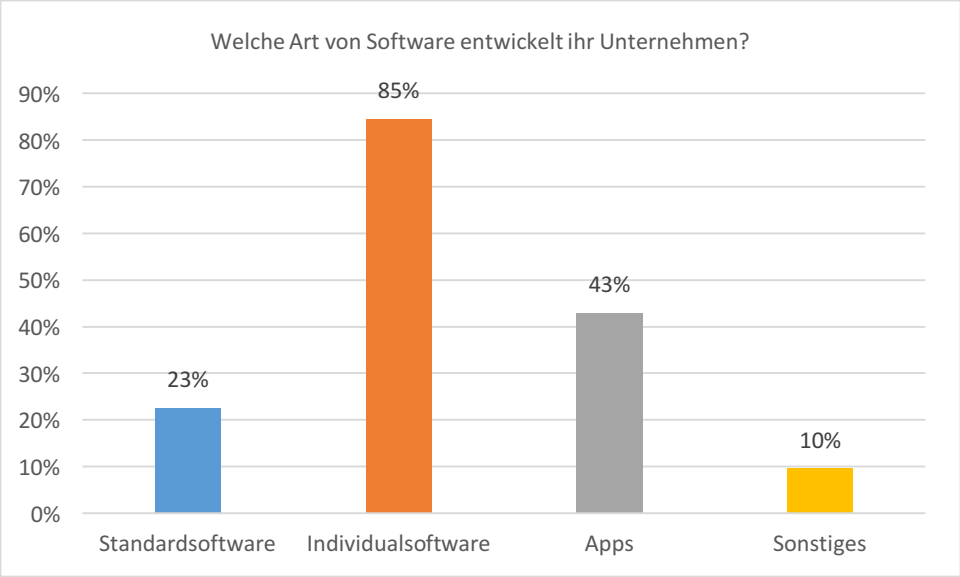

Abbildung 9: Art der Software, die in den Unternehmen der Befragten entwickelt wird

2 Auswertung

In diesem Kapitel werden die Ergebnisse der Online-Studie dargelegt. Die Auswertung der Fragen ist in fünf Unterkapitel aufgeteilt, deren Gliederung sich wie folgt nach den Themengebieten der Fragegruppen richtet.

Im ersten Unterkapitel (Kapitel 2.1) werden die Ergebnisse der Fragen über das Verständnis und die Einschätzung zum Thema Usability erörtert. Das nächste Unterkapitel (Kapitel 2.2) legt die Resultate der Fragen über das Verständnis und die Einschätzung zum Thema IT-Sicherheit dar. Das Kapitel 2.3 beschäftigt sich mit der Auswertung der Fragen über die Einordnung und Relevanz von Usable Security. Im Kapitel 2.4 werden die Fragen und Antworten zu dem aktuellen Umsetzungsgrad von Usability und IT-Sicherheit dargelegt. Das letzte Unterkapitel (Kapitel 2.5) stellt die Auswertung der Antworten über die Investitionsbereitschaft in Usability und IT-Sicherheit vor. Alle Unterkapitel außer dem Kapitel 2.4 beginnen mit einer allgemeinen Auswertung der jeweiligen Fragegruppe. Anschließend folgt eine Auswertung der Antworten mit dem Fokus auf Softwareanwender-Unternehmen und Softwareentwickler-Unternehmen. Da USecureD das primäre Ziel hat, das Qualitätsmerkmal Usable Security stärker in den IKT-Sektor von KMU zu verankern, erfolgt eine weitere Differenzierung der Auswertung in KMU und GU. Dadurch können das Verständnis, die Anforderungen und die Bedürfnisse an Usability, IT-Sicherheit und Usable Security von KMU und GU direkt miteinander verglichen werden. Für Kapitel 2.4 eignet sich keine allgemeine Auswertung, da sich die Fragen für Softwareanwender- und Softwareentwickler-Unternehmen in dieser Gruppe komplett unterscheiden.

2.1 Verständnis und Einschätzung zum Thema Usability

86% aller Teilnehmer kennen den Begriff Usability und können eine Definition angeben. 13% haben den Begriff schon einmal gehört, kennen den Begriff aber nicht wirklich. 1% kennen den Begriff Usability nicht (siehe Abbildung 10).

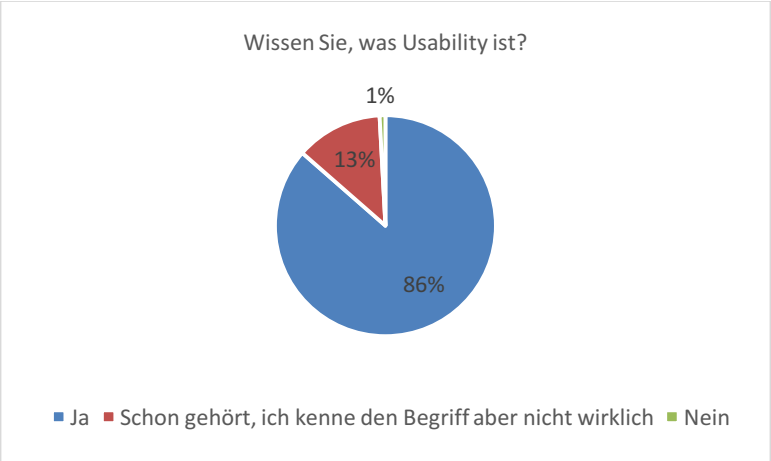

Abbildung 10: Verständnis des Begriffs Usability der Befragten

Von den angegebenen Definitionen sind 23% sinngemäß nach der ISO 9241-11[2] [DIN EN ISO 9241-11:1999-01] beschrieben oder enthalten jeweils Verweise auf die ISO 9241 wie z. B.:

- „Grad an Effektivität, Effizienz und Zufriedenheit, die eine Software (ein Produkt) beim Benutzer hervorruft“
- „Ausmaß in dem ein Nutzer ein Produkt im bestimmten Kontext nutzen kann und damit Ziele effizient, effektiv und zufriedenstellend erreicht.“
- „Gebrauchstauglichkeit von Software, die sich aus Effektivität, Effizienz und Nutzerzufriedenheit in bestimmten Anwendungskontexten ergibt.“
- „Gebrauchtauglichkeit nach 9241-110“
- „Gebrauchstauglichkeit nach DIN EN ISO“

45% der Definition enthalten Aussagen, die ansatzweise der ISO 9241-11 entsprechen, wie z. B.:

- „Nach meinem Verständnis: Ein System/eine Anwendung/ein Produktmerkmal ist umso benutzbarer, je weniger Aufwand (geistig, physisch, zeitlich) in dessen nutzenbringende Verwendung (d.h. auch in Integration in die eigenen Arbeitsprozesse) gesteckt werden muss. Ganz konkret: wenig Installationsaufwand, kurze/sparsame Dialogführung, aufgabenorientierte Features, visuell ergonomische und verständliche Benutzeroberfläche, leichte Einbindung in gängige Infrastruktur, uvm.“

[2] Die Definition von Usability laut der ISO 9241-11 lautet: „Ausmaß, in dem ein System, ein Produkt oder eine Dienstleistung durch bestimmte Benutzer in einem bestimmten Nutzungskontext genutzt werden kann, um festgelegte Ziele effektiv, effizient und zufriedenstellend zu erreichen“.

- „Ich verstehe unter dem Begriff die Nutzungsmöglichkeit der Software im Hinblick auf Ergonomie, Bedienungsfreundlichkeit, Performance, Funktionalität und weitere "gern gesehene" Eigenschaften“
- „Die Nutzerfahrung so angenehm wie möglich zu gestalten. Das bedingt neben dem einfachen und logisch nachvollziehbarem Bedienkonzept auch vernünftige Farb- und Schriftauswahl. Hinzu kommt die Rücksichtnahme auf Nutzer mit Einschränkungen im audiovisuellen oder motorischen Bereich.“

32% der Definition sind einfache Übersetzungen des Begriff Usability auf Deutsch wie z. B.:

- „Nutzerfreundlichkeit“
- „Gebrauchstauglichkeit“
- „Gebrauchstauglichkeit von Software“

40% aller befragten Teilnehmer schätzen die Relevanz von Usability in Software-Produkten als hoch ein, 52% sogar als sehr hoch. 7% bewerten die Relevanz von Usability als durchschnittlich und 1% als niedrig. Keiner der Befragten erachtet die Relevanz von Usability als sehr niedrig (siehe Abbildung 11). Folglich sehen 92% der Befragten Usability als wesentliches Qualitätsmerkmal in Software-Produkten an.

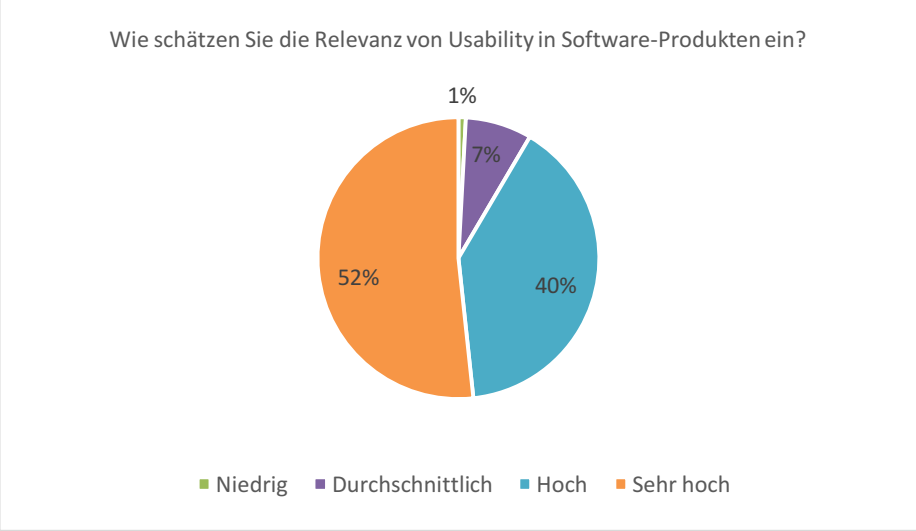

Abbildung 11: Relevanz von Usability in Software-Produkten aus Sicht der Befragten

2.1.1 Softwareanwender-Unternehmen

Alle Teilnehmer, welche in einem Softwareanwender-Unternehmen beschäftigt sind, haben den Begriff Usability schon einmal gehört. 94% kennen den Begriff und können eine Definition angeben. 6% haben den Begriff schon gehört, kennen aber den Begriff nicht wirklich. Keiner der Befragten aus Softwareanwender-Unternehmen gab „Nein“ als Antwort an (siehe Abbildung 12).

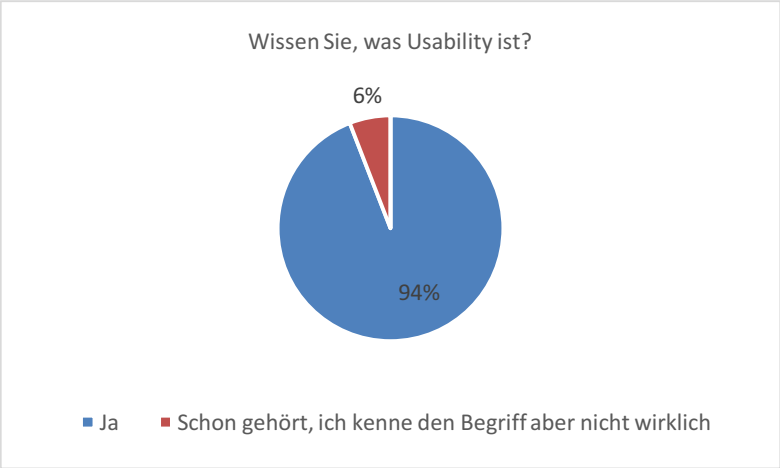

Abbildung 12: Verständnis des Begriffs Usability der Befragten aus Softwareanwender-Unternehmen

22% der abgegebenen Definition geben eine sinngemäße Beschreibung für Usability nach der ISO 9241-11 [DIN EN ISO 9241-11:1999-01] wieder oder verwiesen auf die ISO 9241-11. 34% der Aussagen sind eine Übersetzung des Begriffs Usability auf Deutsch. Bei 44% ist die Definition in Ansätzen gemäß der Beschreibung nach ISO 9241-11.

53% aller Teilnehmer, die in einem Softwareanwender-Unternehmen beschäftigt sind, schätzen die Relevanz von Usability in Software-Produkten als hoch ein, 41% schätzen Usability sogar als sehr hoch ein. 6% erachten die Relevanz von Usability als durchschnittlich. Keiner schätzt die Relevanz als niedrig oder sehr niedrig ein (siehe Abbildung 13). Somit erachten 94% der Teilnehmer aus Softwareanwender-Unternehmen Usability als wesentliches Qualitätsmerkmal in Software-Produkten.

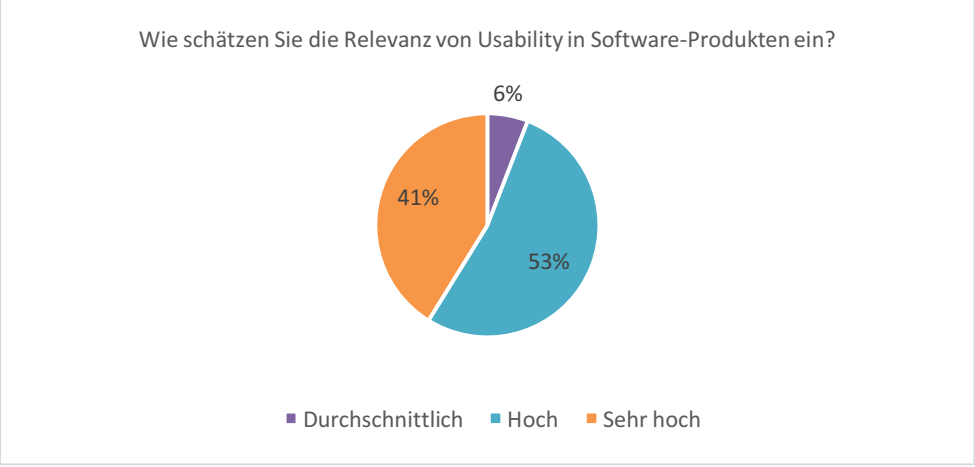

Abbildung 13: Relevanz von Usability in Software-Produkten aus Sicht der Softwareanwender-Unternehmen

2.1.2 Softwareentwickler-Unternehmen

83% der Befragten, die in einem Softwareentwickler-Unternehmen angestellt sind, kennen den Begriff Usability und können auch eine Definition dafür angeben. 16% haben den Begriff

Usability schon gehört, kennen den Begriff aber nicht wirklich. 1% kennen den Begriff nicht (siehe Abbildung 14).

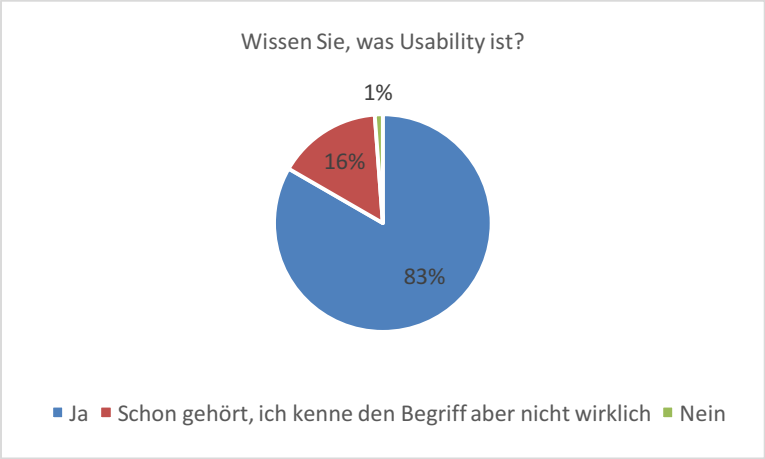

Abbildung 14: Verständnis des Begriffs Usability der Befragten aus Softwareentwickler-Unternehmen

Auch bei den Teilnehmern aus Softwareentwickler-Unternehmen, die eine Erläuterung des Begriffs Usability nennen, sind 23% in der Lage eine sinngemäße Definition nach der ISO 9241-11 [DIN EN ISO 9241-11:1999-01] anzugeben. 31% geben eine Übersetzung auf Deutsch an. 47% sind in der Lage eine Definition zu nennen, die ansatzweise die Darlegung der ISO 9241-11 wiedergibt.

35% der Befragten, in deren Unternehmen Software entwickelt wird, stufen Usability in Software-Produkten als hoch ein. Bei 56% ist die Relevanz von Usability sogar sehr hoch. 8% erachten die Relevanz von Usability als durchschnittlich und 1% als niedrig. Keiner schätzt Usability als sehr niedrig ein (siehe Abbildung 15). Demnach betrachten 91% der Befragten, die in einem Softwareentwickler-Unternehmen beschäftigt sind, Usability als wichtiges Qualitätsmerkmal von Software-Produkten.

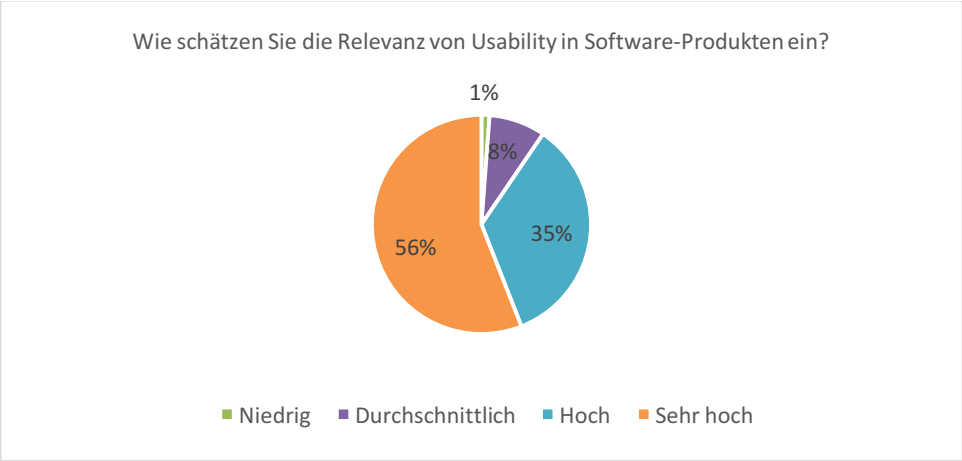

Abbildung 15: Relevanz von Usability in Software-Produkten aus Sicht der Befragten aus Softwareentwickler-Unternehmen

2.1.3 Kleine und mittlere Unternehmen

85% der Befragten aus KMU kennen den Begriff Usability und können auch eine Definition dafür angeben. 15% haben den Begriff Usability schon gehört, kennen den Begriff aber nicht wirklich. Jeder hat den Begriff Usability vorher schon gehört (siehe Abbildung 16).

Abbildung 16: Verständnis des Begriffs Usability der Befragten aus KMU

18% der Definitionen sind sinngemäße Erläuterungen nach der ISO 9241-11 [DIN EN ISO 9241-11:1999-01]. 35% nennen eine einfache Übersetzung auf Deutsch als Definition. 47% geben eine Erläuterung an, die ansatzweise sich nach der ISO 9241-11 richtet.

37% der Befragten, die in einem KMU angestellt sind, schätzen die Relevanz von Usability als hoch ein, 57% sogar als sehr hoch. 5% erachten die Relevanz von Usability als durchschnittlich und 1% als niedrig. Keiner der Befragten schätzt die Relevanz von Usability als sehr niedrig ein (siehe Abbildung 17). Somit empfinden 94% der Befragten aus KMU Usability als wesentliches Qualitätsmerkmal in Software-Produkten.

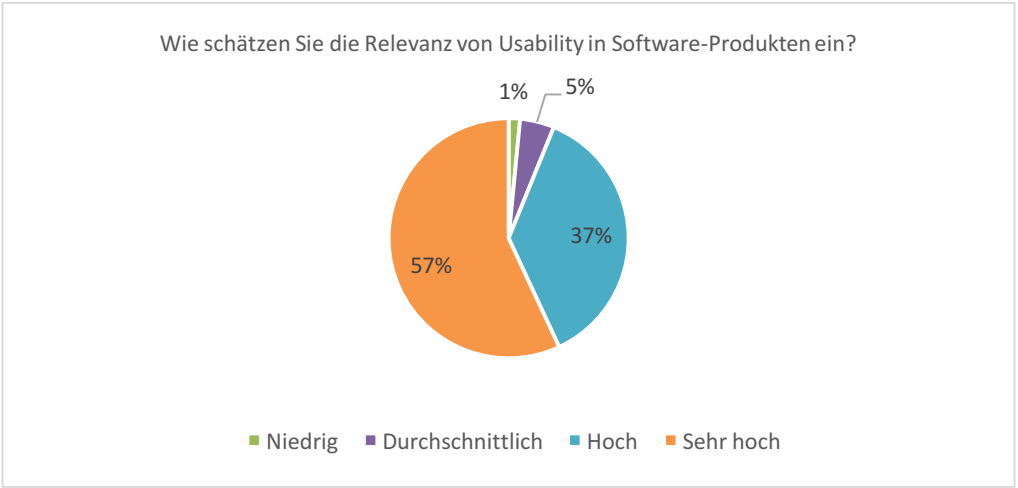

Abbildung 17: Relevanz von Usability aus Sicht der Befragten aus KMU

2.1.4 Großunternehmen

89% der Befragten, die eine berufliche Tätigkeit in einem GU ausüben, kennen den Begriff Usability und können auch eine Definition dafür angeben. 9% haben den Begriff schon

einmal gehört, kennen den Begriff aber nicht wirklich. 2% kennen den Begriff Usability nicht (siehe Abbildung 18).

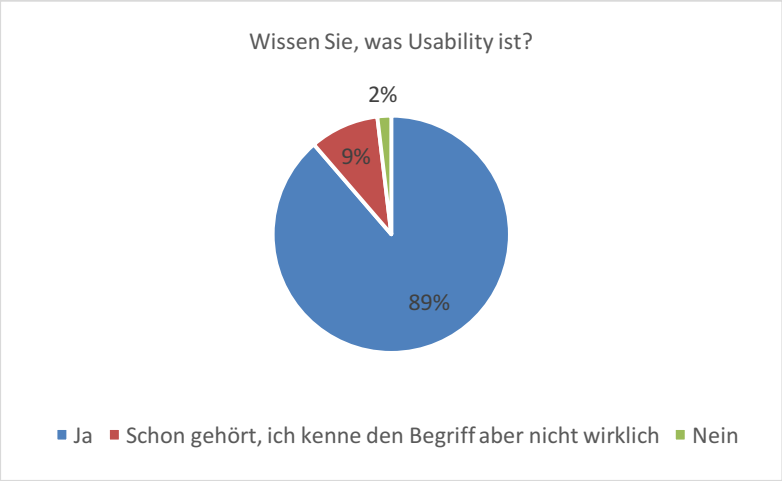

Abbildung 18: Verständnis des Begriffs Usability der Befragten aus GU

28% der Befragten aus GU, die eine Definition für den Begriff Usability angeben können, nennen eine sinngemäße Erläuterung nach der ISO 9241-11 [DIN EN ISO 9241-11:1999-01]. Ebenfalls 28% übersetzen den Begriff Usability auf Deutsch. 44% der Definitionen sind ansatzweise gemäß der Erläuterung nach der ISO 9241-11.

44% der Befragten, die in einem GU beschäftigt sind, schätzen die Relevanz von Usability in Software-Produkten als hoch ein, 45% sogar als sehr hoch. 11% erachten die Relevanz von Usability als durchschnittlich. Keiner schätzt die Relevanz von Usability als niedrig oder sehr niedrig ein (siehe Abbildung 19). Folglich erachten 89% der Befragten, die einer beruflichen Tätigkeit in einem GU nachgehen, Usability als wesentliches Qualitätsmerkmal in Software-Produkten.

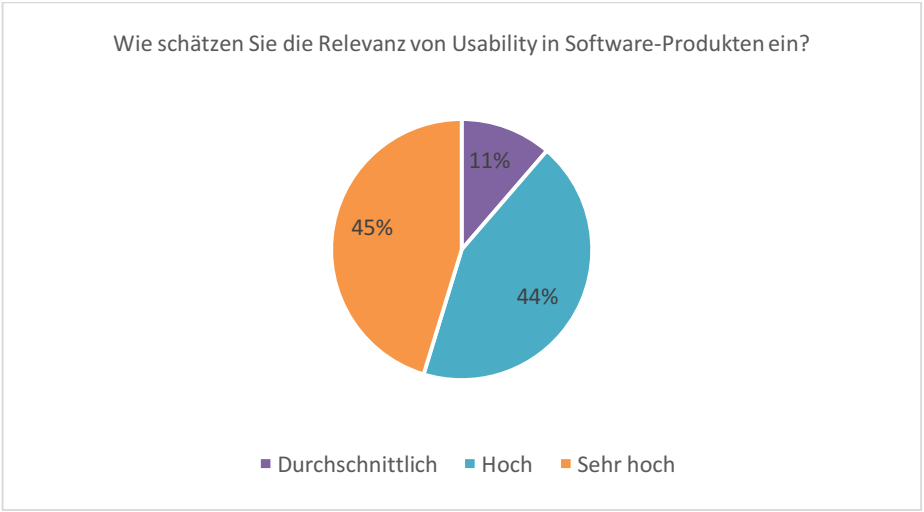

Abbildung 19: Relevanz von Usability aus Sicht der Befragten aus GU

2.2 Verständnis und Einschätzung zum Thema IT-Sicherheit

90% aller befragten Teilnehmer kennen den Begriff IT-Sicherheit und 87% können eine Definition angeben. 9% haben den Begriff Usability schon einmal gehört, kennen den Begriff aber nicht wirklich. 1% kennt den Begriff nicht (siehe Abbildung 20).

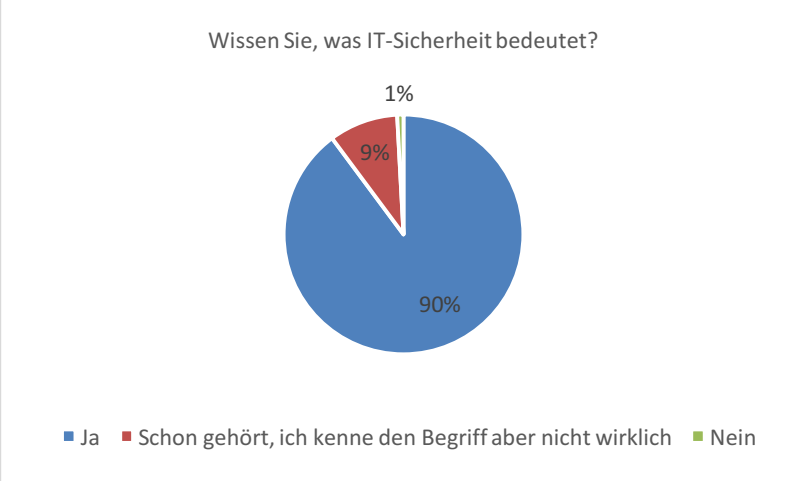

Abbildung 20: Verständnis des Begriffs IT-Sicherheit der Befragten

94% der Definitionen richten sich ansatzweise nach der Begriffserklärung von Sorge et al.[3] [Sorge et al. 2013], wie z.B.:

- „IT-Sicherheit ist die Absicherung von informationstechnischen Systemen gegen Bedrohungen jedweder Art. Entgegen häufig getätigter Aussagen umfasst die IT-Security nicht nur die Abwehr vor IT-bezogenen Angriffen (z.B. Hacker und DOS) und IT-bezogenen Bedrohungen (z.B. Fault-Tolerance und Backups), sondern auch nicht-IT-bezogene Bedrohungen gegenüber IT-Systemen (z.B. Stromausfall, physikalischer Zugang zum Serverraum).“
- „Unter IT-Sicherheit verstehe ich die Sicherheit von Rechner- und Telekommunikationsnetzen. Der Begriff Sicherheit fasst hier u.a. die Verhinderung von unbefugten Zugriffen auf geschlossene Systeme und natürlich der Schutz persönlicher Daten bzw. Daten von Nutzern zusammen.“
- „IT-Sicherheit dient dem Schutz vor Gefahren und Bedrohungen, der Vermeidung von (wirtschaftlichen) Schäden und der Minimierung von Risiken. Primäre Schutzziele sind hierbei die Vertraulichkeit, Verfügbarkeit und Integrität der von einem IT-System verarbeiteten Daten.“
- „Die IT-Sicherheit umfasst die Eigenschaften eines Informationssystems, wie Daten in Hinsicht auf die Vertraulichkeit, Verfügbarkeit und Integrität behandelt werden. Es werden also Maßnahmen gebildet, um wirtschaftliche Schäden durch z.B. Datenmissbrauch zu verhindern.“

[3] Die Definition von IT-Sicherheit nach Sorge et al. lautet: „Unter IT-Sicherheit versteht man Maßnahmen, die beabsichtigte Angriffe auf IT-Systeme, gespeicherte und übertragene Daten sowie Kommunikationsbeziehungen vereiteln.“

3% nennen trotz der Angabe, dass sie wissen, was IT-Sicherheit bedeutet, keine Definition. Die anderen 3% der Definitionen sind falsch oder können nicht gewertet werden.

40% aller Teilnehmer schätzen die Relevanz von Sicherheitsmechanismen in Software-Produkten als hoch ein, 50% sogar als sehr hoch. 9% empfinden die Relevanz von Sicherheitsmechanismen als durchschnittlich. Jeweils 1% schätzen die Relevanz von Sicherheitsmechanismen als niedrig oder sehr niedrig ein (siehe Abbildung 21). Folglich erachten 90% der Befragten Sicherheitsmechanismen als wesentlichen Bestandteil von Software-Produkten.

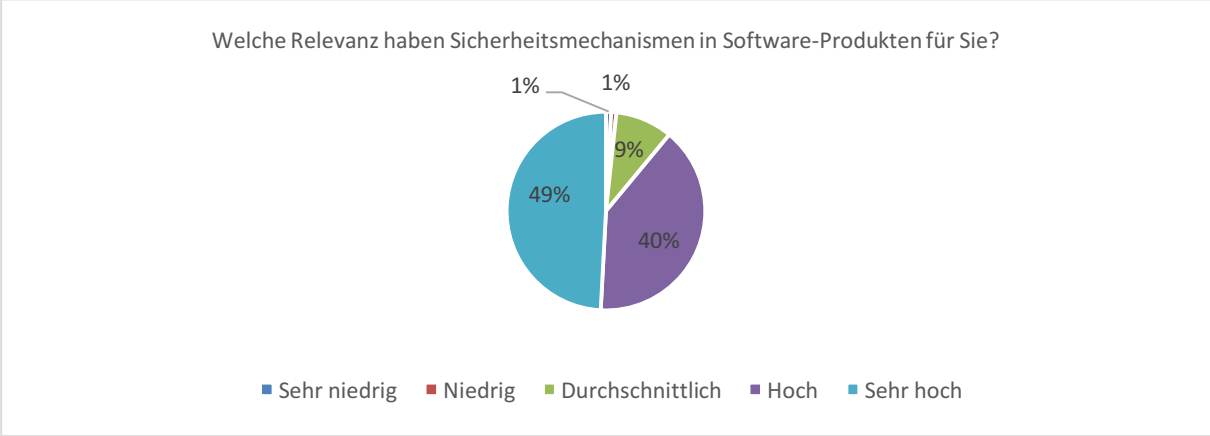

Abbildung 21: Relevanz von Sicherheitsmechanismen in Software-Produkten aus Sicht der Befragten

Als die am häufigsten verwendeten Sicherheitskomponenten (Nennungen ab 35%) wurden Firewall, Virenschutz, Passwortmanager, Kommunikations- und Datenverschlüsselung, Digitale Signatur, Malwareschutz, Security-Token und Spamfilter genannt (siehe Abbildung 22). Des Weiteren haben Teilnehmer unter Sonstiges Incident Response Tools, Patchmanagement, DDos-Schutz, Tor, Keyfiles, Anomalie-Erkennung, Zugriffschutzmaßnahmen (Bildschirmsperren), IFC und Static-Code-Analyse angegeben.

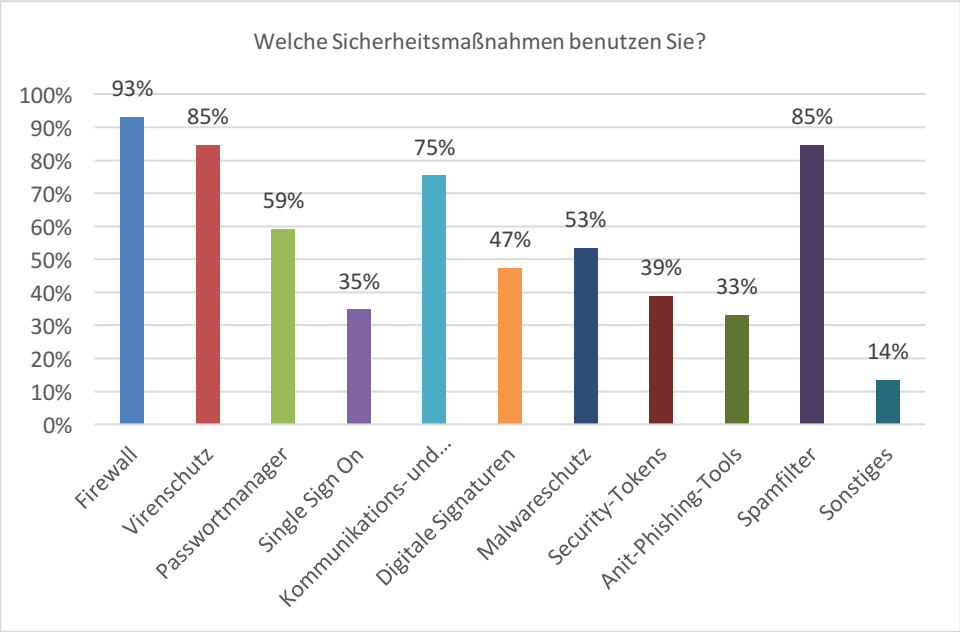

Abbildung 22: Verwendung von Sicherheitsmaßnahmen laut den Befragten

64% aller befragten Teilnehmer empfinden die verwendeten Sicherheitskomponenten als nicht belastend während ihrer täglichen Arbeit. 34% empfinden diese als belastend, 2% sogar als sehr belastend[4] (siehe Abbildung 23).

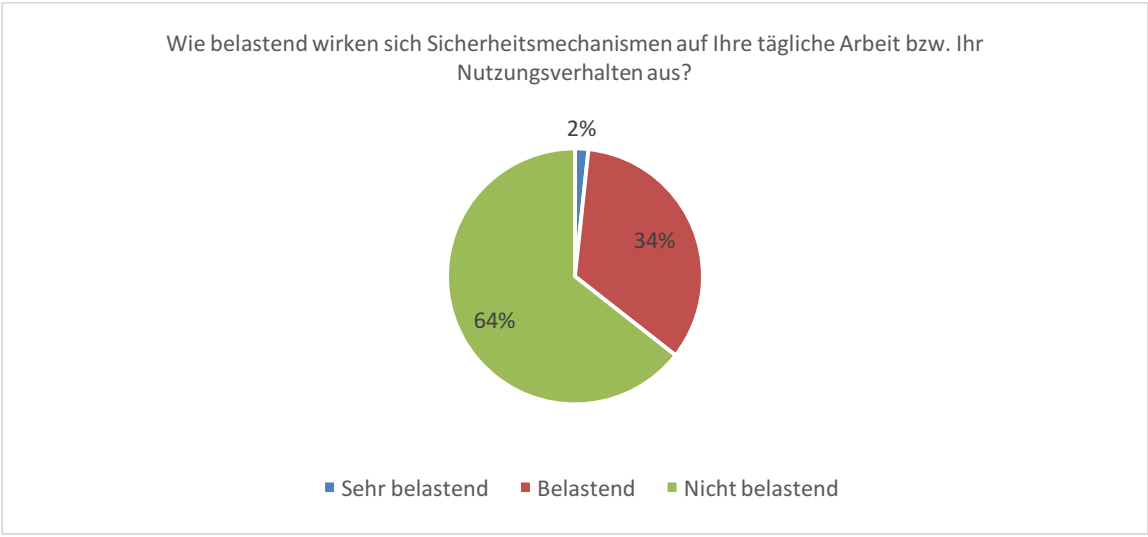

Abbildung 23: Belastungsgrad bei der Verwendung von Sicherheitsmechanismen

65% der Befragten geben an, bis zu 1 Stunde für die Verwendung von Sicherheitsmechanismen am Tag aufzuwenden, 4% sogar zwischen 1 und 2 Stunden. 31%

[4] Da es sich hierbei um eine allgemeine Frage handelt, sind keine Rückschlüsse auf einzelne Sicherheitskomponenten möglich.

wenden keine Zeit dafür auf. Keiner der Befragten benötigt mehr als 2 Stunden (siehe Abbildung 24).

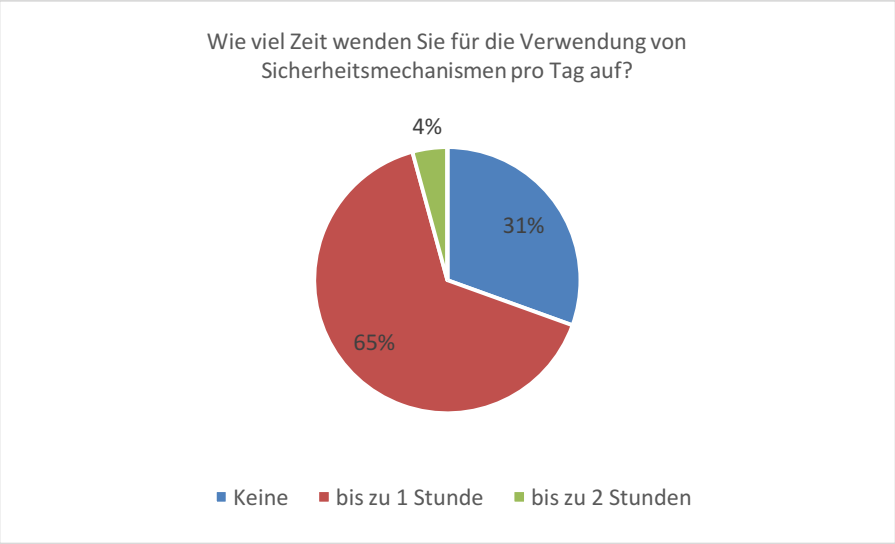

Abbildung 24: Zeitaufwand für die Verwendungen von Sicherheitsmechanismen laut den Befragten

2.2.1 Softwareanwender-Unternehmen

91% der Befragten, die in einem Softwareanwender-Unternehmen beschäftigt sind, kennen den Begriff IT-Sicherheit und 88% können auch eine Definition dafür angeben. 9% haben den Begriff IT-Sicherheit schon gehört, kennen den Begriff aber nicht wirklich (siehe Abbildung 25).

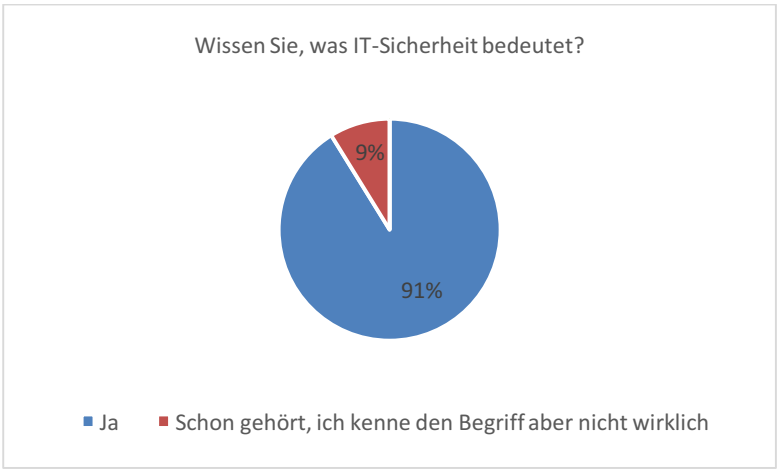

Abbildung 25: Verständnis des Begriffs IT-Sicherheit der Befragten aus Softwareanwender-Unternehmen

Auch hier sind 94% der Definition ansatzweise gemäß der Erläuterung von Sorge et al. [Sorge et al. 2013]. 3% sind leere Definitionen und ebenfalls 3% sind falsch oder können nicht gewertet werden.

Für 38% der Teilnehmer, die in einem Softwareanwender-Unternehmen angestellt sind, haben Sicherheitsmechanismen eine hohe Relevanz, für 56% sogar eine sehr hohe Relevanz. 6% schätzen die Wichtigkeit von Sicherheitsmechanismen als durchschnittlich ein. Keiner erachtet die Relevanz von Sicherheitsmechanismen als niedrig oder sehr niedrig (siehe Abbildung 26). Demzufolge stufen 94% der Befragten, die in Softwareanwender-Unternehmen einer Tätigkeit nachgehen, Sicherheitsmechanismen als wesentlichen Bestandteil von Software-Produkten ein.

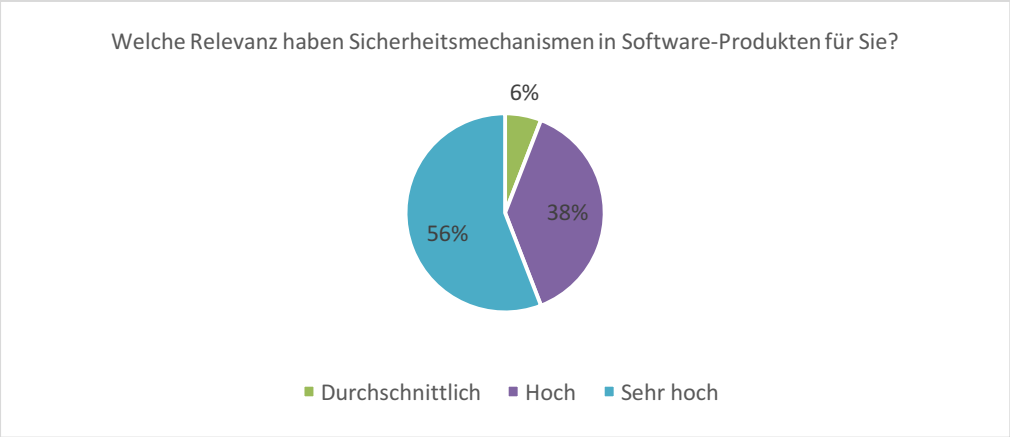

Abbildung 26: Relevanz von Sicherheitsmechanismen aus Sicht der Befragten aus Softwareanwender-Unternehmen

Als die am häufigsten verwendeten Sicherheitskomponenten der Befragten aus Softwareanwender-Unternehmen wurden (Nennungen ab 35%) Firewall, Virenschutz, Passwortmanager, Kommunikations- und Datenverschlüsselung, Digitale Signaturen und Spamfilter genannt (siehe Abbildung 27).

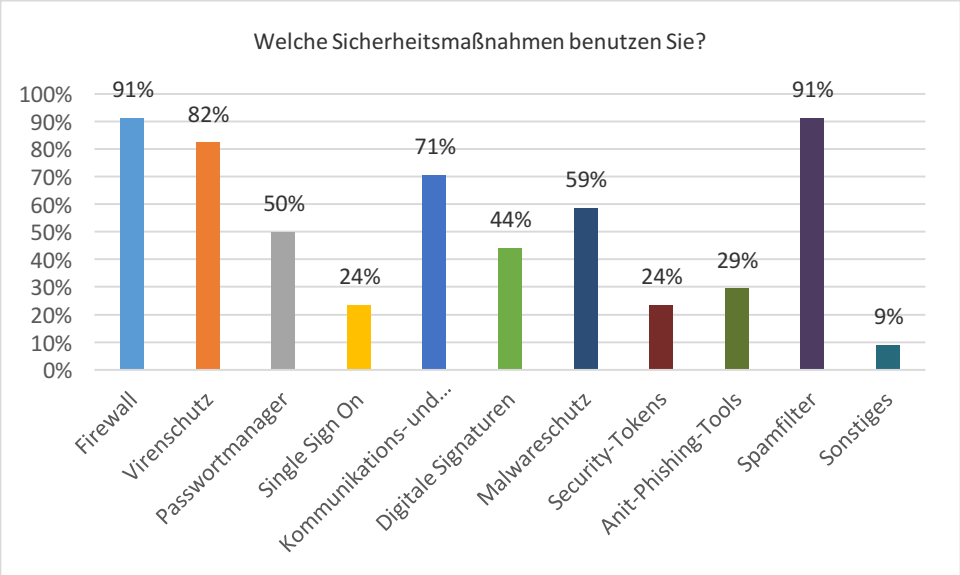

Abbildung 27: Verwendung von Sicherheitsmechanismen laut den Befragten aus Softwareanwender-Unternehmen

Für 65% der Befragten, die in einem Softwareanwender-Unternehmen angestellt sind, wirken sich Sicherheitsmechanismen nicht belastend auf ihre tägliche Arbeit bzw. auf ihr Nutzerverhalten aus. 35% der Teilnehmer empfinden Sicherheitsmechanismen als belastend. Auf keinen der Teilnehmer wirken sich Sicherheitsmechanismen sehr belastend aus[5] (siehe Abbildung 28).

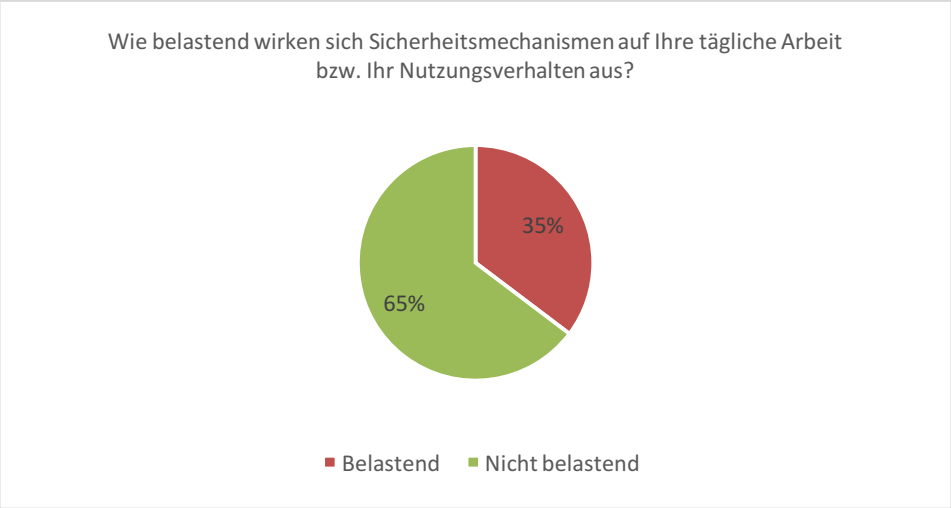

Abbildung 28: Belastungsgrad von Sicherheitsmechanismen aus Sicht der Befragten aus Softwareanwender-Unternehmen

62% der Teilnehmer, die in einem Softwareanwender-Unternehmen ihrer Tätigkeit nachgehen, benötigen bis zu 1 Stunde für die Verwendung von Sicherheitsmechanismen pro Tag, bei 9% sind es sogar zwischen 1 und 2 Stunden. 29% wenden keine Zeit dafür auf. Keiner der Teilnehmer wendet mehr als 2 Stunden auf (siehe Abbildung 29).

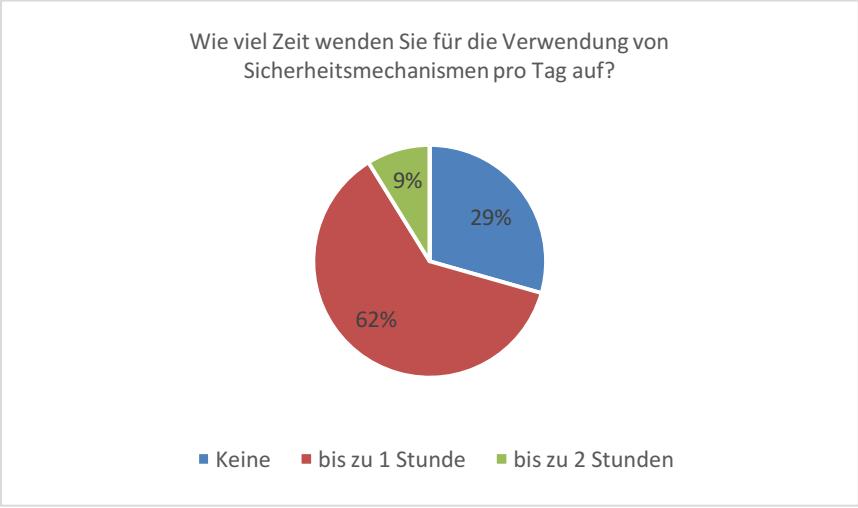

Abbildung 29: Zeitaufwand für die Verwendung von Sicherheitsmechanismen laut den Befragten aus Softwareanwender-Unternehmen

[5] Da es sich hierbei um eine allgemeine Frage handelt, sind keine Rückschlüsse auf einzelne Sicherheitskomponenten möglich.

2.2.2 Softwareentwickler-Unternehmen

89% der Befragten, die in einem Softwareentwickler-Unternehmen beschäftigt sind, kennen den Begriff IT-Sicherheit und sind zudem in der Lage eine Definition dafür anzugeben. 10% haben den Begriff IT-Sicherheit schon gehört, kennen den Begriff aber nicht wirklich. 1% kennen den Begriff nicht (siehe Abbildung 30).

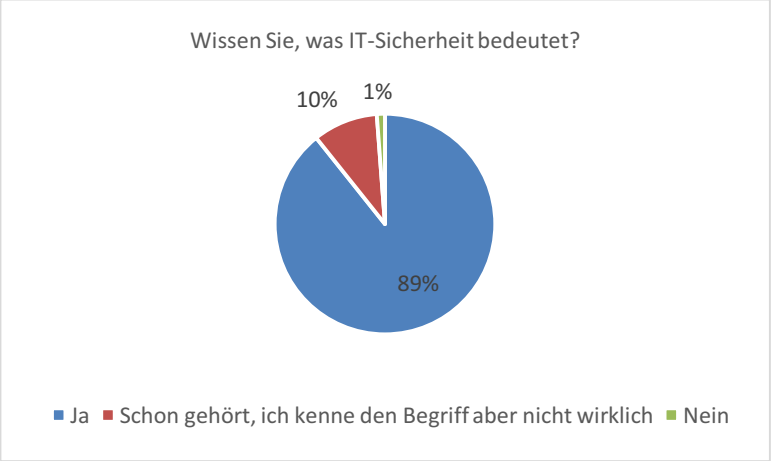

Abbildung 30: Verständnis des Begriffs IT-Sicherheit der Befragten aus Softwareentwickler-Unternehmen

95% der Teilnehmer aus Softwareentwickler-Unternehmen, die eine Definition für IT-Sicherheit geben, können ansatzweise den Begriff nach der Erklärung von Sorge et al. [Sorge et al.] erläutern. 2% geben eine leere Definition an. 3% der Definition sind falsch bzw. können nicht gewertet werden.

Für 41% der Befragten, die in einem Softwareentwickler-Unternehmen beschäftigt sind, haben Sicherheitsmechanismen in Software-Produkten eine hohe Relevanz. 46% geben sogar eine sehr hohe Relevanz an. 11% erachten die Relevanz von Sicherheitsmechanismen als durchschnittlich. Jeweils 1% schätzen die Relevanz von Sicherheitsmechanismen als niedrig oder sehr niedrig ein (siehe Abbildung 31). Folglich empfinden 87% der Befragten, deren Unternehmen Software entwickeln, Sicherheitsmechanismen als wesentlichen Bestandteil von Software-Produkten.

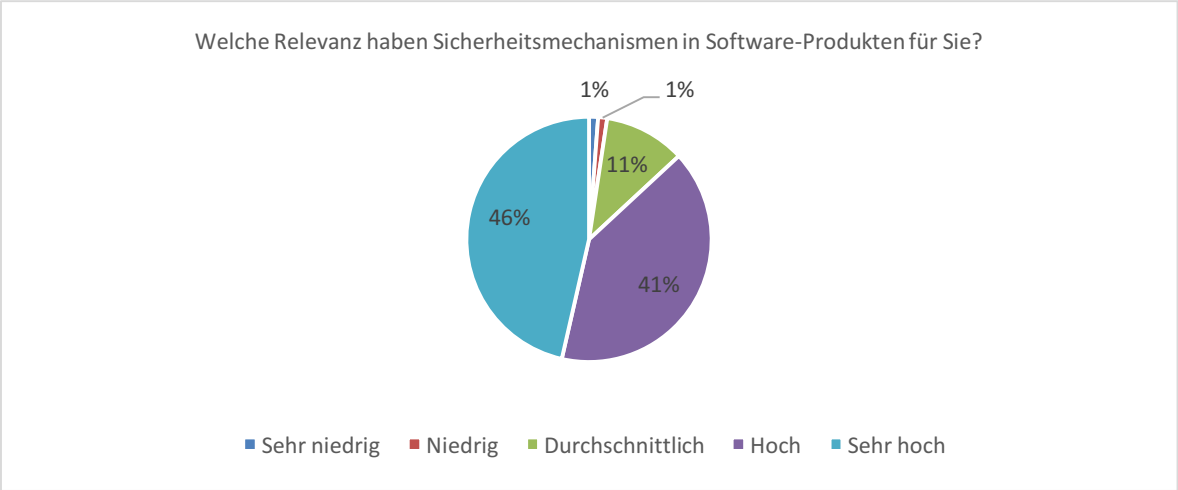

Abbildung 31: Relevanz von Sicherheitsmechanismen in Software-Produkten aus Sicht der Softwareentwickler-Unternehmen

Als die am häufigsten verwendeten Sicherheitsmaßnahmen der Befragten aus Softwareentwickler-Unternehmen wurden (Nennungen ab 35%) Firewall, Virenschutz, Passwortmanager, Kommunikations- und Datenverschlüsselung, Digitale Signaturen, Malwareschutz, Security-Tokens, Anti-Phishing-Tools und Spamfilter genannt (siehe Abbildung 32).

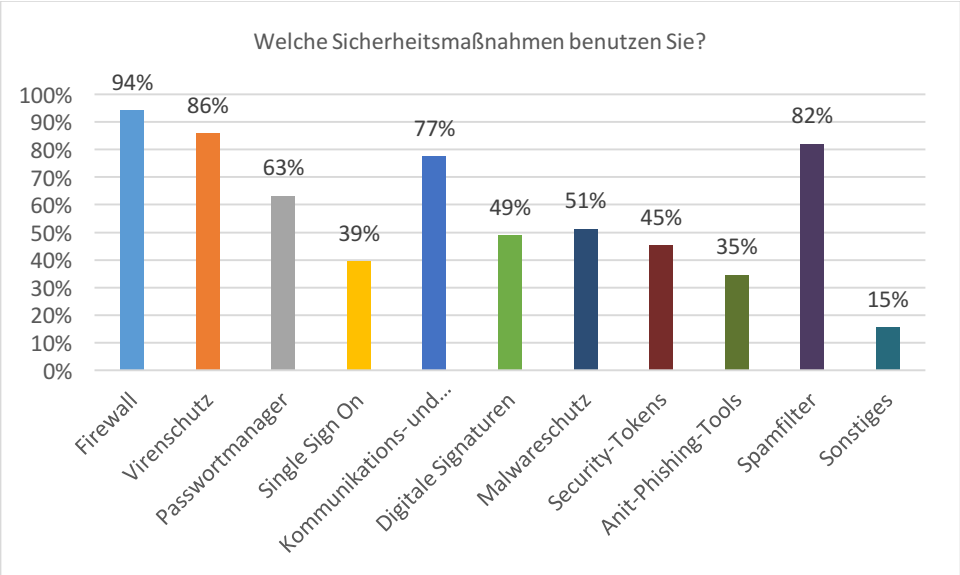

Abbildung 32: Verwendung von Sicherheitsmechanismen laut den Befragten in Softwareentwickler-Unternehmen

64% der Befragten empfinden Sicherheitsmechanismen als nicht belastend für ihre tägliche Arbeit bzw. für ihr Nutzerverhalten. Für 33% wirken sich Sicherheitsmechanismen belastend, für 3% sogar sehr belastend aus[6] (siehe Abbildung 33).

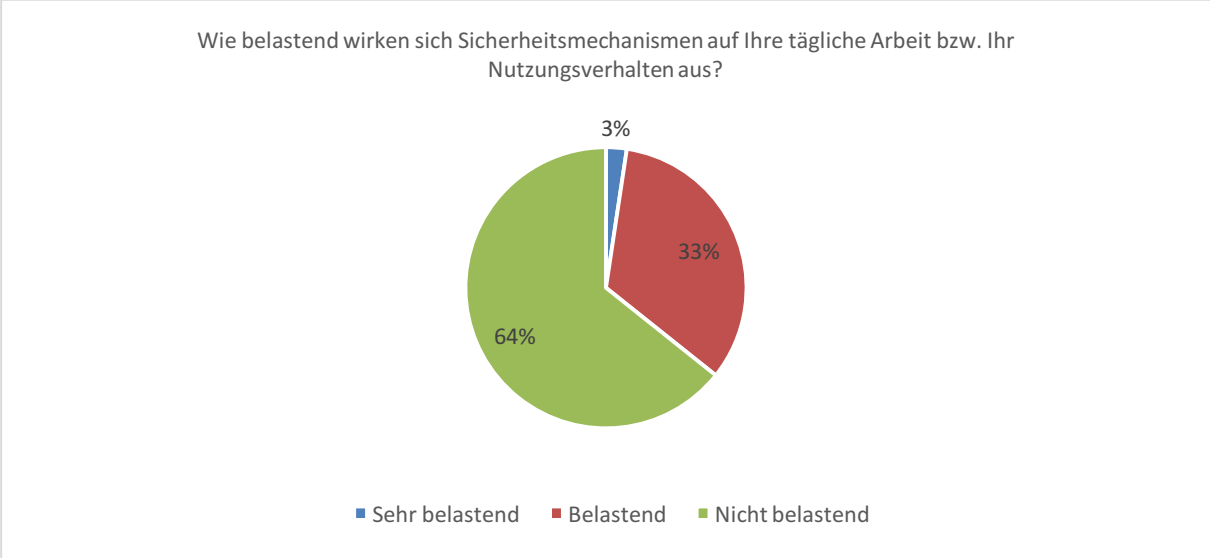

Abbildung 33: Belastungsgrad bei der Verwendung von Sicherheitsmechanismen laut den Befragten aus Softwareentwickler-Unternehmen

67% der Befragten aus Softwareentwickler-Unternehmen wenden bis zu 1 Stunde für die Verwendung von Sicherheitsmechanismen pro Tag auf, 2% sogar zwischen 1 und 2 Stunden. 31% wenden keine Zeit für Sicherheitsmechanismen auf. Keiner der Teilnehmer wendet mehr als 2 Stunden auf (siehe Abbildung 34).

[6] Da es sich hierbei um eine allgemeine Frage handelt, sind keine Rückschlüsse auf einzelne Sicherheitskomponenten möglich.

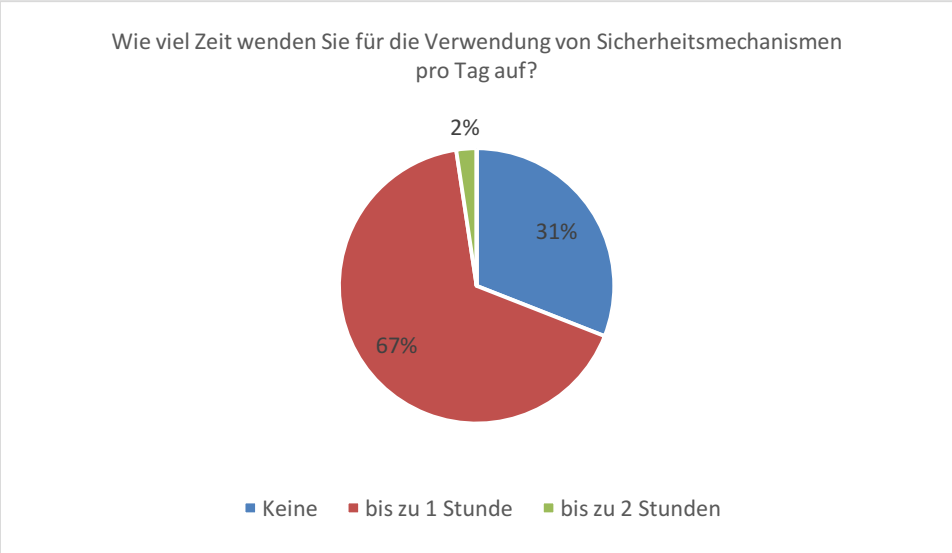

Abbildung 34: Zeitaufwand für die Verwendung von Sicherheitsmechanismen laut den Befragten aus Softwareentwickler-Unternehmen

2.2.3 Kleine und mittlere Unternehmen

86% der Befragten, die einer beruflichen Tätigkeit in einem KMU nachgehen, kennen den Begriff IT-Sicherheit. 86% von ihnen können auch eine Definition angeben. 14% haben den Begriff schon gehört, kennen den Begriff aber nicht wirklich. Keiner der Teilnehmer hat den Begriff noch nicht gehört (siehe Abbildung 35).

Abbildung 35: Verständnis des Begriffs IT-Sicherheit der Befragten aus KMU

95% der angegebenen Definitionen richten sich ansatzweise nach der Begriffserklärung von Sorge et al. [Sorge et al. 203]. 2% sind leere Definitionen. 3% der Antworten sind falsch oder sind nicht berücksichtigt worden.

37% der Befragten, die in einem KMU angestellt sind, erachten die Relevanz von Sicherheitsmechanismen als hoch, 48% sogar als sehr hoch. 12% schätzen die Relevanz von Sicherheitsmechanismen als durchschnittlich ein. 3% erachten die Relevanz jeweils als

niedrig bis sehr niedrig (siehe Abbildung 36). Folglich empfinden 85% der Befragten aus KMU Sicherheitsmechanismen als wesentlichen Bestandteil von Software-Produkten.

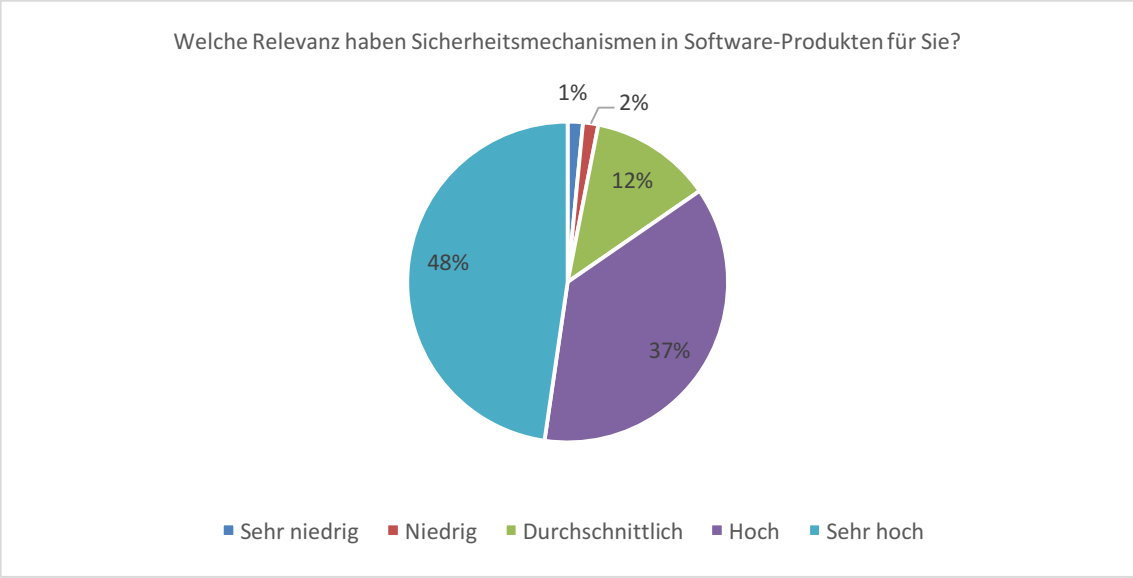

Abbildung 36: Relevanz von Sicherheitsmechanismen aus Sicht der Befragten aus KMU

Als die am häufigsten verwendeten Sicherheitsmaßnahmen der Befragten aus KMU wurden (Nennungen ab 35%) Firewall, Virenschutz, Passwortmanager, Kommunikations- und Datenverschlüsselung, Malwareschutz und Spamfilter genannt (siehe Abbildung 37).

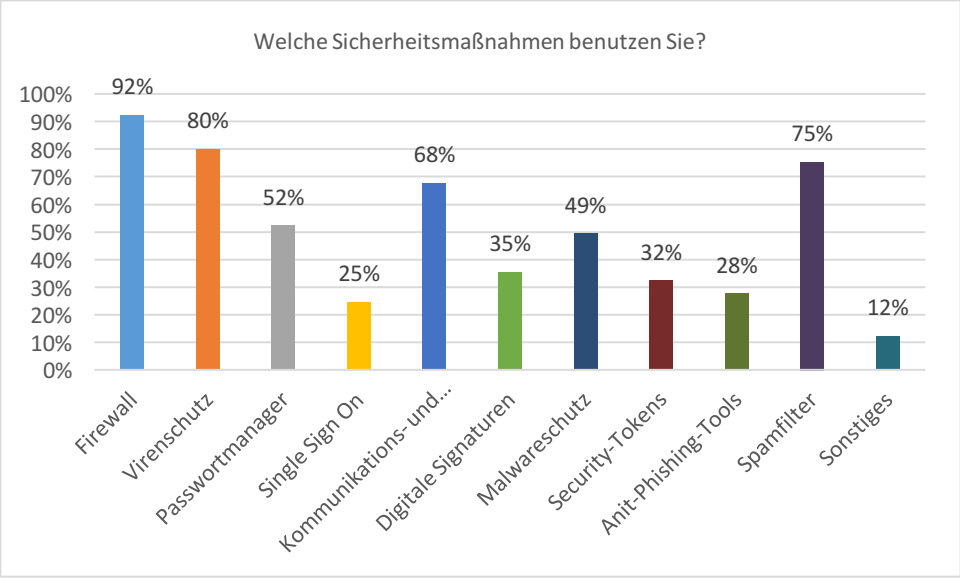

Abbildung 37: Verwendung von Sicherheitsmechanismen laut den Befragten aus KMU

Für 66% der Befragten, die in einem KMU beruflich tätig sind, wirken sich Sicherheitsmechanismen nicht belastend auf ihre tägliche Arbeit bzw. auf ihr Nutzungsverhalten aus. Bei 43% wirken sich Sicherheitsmechanismen belastend aus[7].

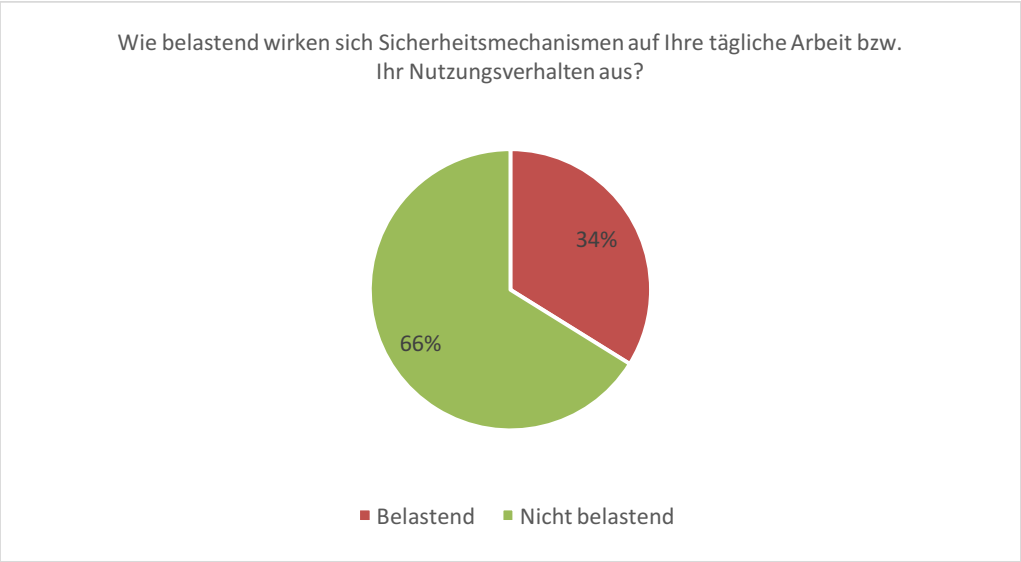

Abbildung 38: Belastungsgrad bei der Verwendung von Sicherheitsmechanismen aus Sicht der Befragten aus KMU

58% der Befragten aus KMU wenden bis zu 1 Stunde für die Verwendung von Sicherheitsmechanismen pro Tag auf, 5% sogar zwischen 1 und 2 Stunden. Keiner der Teilnehmer wendet mehr als 2 Stunden auf. 37% wenden keine Zeit für die Verwendung von Sicherheitsmechanismen auf (siehe Abbildung 39).

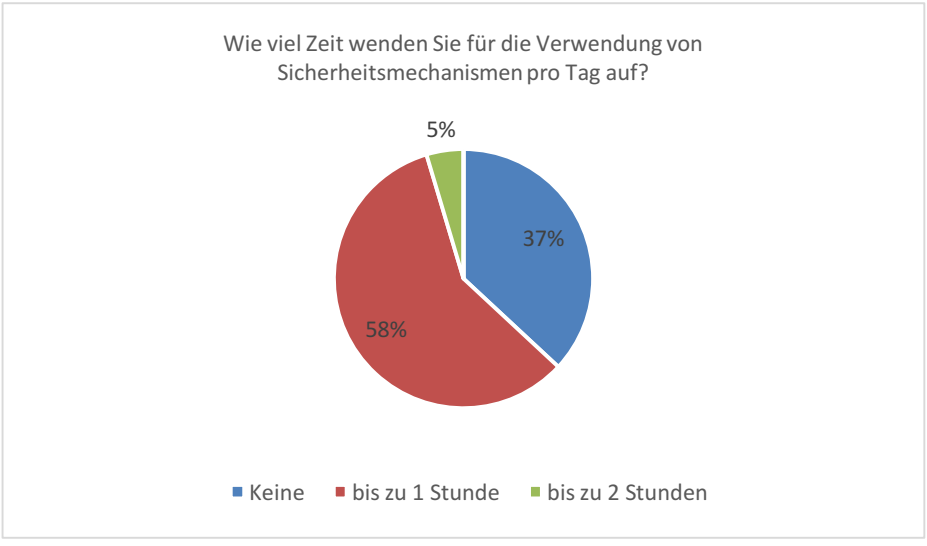

Abbildung 39: Zeitaufwand für die Verwendung von Sicherheitsmechanismen laut den Befragten aus KMU

[7] Da es sich hierbei um eine allgemeine Frage handelt, sind keine Rückschlüsse auf einzelne Sicherheitskomponenten möglich.

2.2.4 Großunternehmen

94% der Teilnehmer, welche eine berufliche Tätigkeit in einem GU ausüben, kennen den Begriff IT-Sicherheit und können auch eine Definition dafür angeben. 4% haben den Begriff schon gehört, kennen Begriff aber nicht wirklich. 2% kennen den Begriff nicht (siehe Abbildung 40).

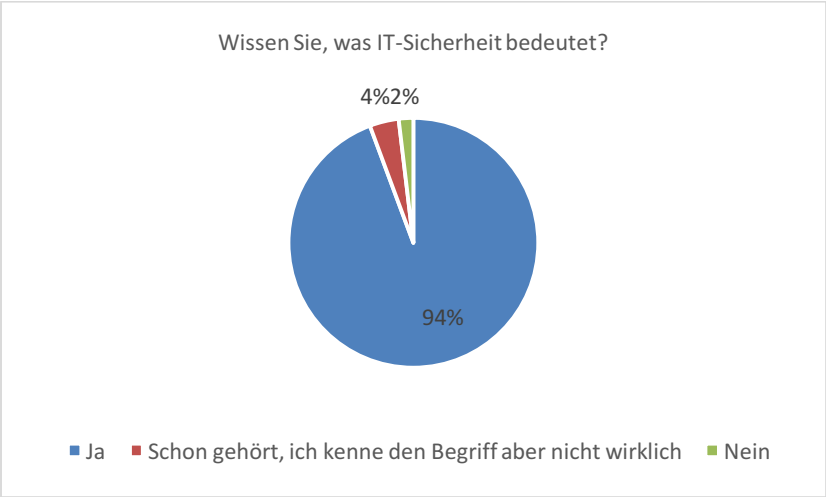

Abbildung 40: Verständnis des Begriffs IT-Sicherheit der Befragten aus GU

94% der Definitionen sind ansatzweise gemäß der Erläuterung von Sorge et al. [Sorge et al. 2013]. 4% der Definitionen sind leer und 2% sind falsch oder sind nicht gewertet worden.

43% der Befragten aus GU schätzen die Relevanz von Sicherheitsmechanismen in Software-Produkten als hoch ein, 51% sogar als sehr hoch. 6% erachten die Relevanz von Sicherheitsmechanismen als durchschnittlich. Keiner der Teilnehmer empfindet die Relevanz von Sicherheitsmechanismen in Software-Produkten als niedrig oder sehr niedrig (siehe Abbildung 41). Demnach sind Sicherheitsmechanismen in Software-Produkten für 94% der Befragten, die eine berufliche Tätigkeit in einer GU ausüben, ein wesentlicher Bestandteil von Software-Produkten.

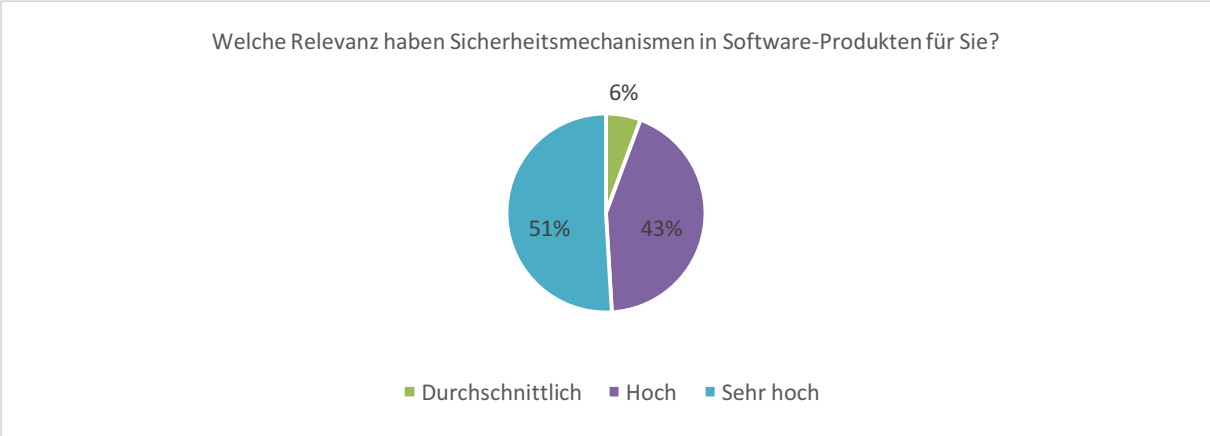

Abbildung 41: Relevanz von Sicherheitsmechanismen in Software-Produkten aus Sicht der Befragten in GU

Als die am häufigsten verwendeten Sicherheitsmaßnahmen bei den Befragten aus GU wurden (Nennungen ab 35%) Firewall, Virenschutz, Passwortmanager, Single Sign-On, Kommunikations- und Datenverschlüsselung, Digitale Signaturen, Malwareschutz, Security-Tokens, Anti-Phishing-Tools und Spamfilter genannt (siehe Abbildung 42).

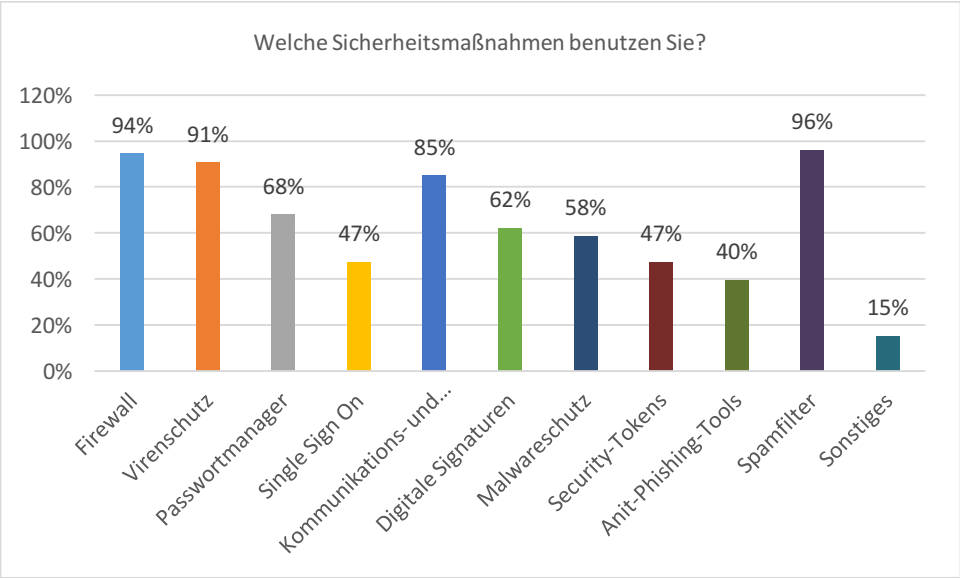

Abbildung 42: Verwendung von Sicherheitsmechanismen laut den Befragten aus GU

Für 62% der Befragten aus GU wirken sich Sicherheitsmechanismen auf ihre tägliche Arbeit bzw. auf ihr Nutzungsverhalten nicht belastend aus. Auf 34% wirken sich Sicherheitsmechanismen belastend, auf 4% sogar sehr belastend aus[8] (siehe Abbildung 43).

[8] Da es sich hierbei um eine allgemeine Frage handelt, sind keine Rückschlüsse auf einzelne Sicherheitskomponenten möglich.

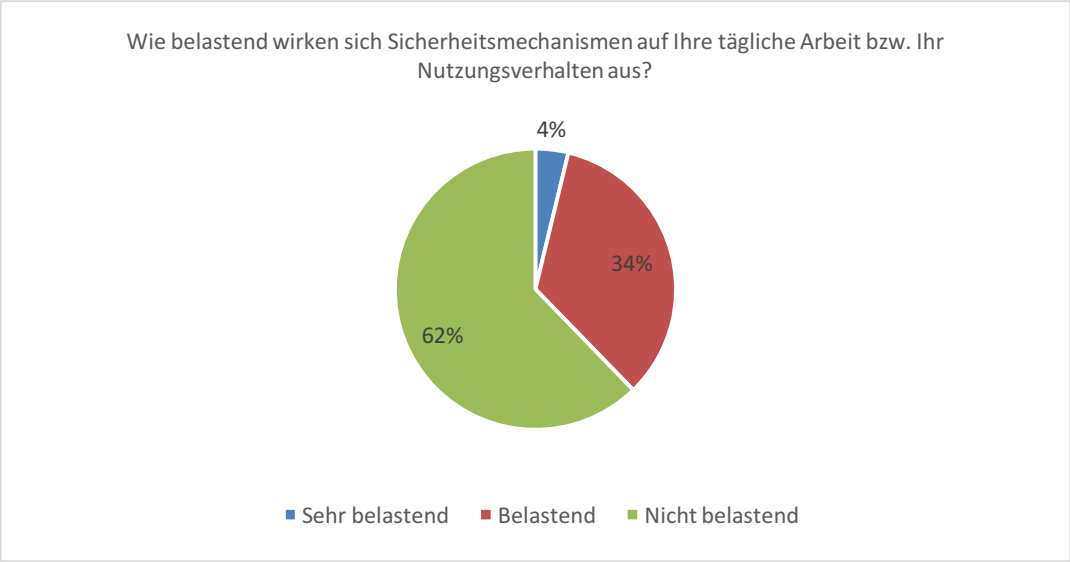

Abbildung 43: Belastungsgrad bei der Verwendung von Sicherheitsmaßnahmen aus Sicht der Befragten aus GU

73% der Befragten aus GU wenden bis zu 1 Stunde für die Verwendung von Sicherheitsmechanismen pro Tag auf. Bei 4% sind es sogar zwischen 1 und 2 Stunden. 23% wenden keine Zeit auf (siehe Abbildung 44).

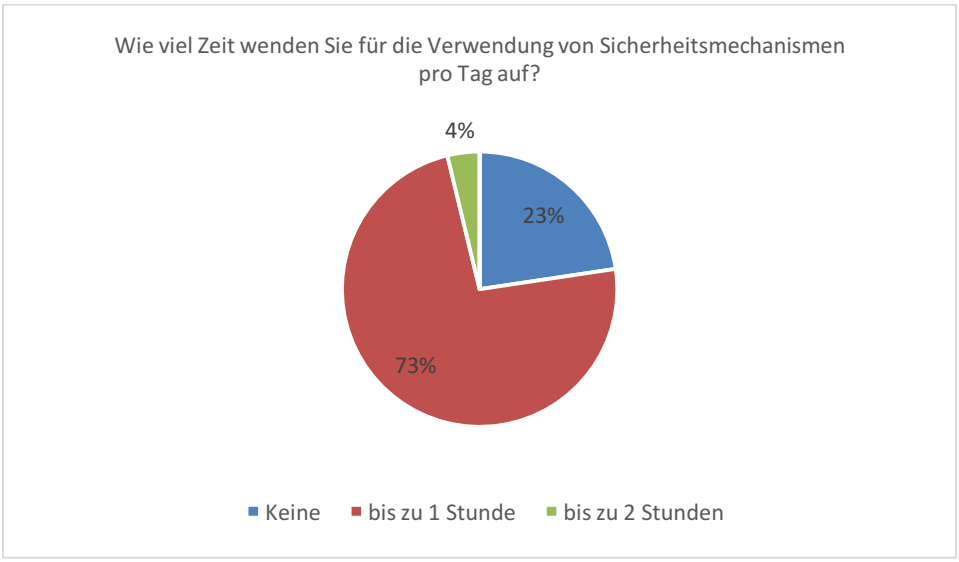

Abbildung 44: Zeitaufwand für die Verwendung von Sicherheitsmechanismen laut den Befragten aus GU

2.3 Einordnung und Relevanz von Usable Security

Als die am häufigsten genannten Antworten auf die Frage „Wie müssen gebrauchstaugliche Sicherheitsmechanismen (Usable Security) in Ihren Augen gestaltet sein?“ antworten die Befragten mit (Nennung ab 35%) im Verborgenen, transparent, nachvollziehbar und einfach anwendbar. Unter Sonstiges wurde u.a. „kontextadäquat“ und „automatisch“ genannt.

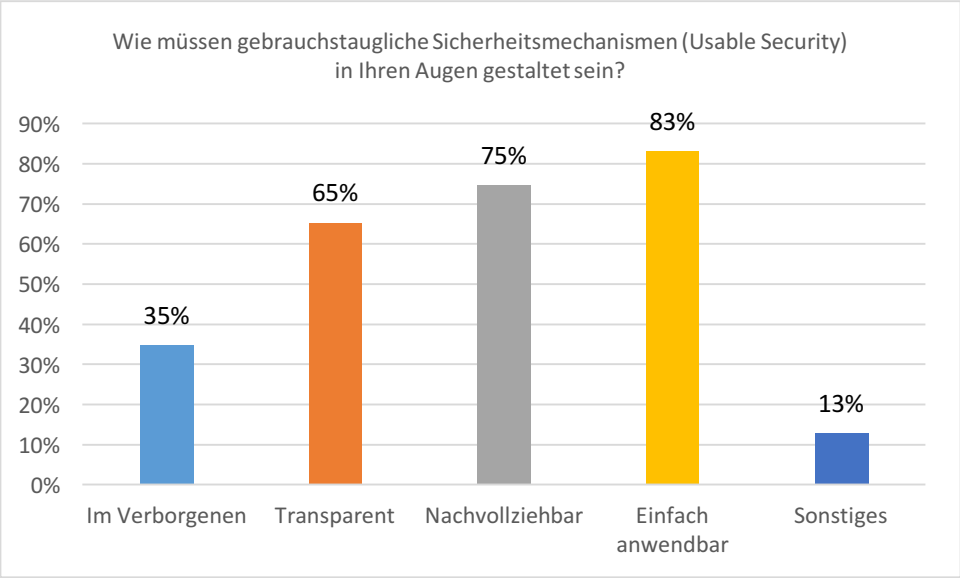

Abbildung 45: Merkmale für die Gestaltung von Usable Security aus Sicht der Befragten

Die Bereiche, in denen akuter Handlungsbedarf für Usable Security gesehen wird, sind (Nennung ab 35%) Zugriffskontrollsysteme, E-Mail-Sicherheit, Datenspeicherung, Mobile Security, Social Media Privacy, Softwareentwicklung und Administration von Sicherheitsfunktionen (siehe Abbildung 46).

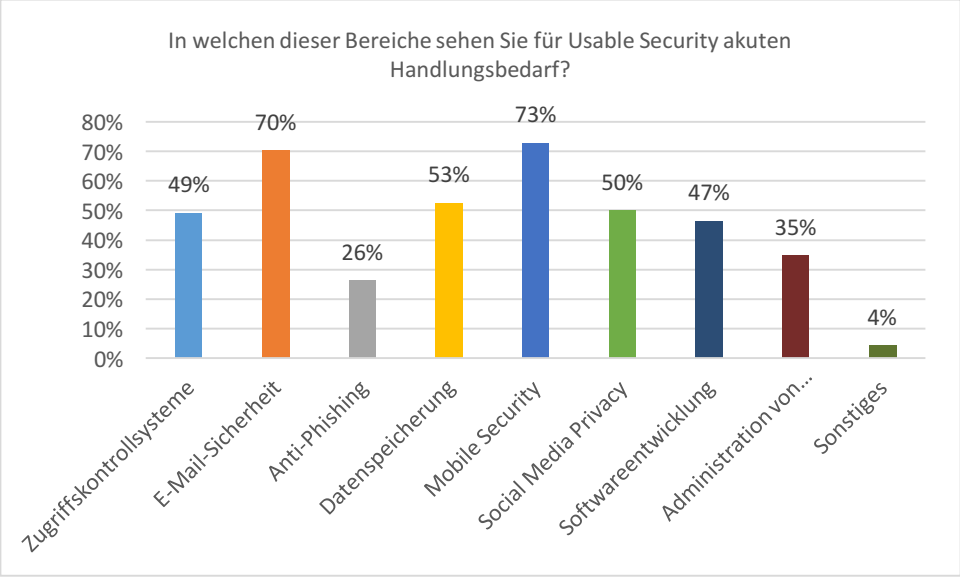

Abbildung 46: Handlungsbedarf für Usable Security aus Sicht der Befragten

2.3.1 Softwareanwender-Unternehmen

Als die am häufigsten genannten Merkmale auf die Frage: „Wie müssen gebrauchstaugliche Sicherheitsmechanismen (Usable Security) in Ihren Augen gestaltet sein?“ antworten die Teilnehmer aus Softwareanwender-Unternehmen mit (Nennungen ab 35%) transparent, nachvollziehbar und einfach anwendbar (siehe Abbildung 47).

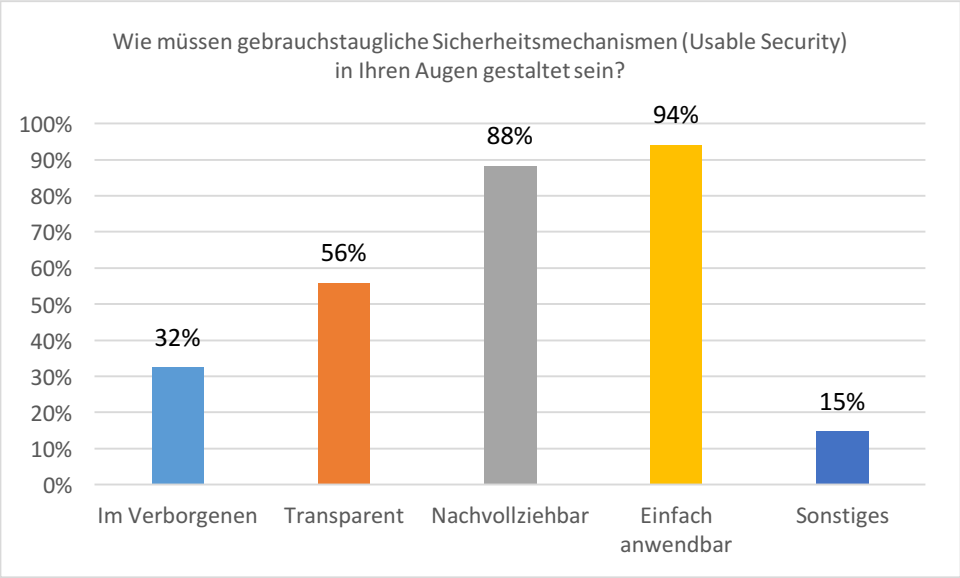

Abbildung 47: Merkmale für die Gestaltung von Usable Security aus Sicht der Befragten aus Softwareanwender-Unternehmen

Akuten Handlungsbedarf für Usable Security sehen die Befragten aus Softwareanwender-Unternehmen am häufigsten im Bereich (Nennung ab 35%) Zugriffskontrollsysteme, E-Mail-Sicherheit, Datenspeicherung, Mobile Security, Social Media Privacy, Softwareentwicklung und Administration von Sicherheitsfunktionen.

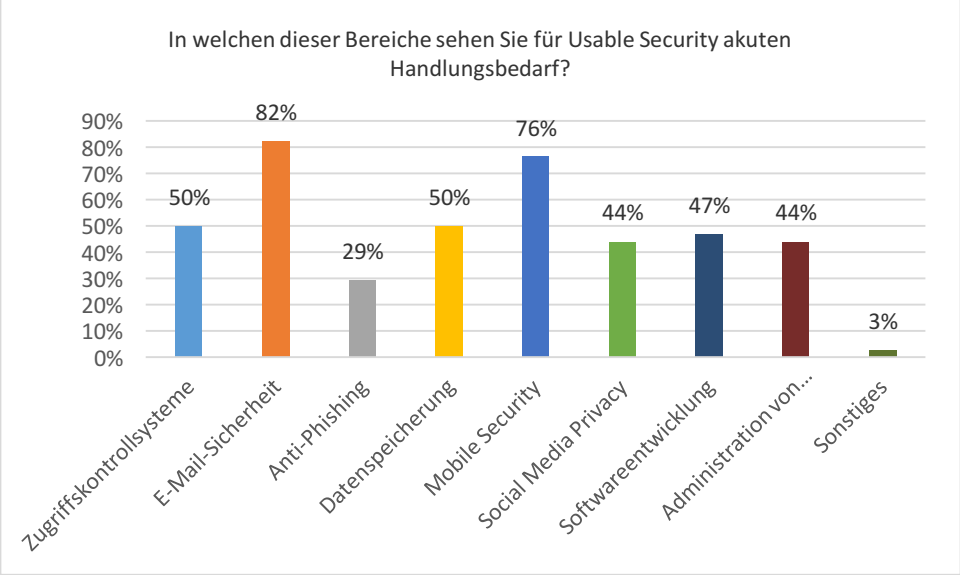

Abbildung 48: Handlungsbedarf für Usable Security aus Sicht von Softwareanwender-Unternehmen

74% der Befragten aus Softwareanwender-Unternehmen wählten die Funktionalität als erstes Kriterium für die Auswahl von Software. Usability und Sicherheit wählen jeweils nur 3% als erstes Auswahlkriterium. Als zweites Kriterium geben 26% der Befragten aus

Softwareanwender-Unternehmen Usability an. 21% wählen hingegen Sicherheit als zweites Auswahlkriterium. 32% erachten Usability als drittes Auswahlkriterium und 15% wählen Sicherheit an dritter Stelle für die Auswahl von Software. Erst bei Rangfolge 4 bestimmen 41% die Sicherheit. In dieser Rangfolge stimmen 18% für Usability ab (siehe Abbildung 49). Anhand von Abbildung 49 ist erkennbar, dass die Funktionalität für die meisten Befragten die höchste Priorität bei der Auswahl von Software hat. Usability und Sicherheit spielen hingegen nur eine untergeordnete Rolle[9].

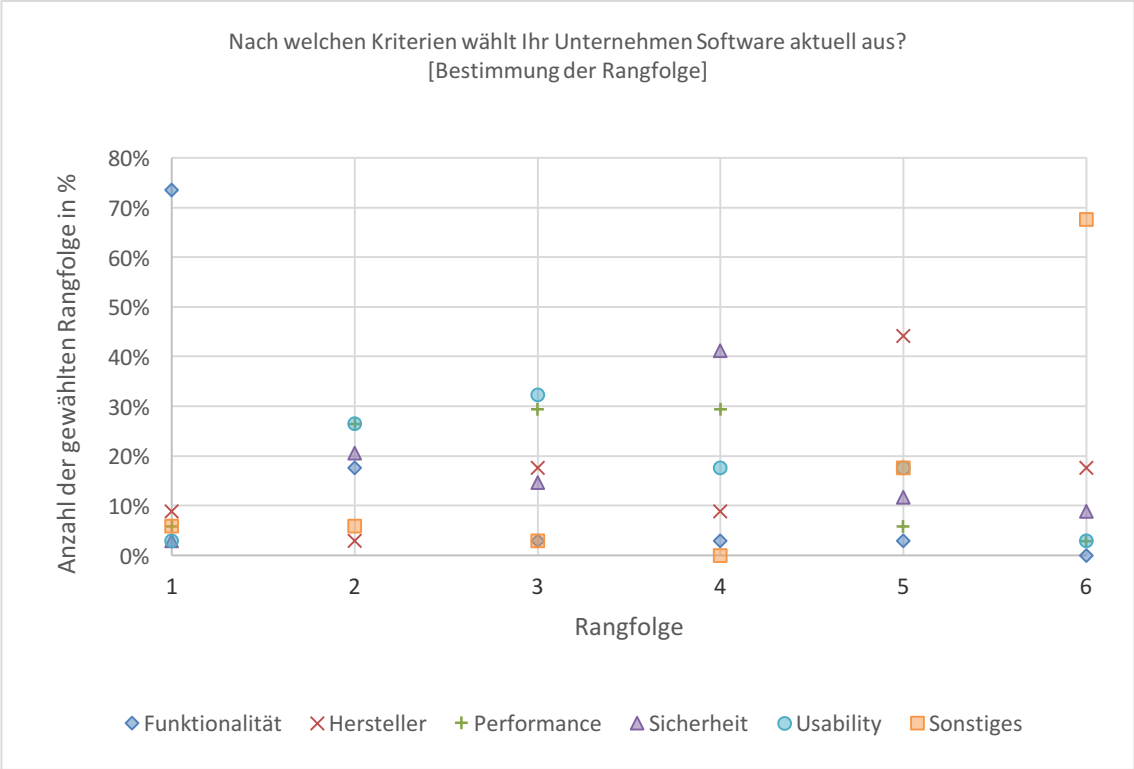

Abbildung 49: Kriterien zur Auswahl von Software laut den Befragten aus Softwareanwender-Unternehmen

2.3.2 Softwareentwickler-Unternehmen

Als die am häufigsten genannten Merkmale auf die Frage „Wie müssen gebrauchstaugliche Sicherheitsmechanismen (Usable Security) in Ihren Augen gestaltet sein?“ antworten die Befragten aus Softwareentwickler-Unternehmen mit (Nennungen ab 35%): im Verborgenen, nachvollziehbar, transparent und einfach anwendbar (siehe Abbildung 50).

[9] Da diese Frage sehr allgemein gestellt ist, kann hieraus nicht hergeleitet werden, welche Kriterien für die Auswahl von spezifischer Software ausschlaggebend sind.

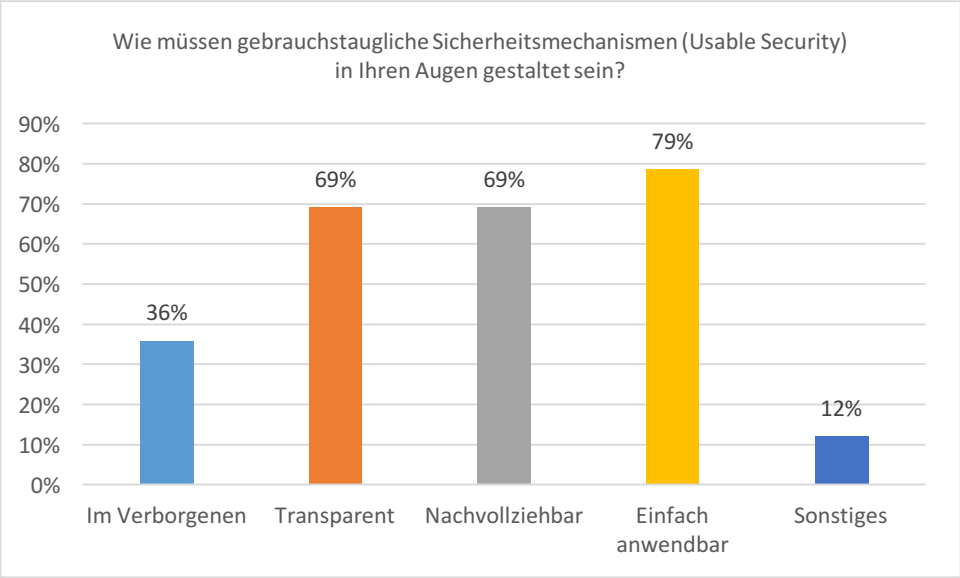

Abbildung 50: Merkmale für die Gestaltung von Usable Security aus Sicht der Befragten aus Softwareentwickler-Unternehmen

Akuten Handlungsbedarf für Usable Security sehen die Teilnehmer, welche in einem Softwareentwickler-Unternehmen angestellt sind, im Bereich (Nennungen ab 35%): Zugriffskontrollsysteme, E-Mail-Sicherheit, Datenspeicherung, Mobile Security, Social Media Privacy und Softwareentwicklung (siehe Abbildung 51).

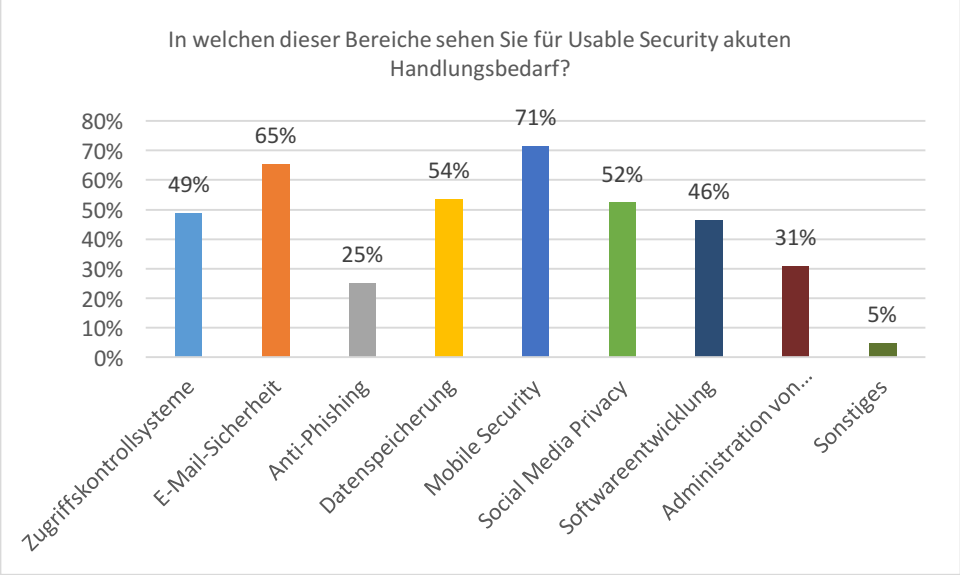

Abbildung 51: Handlungsbedarf für Usable Security aus Sicht der Befragten aus Softwareentwickler-Unternehmen

2.3.3 Kleine und mittlere Unternehmen

Als die am häufigsten genannten Antworten auf die Frage „Wie müssen gebrauchstaugliche Sicherheitsmechanismen (Usable Security) in Ihren Augen gestaltet sein?“ wählten die

Befragten aus KMU die Merkmale (Nennungen ab 35%): im Verborgenen, transparent, nachvollziehbar und einfach anwendbar (siehe Abbildung 52).

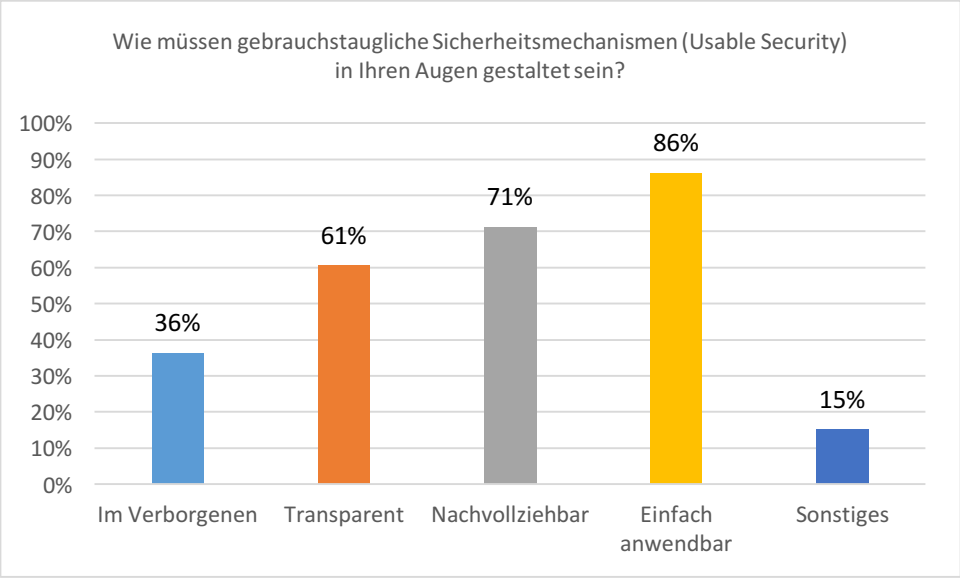

Abbildung 52: Merkmale für die Gestaltung von Usability Security aus Sicht der Befragten aus KMU

Die am häufigsten genannten Bereiche, in denen die Befragten aus KMU Handlungsbedarf für Usable Security sehen, sind (Nennungen ab 35%): Zugriffskontrollsysteme, E-Mail-Sicherheit, Datenspeicherung, Mobile Security, Social Media Privacy und Softwareentwicklung (siehe Abbildung 53).

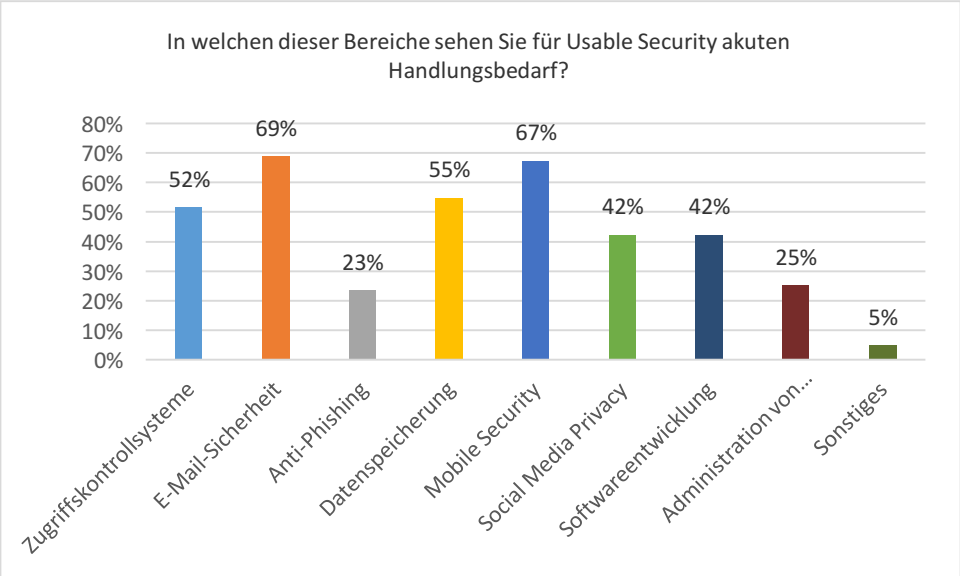

Abbildung 53: Handlungsbedarf für Usable Security aus Sicht der Befragten aus KMU

Für 80% der Befragten aus einem Softwareanwender-KMU ist Funktionalität das erste Kriterium für die Auswahl von Software. Nur 5% wählten hierfür Usability oder Sicherheit. Als zweites Kriterium wählten 35% Usability und 25% Sicherheit. 30% stimmten für Usability als drittes Kriterium ab, wohingegen in der gleichen Rangfolge 10% für Sicherheit stimmten. Erst als viertes Kriterium wählten 45% Sicherheit. In derselben Rangfolge wählten 15% Usability (siehe Abbildung 54). Auch hier lässt sich anhand von Abbildung 54 ableiten, dass für die Befragten aus KMU die Funktionalität ein wesentliches Kriterium für die Auswahl von Software ist. Usability und Sicherheit hat auch hier bei vielen Befragten nicht die höchste Priorität[10].

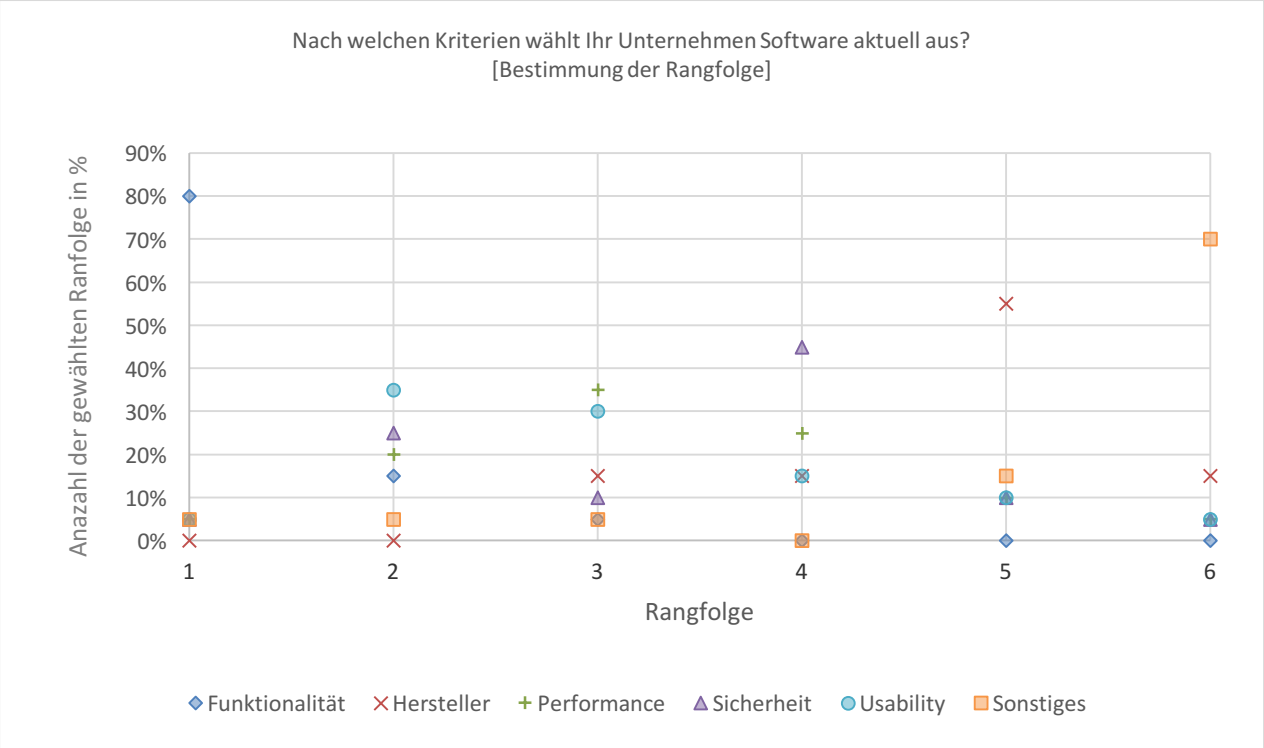

Abbildung 54: Kriterien zur Auswahl von Software laut den Befragten aus Softwareanwender-KMU

2.3.4 Großunternehmen

Auf die Frage „Wie müssen gebrauchstaugliche Sicherheitsmechanismen (Usable Security) in Ihren Augen gestaltet sein?“ stimmten die Befragten aus GU am häufigsten für (Nennungen ab 35%): transparent, nachvollziehbar und einfach anwendbar (siehe Abbildung 55).

[10] Da diese Frage sehr allgemein gestellt ist, kann hieraus nicht hergeleitet werden, welche Kriterien für die Auswahl von spezifischer Software ausschlaggebend sind.

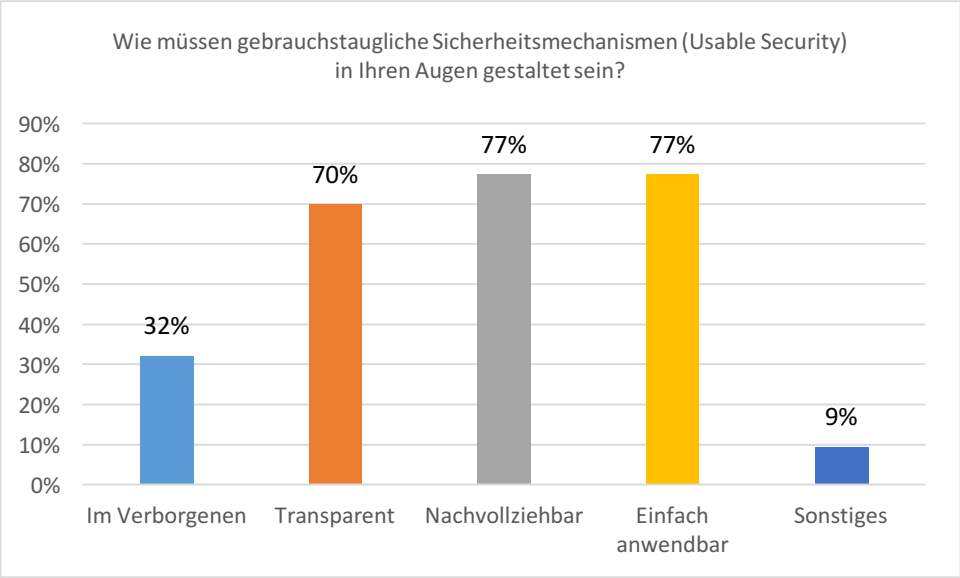

Abbildung 55: Merkmale für die Gestaltung von Usable Security aus Sicht der Befragten aus GU

Die Befragten aus GU sehen am häufigsten Handlungsbedarf für Usability in den Bereichen (Nennungen ab 35%): Zugriffskontrollsysteme, E-Mail-Sicherheit, Datenspeicherung, Mobile Security, Social Media Privacy, Softwareentwicklung und Administration von Sicherheitsfunktionen (siehe Abbildung 56).

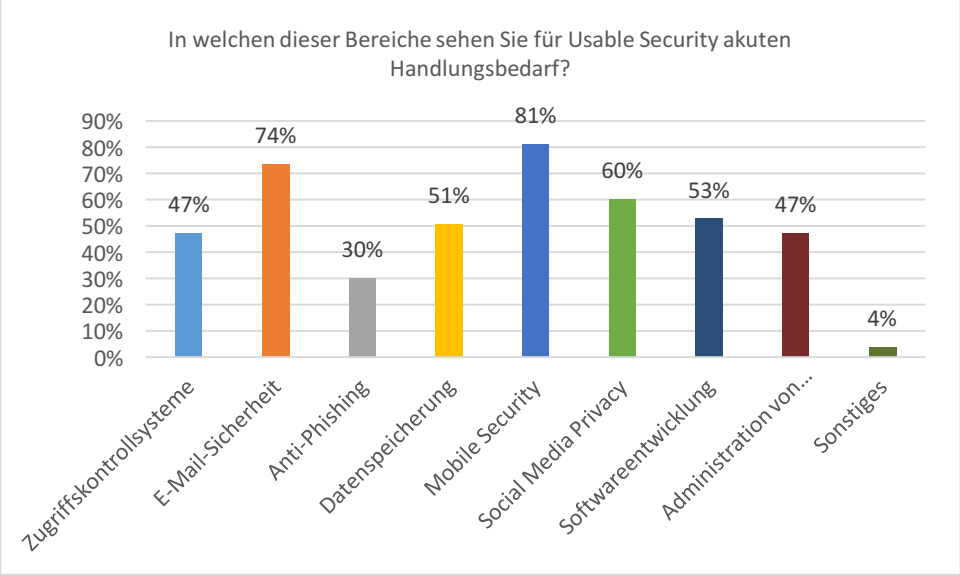

Abbildung 56: Handlungsbedarf für Usable Security aus Sicht der Befragen aus GU

64% der Teilnehmer aus einem Softwareanwender-GU wählten die Funktionalität als erstes Auswahlkriterium für Software. Keiner wählte Usability oder Sicherheit als erstes Auswahlkriterium. Jeweils 14% stimmten für Usability und Sicherheit als zweites Kriterium. Auf Rang 3 wählten 36% Usability und 21% Sicherheit. Als viertes Auswahlkriterium wählten 36% Sicherheit und 21% Usability (siehe Abbildung 57). Ebenfalls kann anhand der Abbildung

57 erschlossen werden, dass Usability und Sicherheit nicht die höchste Priorität bei den Befragten aus GU haben, wenn diese Software auswählen[11].

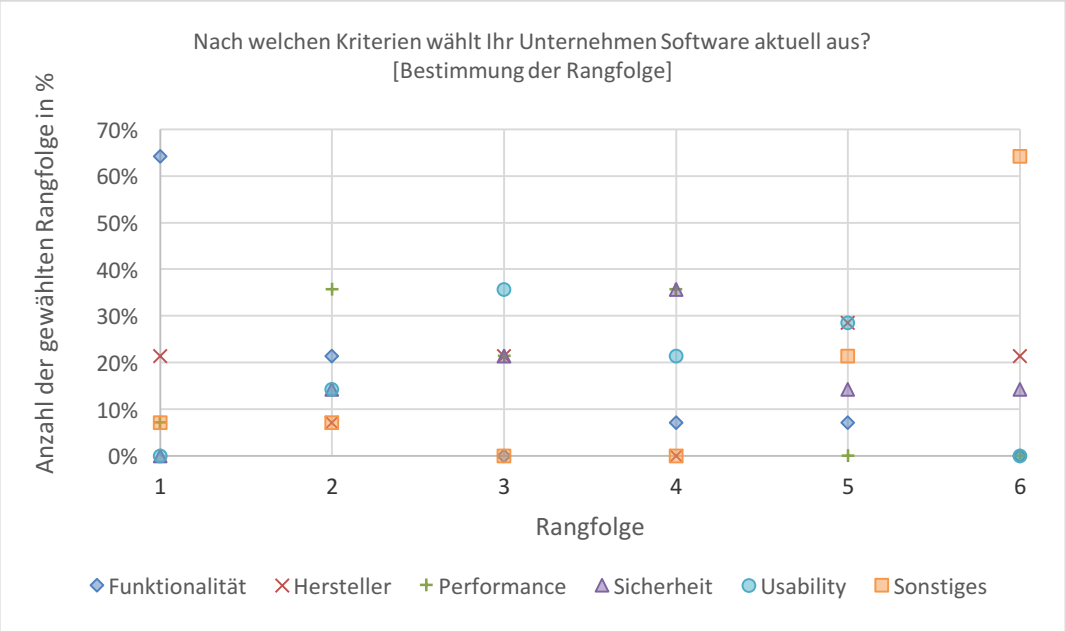

Abbildung 57: Kriterien zur Auswahl von Software laut den Befragten aus Softwareanwender-GU

2.4 Aktueller Umsetzungsgrad von Usability und IT-Sicherheit

In diesem Kapitel werden die Antworten zu dem aktuellen Umsetzungsgrad von Usability und IT-Sicherheit ausgewertet. Wie schon oben erwähnt, wurde nicht allen Teilnehmern die selben Fragen gestellt. Softwareanwender- und Softwareentwickler-Unternehmen mussten unterschiedliche Fragen beantworten.

2.4.1 Softwareanwender-Unternehmen

Bei 47% der Befragten aus Softwareanwender-Unternehmen finden Sicherheitsguidelines oder Sicherheitschecklisten für Software im Unternehmen Anwendung, bei 53% hingegen nicht (siehe Abbildung 58).

[11] Da diese Frage sehr allgemein gestellt ist, kann hieraus nicht hergeleitet werden, welche Kriterien für die Auswahl von spezifischer Software ausschlaggebend sind.

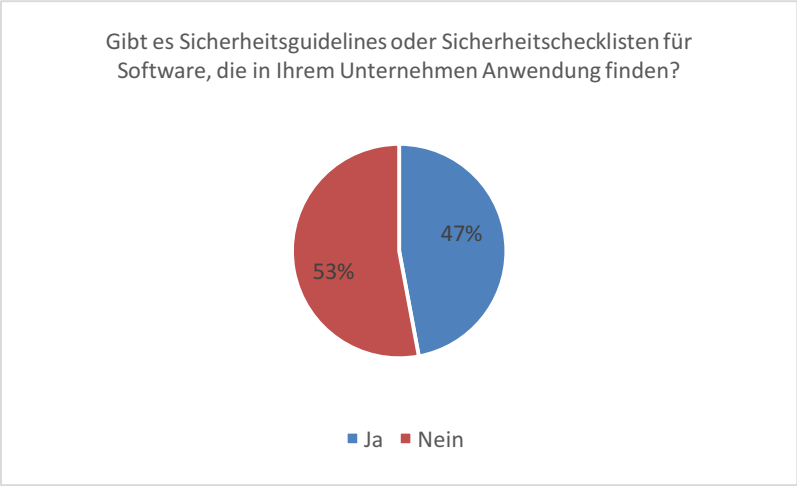

Abbildung 58: Anwendung von Sicherheitsguidelines laut den Befragten

44% der Teilnehmer aus Unternehmen, in denen Sicherheitsguidelines oder Sicherheitschecklisten Anwendung finden, geben an, dass ihr Unternehmen regulatorische Rahmenbedingungen, Zertifizierungen oder Ähnliches berücksichtigen muss. 31% müssen diese nicht beachten. 25% können oder wollen zu dieser Frage keine Stellung nehmen (siehe Abbildung 59).

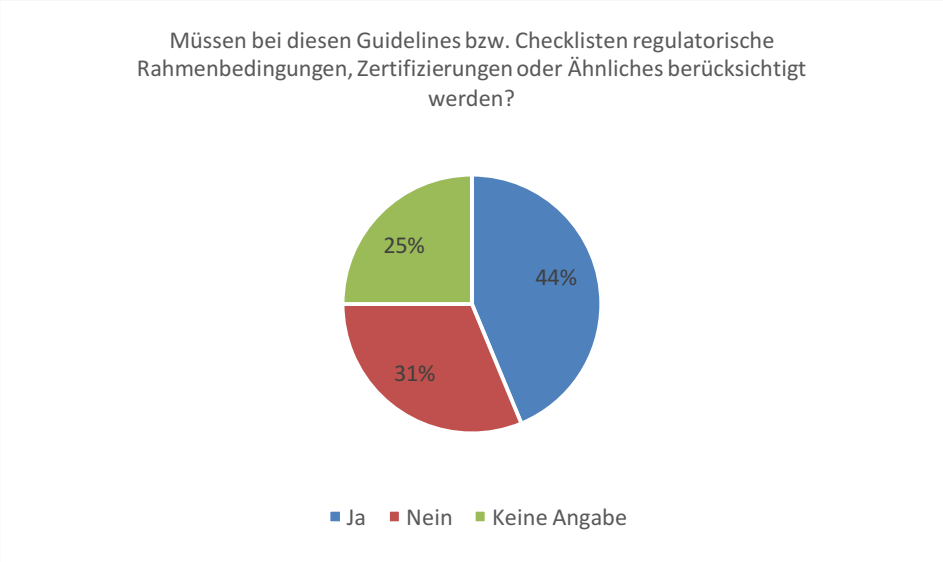

Abbildung 59: Berücksichtigung von regulatorischen Rahmenbedingungen, Zertifizierungen oder Ähnlichem laut den Befragten aus Softwareanwender-Unternehmen

Als konkrete regulatorische Rahmenbedingungen, Zertifizierungen oder Ähnliches geben die Befragen u. a. Folgendes an: „ISO 27001“, „Berücksichtigung von Zugriffsrechten extern wie intern“ und „ISO Standards (insb. Qualität und Sicherheit)“.

2.4.2 Softwareentwickler-Unternehmen

44% der Befragten aus Softwareentwickler-Unternehmen geben an, dass Usability-Engineering punktuell im Softwareentwicklungsprozess ihres Unternehmens integriert ist. 40% geben sogar an, dass Usability-Engineering ein ganzheitlicher integraler Bestandteil im Softwareentwicklungsprozess ist. Bei 10% wird Usability-Engineering nur am Ende

durchgeführt. Bei 6% findet kein Usability-Engineering statt (siehe Abbildung 60). Folglich geben 94% der Teilnehmer aus Softwareentwickler-Unternehmen an, dass Usability-Engineering in ihrem Unternehmen Bestandteil des Softwareentwicklungsprozesses ist.

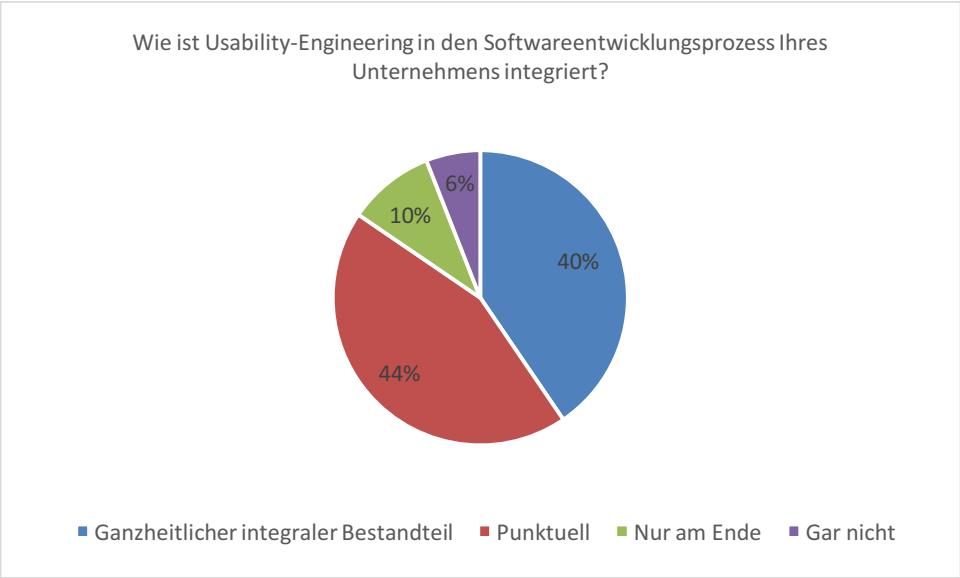

Abbildung 60: Integrationsgrad von Usability-Engineering im Softwareentwicklungsprozess laut den Befragten aus Softwareentwickler-Unternehmen

Security-Engineering wird bei 49% der Befragten aus Softwareentwickler-Unternehmen punktuell in den Softwareentwicklungsprozess integriert. Für 38% ist das Security-Engineering sogar ein ganzheitlicher integraler Bestandteil. Bei 8% findet Security-Engineering nur am Ende statt. 5% führen kein Security-Engineering durch (siehe Abbildung 61). Somit geben 95% der Teilnehmer an, dass Security-Engineering in ihrem Unternehmen Bestandteil des Softwareentwicklungsprozesses ist.

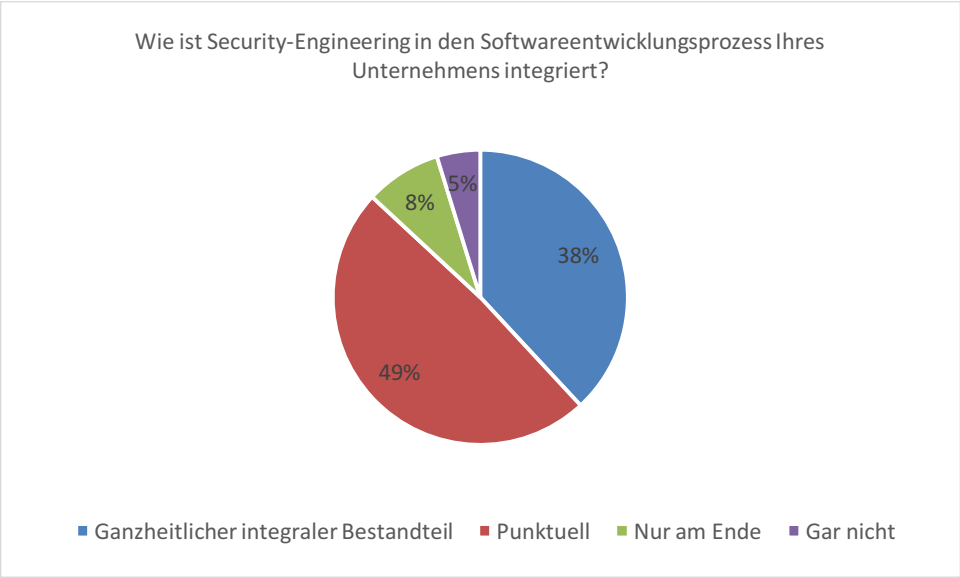

Abbildung 61: Integrationsgrad von Security-Engineering im Softwareentwicklungsprozess laut den Befragten aus Softwareentwickler-Unternehmen

Als adäquate Methoden und Werkzeuge im Usability-Engineering und Security-Engineering werden am häufigsten (Nennungen ab 35%) Vorgehensmodelle, Patterns, Guidelines, Checklisten und Tools angesehen (siehe Abbildung 62). Unter Sonstiges wurde u. a. „Iterationen durch Nutzerstudien“, „User Testing“ und „Penetrationstests“ angegeben.

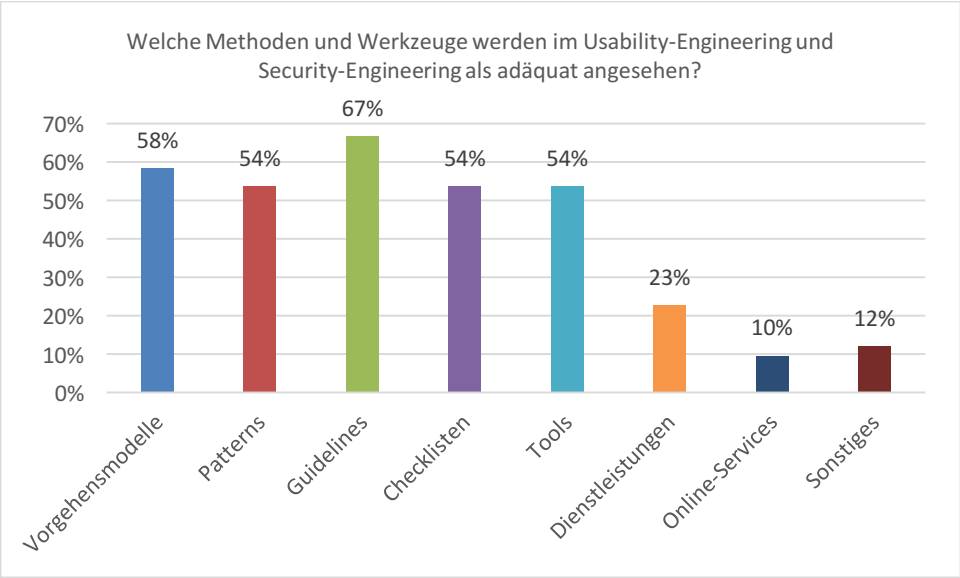

Abbildung 62: Adäquate Methoden und Werkzeuge im Usability-Engineering und Security-Engineering aus Sicht der Befragten aus Softwareentwickler-Unternehmen

Auf die Frage „Wie darf sich der aktuelle Softwareentwicklungsprozess in Ihrem Unternehmen auf keinen Fall verändern?“ antworten 34% der Teilnehmer aus Softwareentwickler-Unternehmen mit „Mehr Kosten“, 33% mit „Mehr Zeit“, 20% mit „Mehr Personal“ und 13% mit „Sonstiges“. Unter Sonstiges geben die Teilnehmer u. a. „Mehr Komplexität“, „weniger Tests“, „Alle Punkte sind gleich relevant.“, „darf sich verändern, solange die andern Bereiche mit ausgleichen“ und „Abweichung von Anforderungen, Projektzielen, Qualität“ an (siehe Abbildung 63).

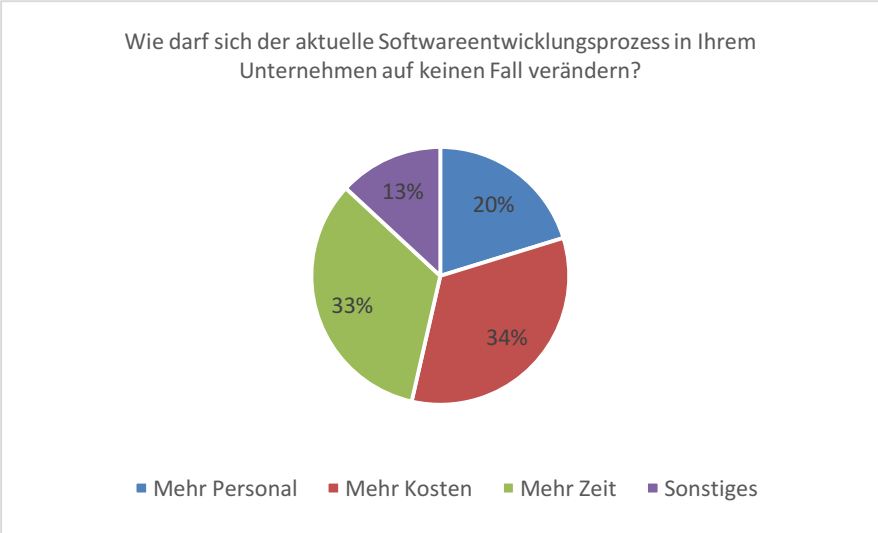

Abbildung 63: Faktoren, die sich laut der Befragten aus Softwareentwickler-Unternehmen nicht im Softwareentwicklungsprozess verändern dürfen

2.4.3 Kleine und mittlere Unternehmen

Bei 45% der Befragten, die eine berufliche Tätigkeit in einem Softwareanwender-KMU ausüben, finden Sicherheitsguidelines oder Sicherheitschecklisten im Unternehmen Anwendung, bei 55% hingegen nicht.

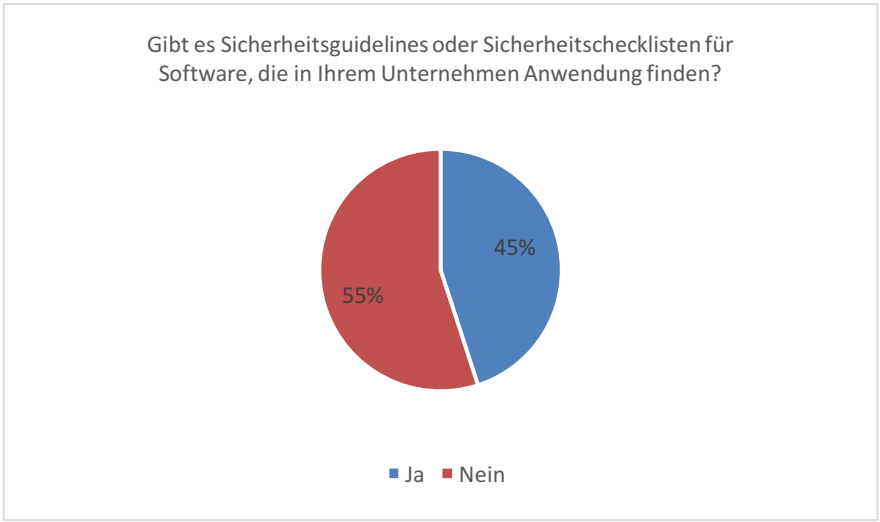

Abbildung 64: Anwendung von Sicherheitsguidelines oder Sicherheitschecklisten laut den Befragten aus Softwareanwender-KMU

33% der Befragten aus Softwareanwender-Unternehmen, in denen Sicherheitsguidelines oder Sicherheitschecklisten Anwendung finden, geben an, dass sie regulatorische Rahmenbedingungen, Zertifizierungen oder Ähnliches berücksichtigen müssen. 33% müssen diese nicht beachten. 33% wollen oder können diese Frage nicht beantworten (siehe Abbildung 65).

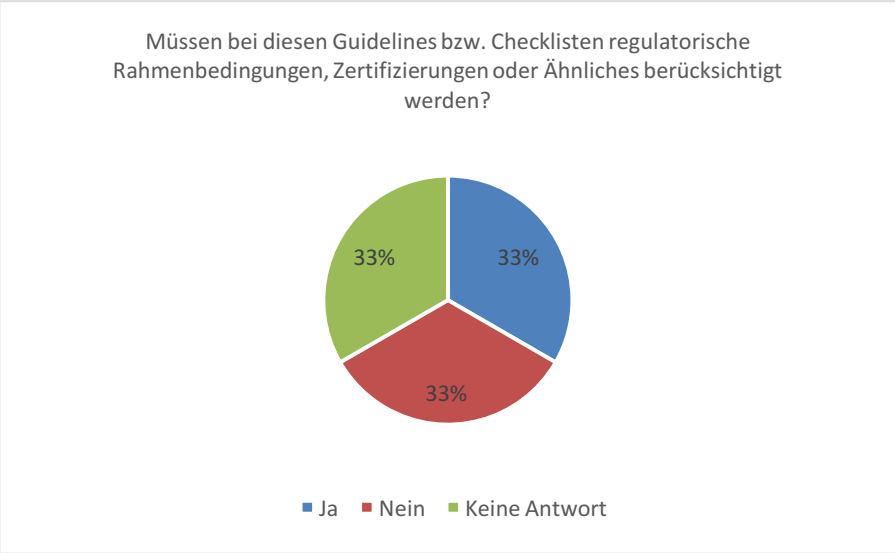

Abbildung 65: Berücksichtigung von regulatorischen Rahmenbedingungen, Zertifizierungen oder Ähnliches laut den Befragten aus Softwareanwender-KMU

42% der Befragten aus Softwareentwickler-KMU geben an, dass in ihren Unternehmen Usability-Engineering ein ganzheitlicher integraler Bestandteil im Softwareentwicklungsprozess ist. 40% geben an, dass Usability-Engineering punktuell integriert ist. Bei 11% wird Usability-Engineering am Ende durchgeführt. Bei 7% findet kein Usability-Engineering statt (siehe Abbildung 66). Folglich geben 93% der Teilnehmer aus Softwareentwickler-KMU an, dass Usability-Engineering Bestandteil des Softwareentwicklungsprozesses ist.

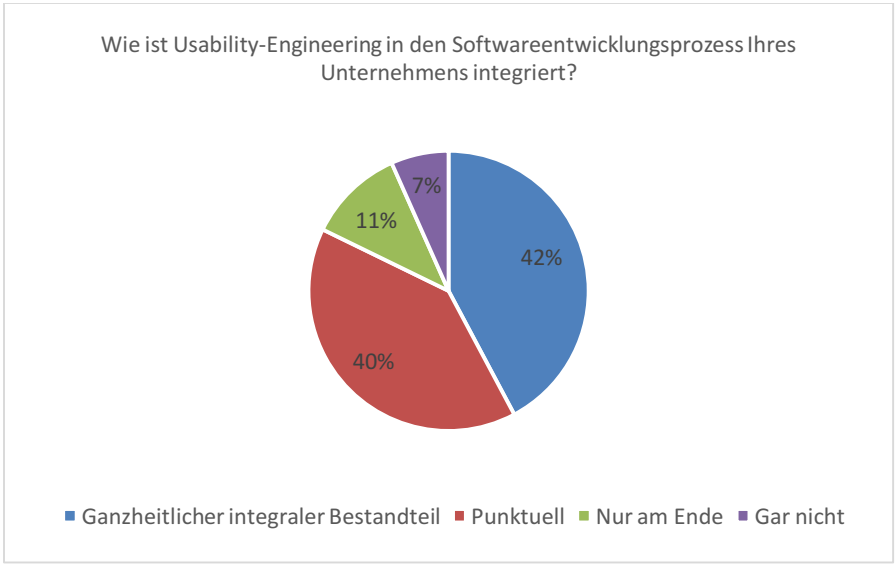

Abbildung 66: Integrationsgrad von Usability-Engineering im Softwareentwicklungsprozess laut den Befragten aus Softwareentwickler-KMU

Bei 27% der Befragten aus Softwareentwickler-KMU ist im Unternehmen Security-Engineering ein ganzheitlicher integraler Bestandteil im Softwareentwicklungsprozess. 51%

geben an, dass Security-Engineering punktuell im Softwareentwicklungsprozess integriert ist. Bei 7% findet Security-Engineering nur am Ende statt. Bei 7% wird kein Security-Engineering durchgeführt (siehe Abbildung 67). Somit geben 93% der Teilnehmer aus Softwareentwickler-KMU an, dass Usability-Engineering in ihrem Unternehmen Bestandteil des Softwareentwicklungsprozesses ist.

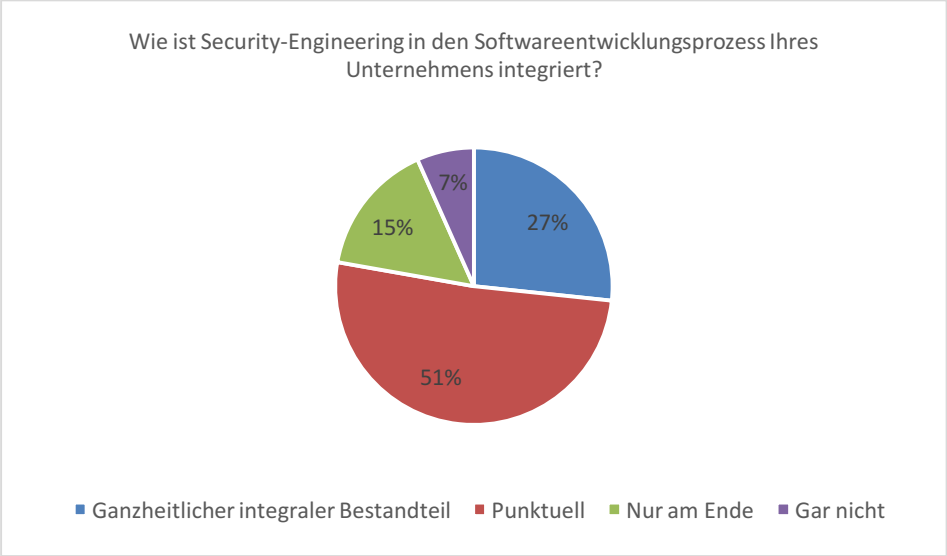

Abbildung 67: Integrationsgrad von Security-Engineering im Softwareentwicklungsprozess laut den Befragten aus Softwareentwickler-KMU

Als adäquate Methoden und Werkzeuge im Usability-Engineering und Security-Engineering werden bei den Befragten aus Softwareentwickler-KMU am häufigsten (Nennungen ab 35%) Vorgehensmodelle, Patterns, Guidelines, Checklisten und Tools angesehen (siehe Abbildung 68).

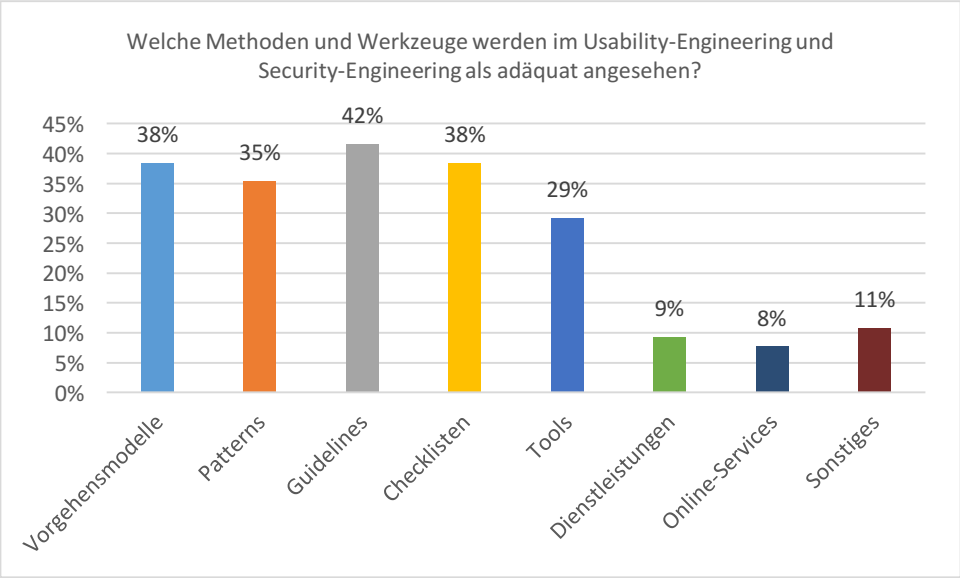

Abbildung 68: Adäquate Methoden und Werkzeuge im Usability-Engineering und Security-Engineering laut den Befragten aus Softwareentwickler-KMU

Für 31% der Teilnehmer, die in einem Softwareentwickler-KMU angestellt sind, darf sich der Softwareentwicklerprozess auf keinen Fall durch mehr Kosten verändern. 27% geben an, dass der Softwareentwicklungsprozess nicht mehr Zeitaufwand benötigen darf. Für 24% darf für den Softwareentwicklungsprozess nicht mehr Personal notwendig sein. 18% geben Sonstiges an (siehe Abbildung 69).

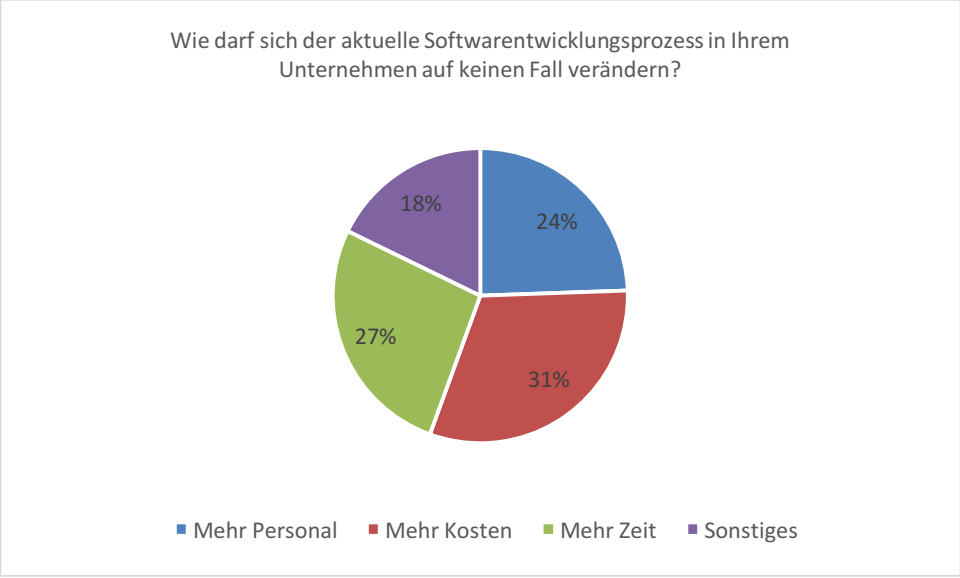

Abbildung 69: Gründe der Befragten aus Softwareentwickler-KMU, die sich nicht im Softwareentwicklungsprozess verändern dürfen

2.4.4 Großunternehmen

Bei 50% der Befragten, die einer beruflichen Tätigkeit in einem Softwareanwender-GU nachgehen, finden im Unternehmen Sicherheitsguidelines oder Sicherheitschecklisten Anwendung. Bei den anderen 50% finden weder Sicherheitsguidelines noch Sicherheitschecklisten Anwendung (siehe Abbildung 70).

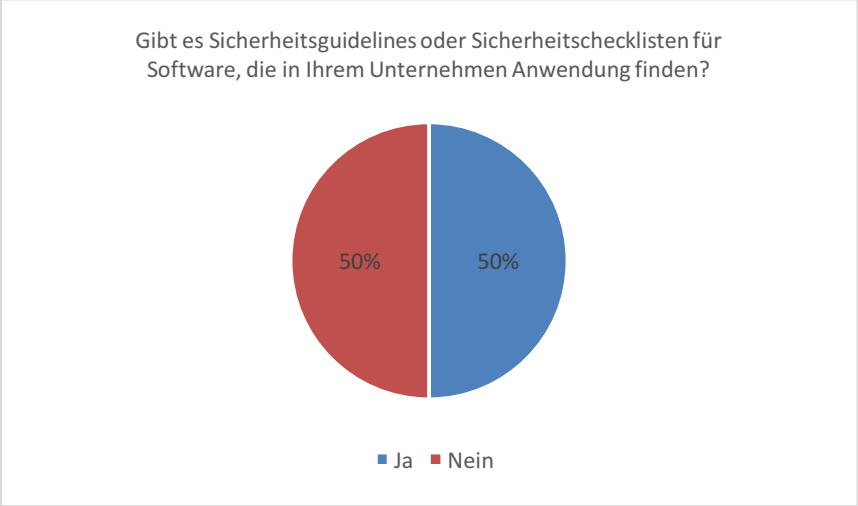

Abbildung 70: Anwendung von Sicherheitsguidelines oder Sicherheitschecklisten laut den Befragten aus Softwareanwender-GU

57% der Teilnehmer aus Softwareanwender-GU, in denen Sicherheitsguidelines oder Sicherheitschecklisten Anwendung finden, geben an, dass regulatorische Rahmenbedingungen, Zertifizierungen oder Ähnliches berücksichtigt werden müssen. 29% müssen diese nicht beachten. 14% können oder wollen diese Frage nicht beantworten (siehe Abbildung 71).

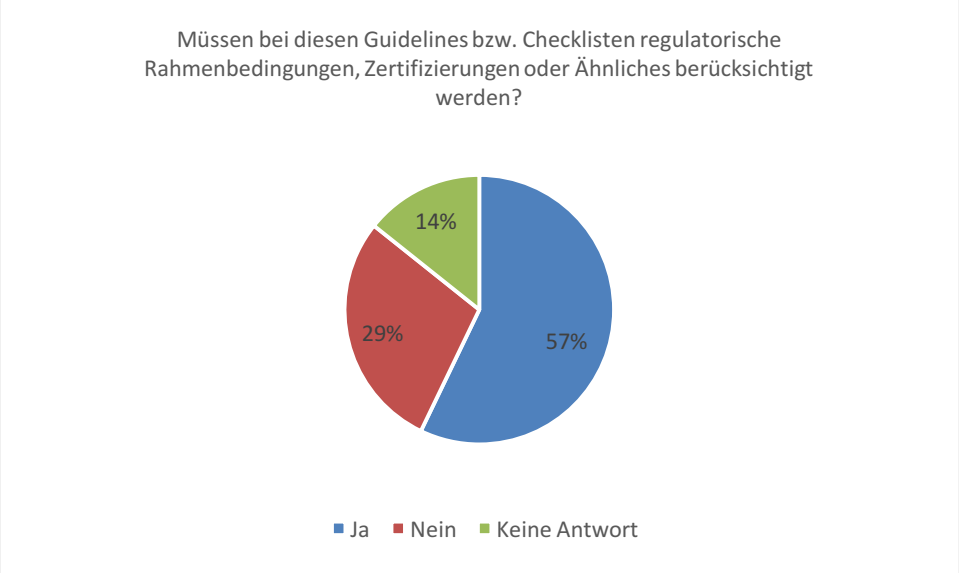

Abbildung 71: Berücksichtigung von regulatorischen Rahmenbedingungen, Zertifizierungen oder Ähnliches laut den Befragten aus Softwareanwender-GU

49% der Teilnehmer aus Softwareentwickler-GU geben an, dass Usability-Engineering punktuell im Softwareentwicklungsprozess integriert ist. Bei 38% ist Usability-Engineering ein ganzheitlicher Bestandteil des Softwareentwicklungsprozesses. Bei 8% wird Usability-Engineering nur am Ende durchgeführt. Bei 5% findet kein Usability-Engineering statt. Somit geben 95% der Befragten aus Softwareentwickler-GU an, dass Usability-Engineering in ihrem Unternehmen Bestandteil des Softwareentwicklungsprozesses ist (siehe Abbildung 72).

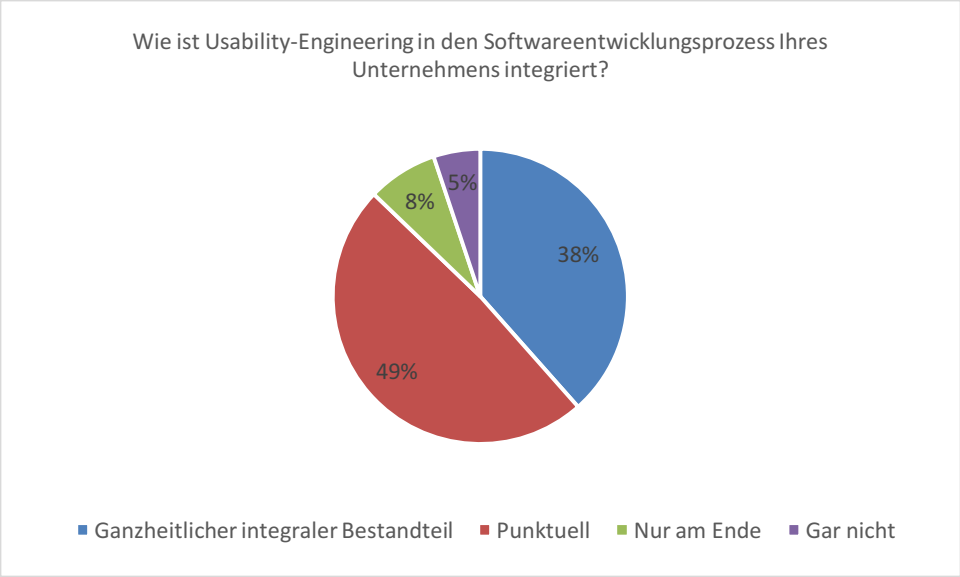

Abbildung 72: Integrationsgrad von Usability-Engineering im Softwareentwicklungsprozess laut den Befragten aus Softwareentwickler-GU

Security-Engineering ist bei 51% aller Teilnehmer aus Softwareentwickler-GU ein ganzheitlicher integraler Bestandteil des Softwareentwicklungsprozesses. Bei 46% wird Security-Engineering punktuell in den Softwareentwicklungsprozess integriert. 3% geben an, dass kein Security-Engineering durchgeführt wird. Bei keinem der Teilnehmer findet Security-Engineering am Ende des Softwareentwicklungsprozesses statt (siehe Abbildung 73). Folglich geben 97% der Teilnehmer aus Softwareentwickler-GU an, dass Security-Engineering in ihrem Unternehmen Bestandteil des Softwareentwicklungsprozesses ist.

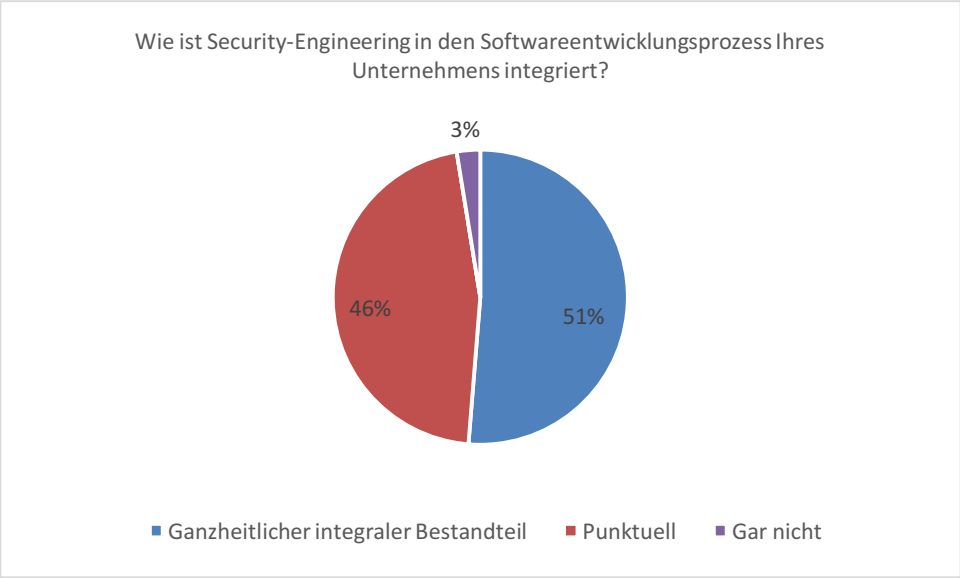

Abbildung 73: Integrationsgrad von Security-Engineering im Softwareentwicklungsprozess laut den Befragten aus Softwareentwickler-GU

Die am häufigsten genannten adäquaten Methoden und Werkzeuge im Usability- und Security-Engineering sind laut den Befragten aus Softwareentwickler-GU (Nennungen ab 35%) Vorgehensmodelle, Patterns, Guidelines, Checklisten und Tools (siehe Abbildung 74).

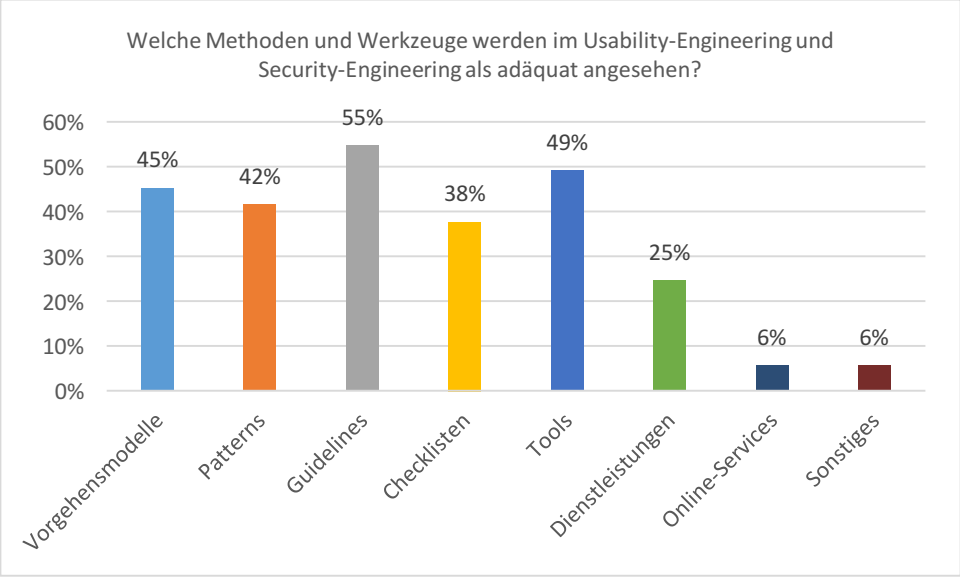

Abbildung 74: Adäquate Methoden und Werkzeuge im Usability- und Security-Engineering laut den Befragten aus Softwareentwickler-GU

Laut 41% der Befragten aus Softwareentwickler-GU darf sich der aktuelle Softwareentwicklungsprozess auf keinen Fall durch einen höheren Zeitaufwand verändern. Bei 36% darf er nicht mehr Kosten verursachen. Für 15% darf für den aktuellen Softwareentwicklungsprozess nicht mehr Personal benötigt werden. 8% geben Sonstiges an.

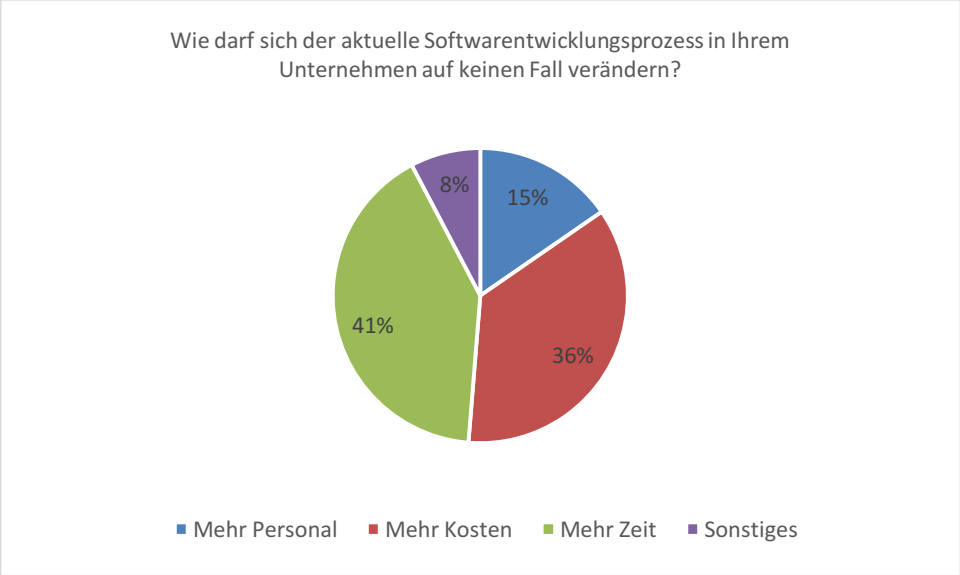

Abbildung 75: Faktoren der Befragten aus Softwareentwickler-GU, die sich nicht im Softwareentwicklungsprozess dürfen

2.5 Investitionsbereitschaft in Usability und IT-Sicherheit

Laut 45% der Befragten besteht die Bereitschaft im Unternehmen eigenes Personal für die Qualitätsthemen Usability und IT-Security zu schulen. Bei 21% besteht nur die Bereitschaft Personal in IT-Security zu schulen. 5% geben an, dass ihr Unternehmen nur bereit ist ihr Personal in Usability zu schulen. Bei 29% der Unternehmen besteht keine Bereitschaft Personal in Usability oder IT-Security zu schulen (siehe Abbildung 76). Daraus lässt sich erkennen, dass laut 71% der Befragten die Unternehmen bereit sind ihr Personal in Usability und/oder IT-Security zu schulen.

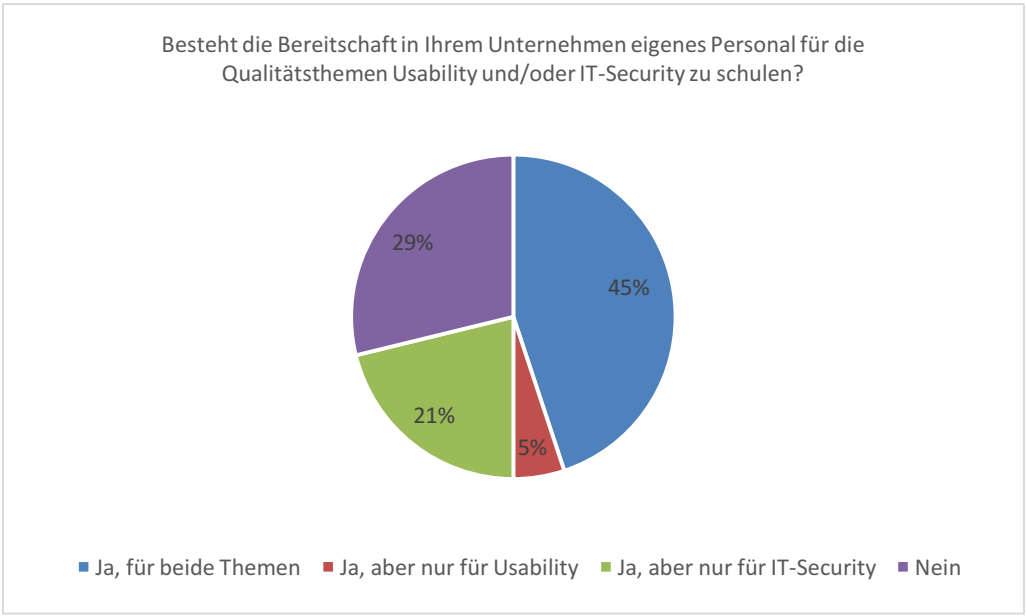

Abbildung 76: Investitionsbereitschaft in Schulung von eigenen Personal für Usability und/oder IT-Security laut den Befragten

Bei 26% der Teilnehmer, deren Unternehmen bereit sind Personal in Usability und/oder IT-Security zu schulen, räumen die jeweiligen Unternehmen bis zu 5 Tage pro Jahr für die Schulungen ein. 23% geben einen Tag an, 22% geben 2 Tage an, 21% geben mehr als fünf Tage an und 8% geben 3 Tage an (siehe Abbildung 77). Folglich geben 77% der Befragten an, dass ihr Unternehmen bereit ist Personal in Usability und/oder IT-Security zu schulen und dafür mindestens zwei Tage pro Jahr für die Schulung investiert.

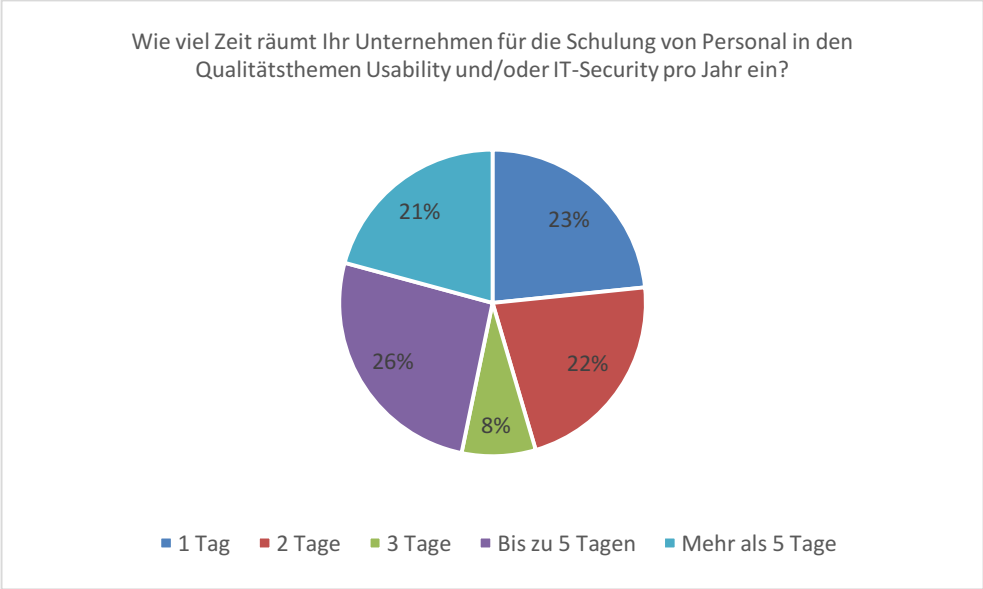

Abbildung 77: Investitionszeit in Schulungen für Usability und/oder IT-Security pro Jahr laut den Befragten

Bei 54% der Befragten besteht die Bereitschaft in ihrem Unternehmen spezialisierte Werkzeuge für die Qualitätsthemen Usability und IT-Security einzusetzen. Bei 19% der Befragten besteht die Bereitschaft in ihrem Unternehmen spezialisierte Werkzeuge nur für IT-Security einzusetzen. Bei 3% sind die Unternehmen bereit spezialisierte Werkzeuge nur für Usability einzusetzen. 24% der Teilnehmer geben an, dass ihr Unternehmen nicht bereit ist, spezialisierte Werkzeuge für Usability oder IT-Security einzusetzen (siehe Abbildung 78). Demnach besteht bei 76% der Befragten die Bereitschaft in ihrem Unternehmen spezialisierte Werkzeuge für Usability und/oder IT-Security zu verwenden.

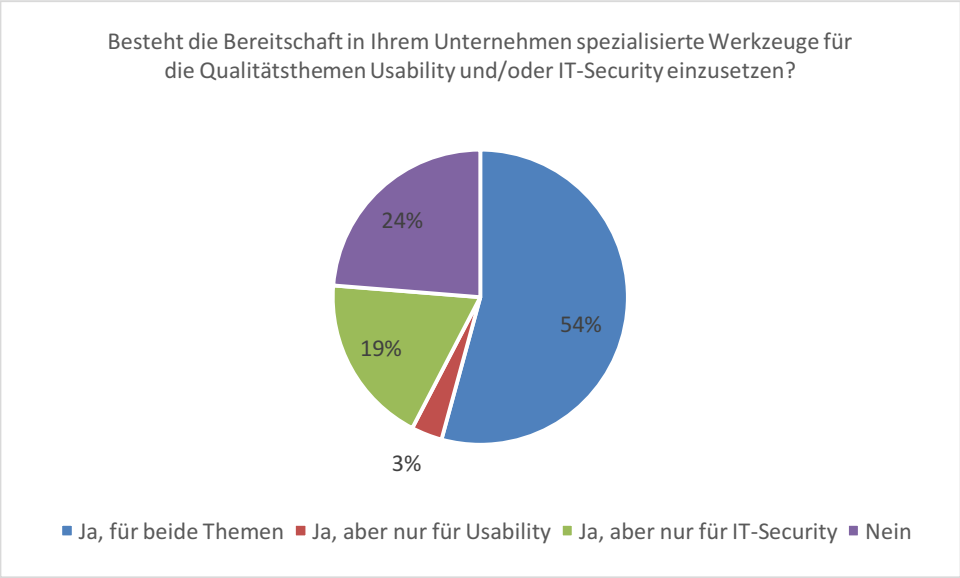

Abbildung 78: Investitionsbereitschaft in spezialisierte Werkzeuge für Usability und/oder IT-Security laut den Befragten

33% der befragten Teilnehmer geben an, dass in ihrem Unternehmen die Bereitschaft besteht unabhängige Dienstleistungen für die Softwarequalitätsmerkmale Usability und/oder IT-Security einzusetzen. Bei 18% der Befragten besteht die Bereitschaft in Ihrem Unternehmen unabhängige Dienstleistungen nur für IT-Security einzusetzen. 3% geben nur die Bereitschaft für Usability an. Bei 46% besteht keine Bereitschaft in Ihrem Unternehmen unabhängige Dienstleistungen für Usability oder IT-Security einzusetzen (siehe Abbildung 79). Folglich geben 54% der Befragten an, dass ihr Unternehmen bereit ist unabhängige Dienstleistungen für Usability und/oder IT-Security zu verwenden.

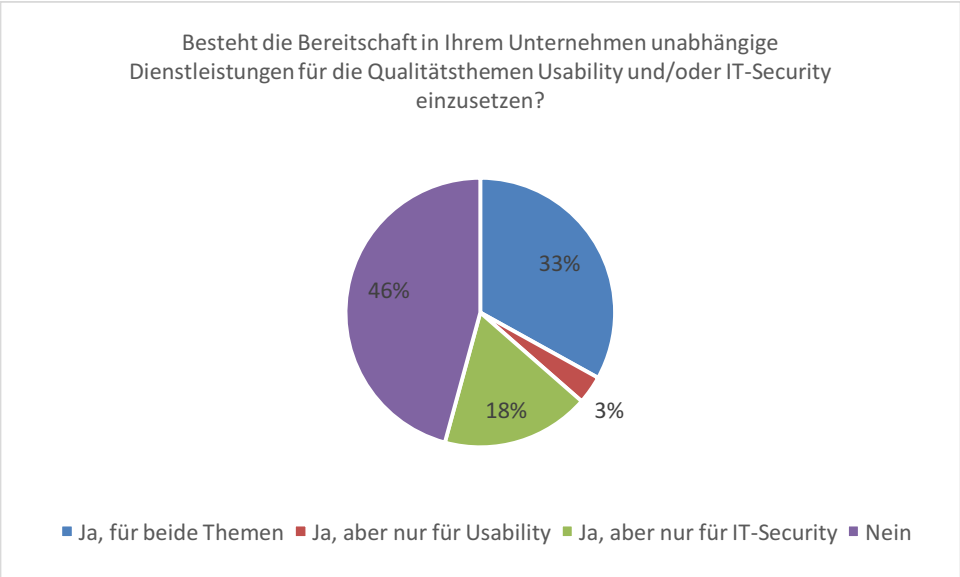

Abbildung 79: Investitionsbereitschaft in unabhängige Dienstleistungen für die Usability und/oder IT-Security laut den Befragten

In dieser Fragegruppe wurde zudem noch erfragt, wie viel Prozent des Umsatzes die Unternehmen der Befragten in Schulungen, spezialisierte Werkzeuge und unabhängige Dienstleistungen für Usability und/oder IT-Sicherheit investieren. Wegen mangelnder Antworten und dadurch fehlender Repräsentativität wurden die Ergebnisse dieser Fragen nicht in der Auswertung berücksichtigt.

2.5.1 Softwareanwender-Unternehmen

Bei 24% der Teilnehmer, die bei einem Softwareanwender-Unternehmen beschäftigt sind, besteht die Bereitschaft in ihrem Unternehmen eigenes Personal für die beiden Qualitätsthemen Usability und IT-Security zu schulen. 29% geben an, dass ihr Unternehmen bereit ist ihr Personal nur für IT-Security zu schulen. Bei 6% sind die Unternehmen bereit ihr Personal nur für Usability zu schulen. 41% geben an, dass bei ihrem Unternehmen nicht die Bereitschaft besteht ihr Personal in Usability oder IT-Security zu schulen (siehe Abbildung 80). Somit besteht die Bereitschaft bei 59% der Befragten, die in einem Softwareanwender-Unternehmen angestellt sind, in ihrem Unternehmen eigenes Personal in Usability und/oder IT-Security zu schulen.

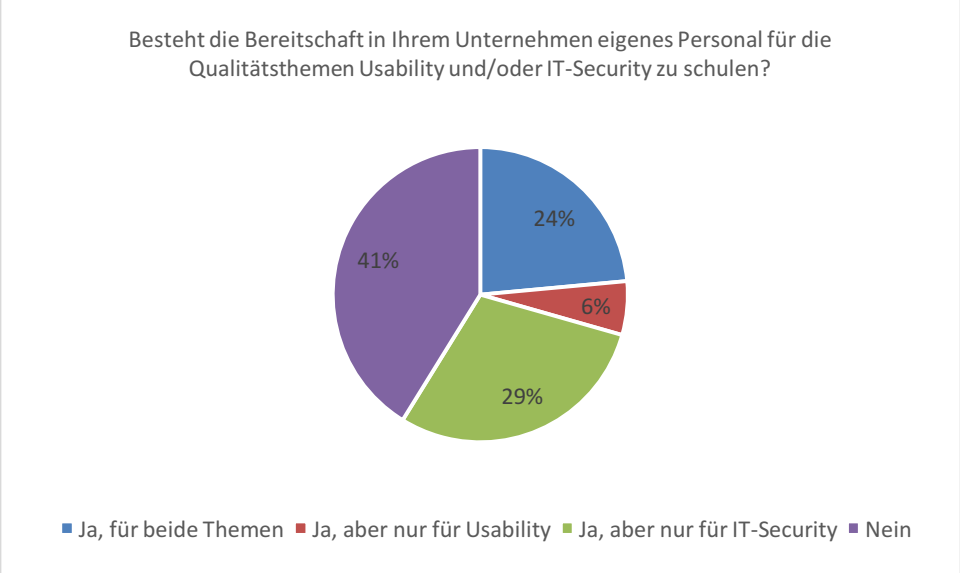

Abbildung 80: Investitionsbereitschaft in Schulung von eignen Personal für Usability und/oder IT-Security laut den Befragten aus Softwareanwender-Unternehmen

54% der Befragten aus Softwareanwender-Unternehmen geben an, dass ihr Unternehmen 1 Tag pro Jahr für die Schulung von Usability und/oder IT-Security einräumt. 23% geben zwei Tage an, 15% mehr als 5 Tage und 8% 2 Tage. Keiner der Befragten gab 3 Tage an (siehe Abbildung 81). Folglich geben 46% der Teilnehmer, die in einem Softwareanwender-Unternehmen beschäftigt sind, an, dass ihr Unternehmen bereit ist mindestens 2 Tage pro Jahr für Schulung von Personal zu den Themen Usability und/oder IT-Security einzuräumen.

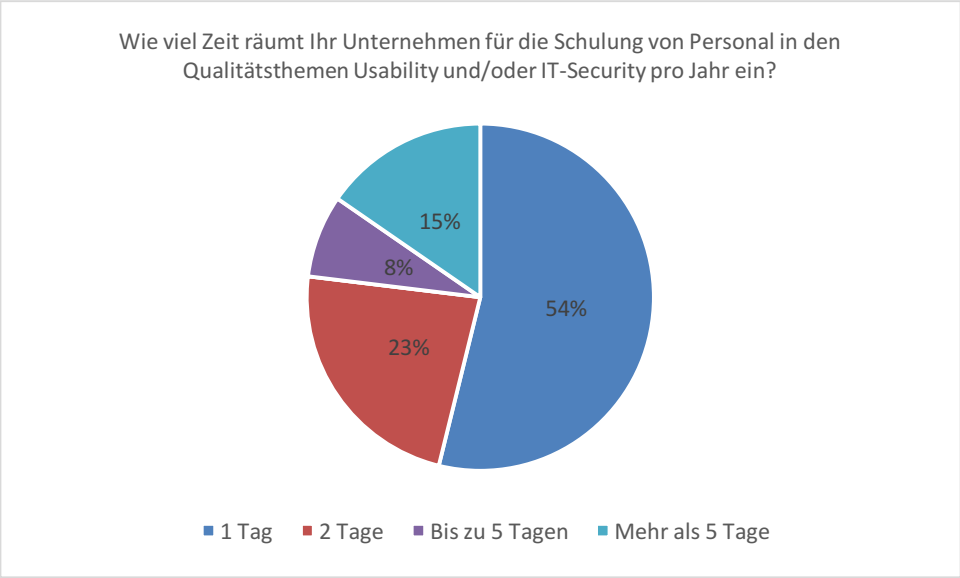

Abbildung 81: Investitionszeit in Schulungen für Usability und/oder IT-Security pro Jahr laut den Befragten aus Softwareanwender-Unternehmen

Laut 21% der befragten Teilnehmer, die in einem Softwareanwender-Unternehmen beschäftigt sind, besteht in ihrem Unternehmen die Bereitschaft spezialisierte Werkzeuge für die beiden Qualitätsthemen Usability und IT-Security einzusetzen. 32% geben an, dass Ihr Unternehmen bereit ist, spezialisierte Werkzeuge nur für IT-Security anzugeben. Bei 3% der Unternehmen besteht die Bereitschaft spezialisierte Werkzeuge nur für Usability einzusetzen. Demnach geben 56% der Teilnehmer, die in einem Softwareanwender-Unternehmen einer Tätigkeit nachgehen, an, dass Ihr Unternehmen bereit ist spezialisierte Werkzeuge für die Qualitätsthemen Usability und/oder IT-Security einzusetzen.

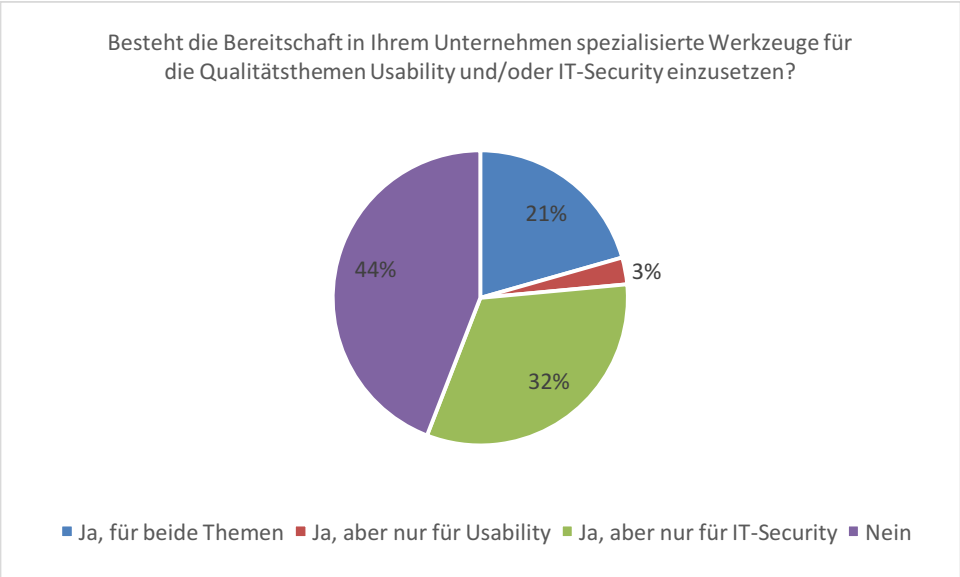

Abbildung 82: Investitionsbereitschaft in spezialisierte Werkzeuge für Usability und/oder IT-Security laut den Befragten Softwareanwender-Unternehmen

27% der Teilnehmer aus Softwareanwender-Unternehmen geben an, dass bei ihrem Unternehmen die Bereitschaft besteht unabhängige Dienstleistungen für die beiden Qualitätsthemen Usability und IT-Security einzusetzen. Bei 32% sind die Unternehmen bereit unabhängige Dienstleistungen nur für IT-Security zu verwenden. Keines der Unternehmen ist bereit unabhängige Dienstleistungen nur für Usability einzusetzen. Bei 41% besteht in den Unternehmen keine Bereitschaft unabhängige Dienstleistungen für Usability oder IT-Security zu verwenden (siehe Abbildung 83). Daraus kann entnommen werden, dass bei 59% der Befragten, die in einem Softwareanwender-Unternehmen angestellt sind, die jeweiligen Unternehmen bereit sind unabhängige Dienstleistungen entweder für Usability und IT-Security oder nur IT-Security einzusetzen.

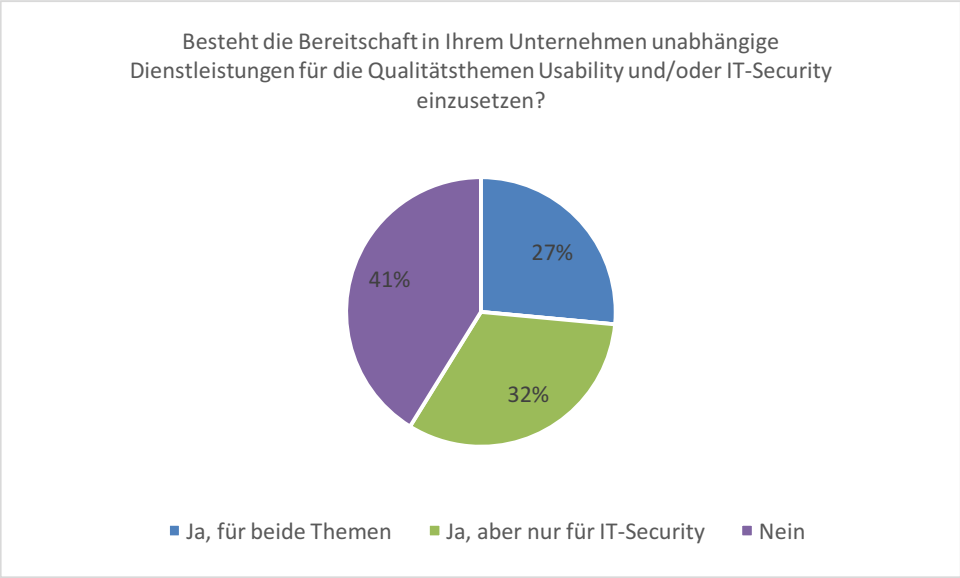

Abbildung 83: Investitionsbereitschaft in unabhängige Dienstleistungen für Usability und/oder IT-Security laut den Befragten aus Softwareanwender-Unternehmen

2.5.2 Softwareentwickler-Unternehmen

53% der Befragten aus Softwareentwickler-Unternehmen geben an, dass ihr Unternehmen bereit ist ihr eigenes Personal für die beiden Qualitätsthemen Usability und IT-Security zu schulen. Bei 18% der Unternehmen besteht nur die Bereitschaft eigenes Personal für IT-Security zu schulen. 5% geben an, dass ihr Unternehmen nur bereit ist eigenes Personal in Usability zu schulen. Bei 24% sind die Unternehmen nicht bereit ihr eignes Personal in Usability oder IT-Security zu schulen (siehe Abbildung 84). Folglich besteht bei 76% der Befragten, die in einem Softwareentwickler-Unternehmen beschäftigt sind, in ihrem Unternehmen die Bereitschaft ihr eigenes Personal in Usability und/oder IT-Security zu schulen.

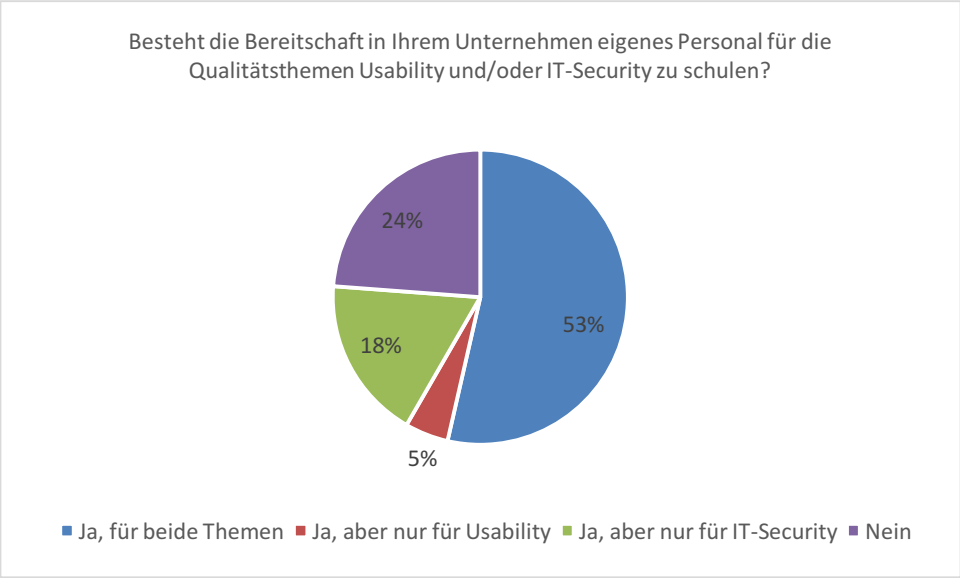

Abbildung 84: Investitionsbereitschaft in Schulungen von eigenem Personal in Usability und/oder IT-Security laut den Befragten aus Softwareentwickler-Unternehmen

30% der Befragten, die ihre berufliche Tätigkeit in einem Softwareentwickler-Unternehmen ausüben, geben an, dass ihr Unternehmen bis zu 5 Tage pro Jahr für Schulungen von Personal in Usability und/oder IT-Security einräumt. Jeweils 22% geben 2 Tage und mehr als 5 Tage an, 17% einen Tag und 9% 3 Tage (siehe Abbildung 85). Damit kann festgestellt werden, dass bei 83% der Befragten aus Softwareentwickler-Unternehmen die jeweiligen Unternehmen bereit sind mindestens 2 Tage pro Jahr für Schulungen von Personal in Usability und/oder IT-Security einzuräumen.

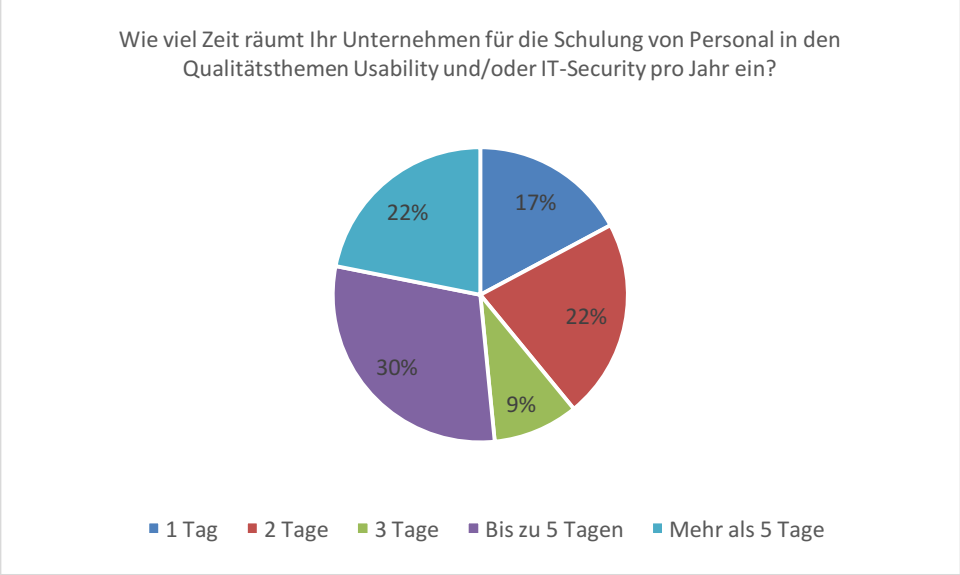

Abbildung 85: Investitionszeit in Schulungen in Usability und/oder IT-Security laut den Befragten aus Softwareentwickler-Unternehmen

68% der Teilnehmer aus Softwareentwickler-Unternehmen geben an, dass ihr Unternehmen bereit ist spezialisierte Werkzeuge für beide Qualitätsthemen Usability und IT-Security einzusetzen. Bei 13% der Unternehmen besteht die Bereitschaft spezialisierte Werkzeuge nur für IT-Security einzusetzen. 4% geben an, das ihr Unternehmen nur bereit ist spezialisierte Werkzeuge für Usability zu verwenden (siehe Abbildung 86). Somit besteht bei 85% der befragten Teilnehmer, die in einem Softwareentwickler-Unternehmen einer Tätigkeit nachgehen, in ihrem Unternehmen die Bereitschaft spezialisierte Werkzeuge für Usability und/oder IT-Security einzusetzen.

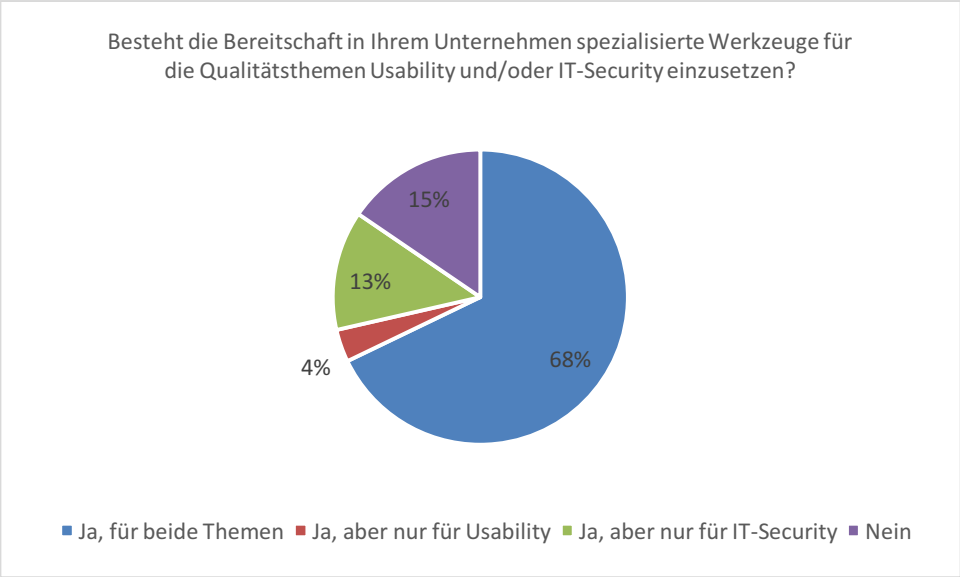

Abbildung 86: Investitionsbereitschaft in spezialisierte Werkzeuge für Usability und/oder IT-Security laut den Befragten aus Softwareentwickler-Unternehmen

36% der Befragten, die eine berufliche Tätigkeit in einem Softwareentwickler-Unternehmen ausüben, geben an, dass ihr Unternehmen bereit ist unabhängige Dienstleistungen für die beiden Qualitätsthemen Usability und IT-Security einzusetzen. Bei 12% besteht in ihrem Unternehmen die Bereitschaft unabhängige Dienstleistungen nur für IT-Security auszugeben. 5% der Teilenehmer geben an, dass ihr Unternehmen bereit ist nur für Usability unabhängige Dienstleistungen zu beauftragen. Demzufolge besteht bei 53% der Befragten, die in einem Softwareentwickler-Unternehmen tätig sind, in ihrem Unternehmen die Bereitschaft unabhängige Dienstleistungen für Usability und/oder IT-Security einzusetzen.

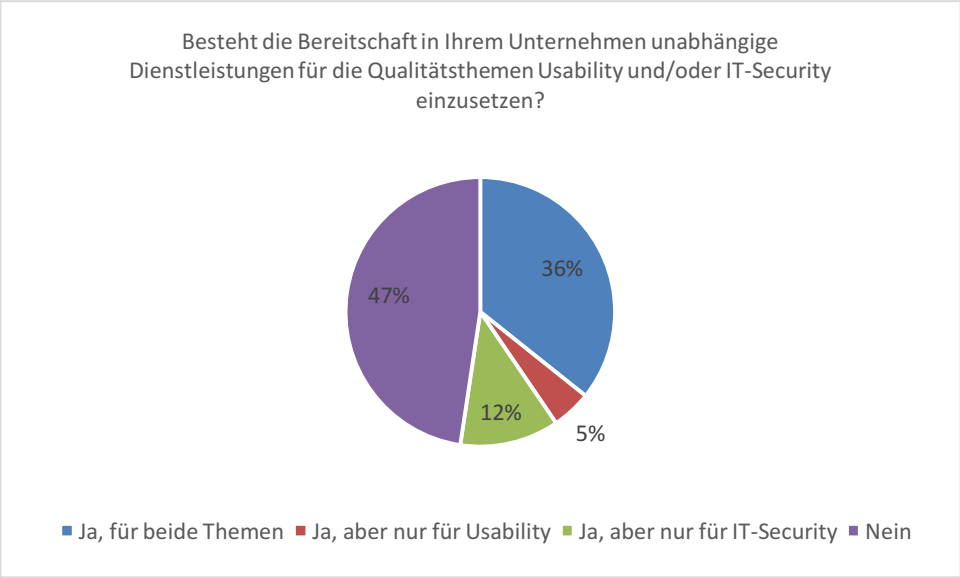

Abbildung 87: Investitionsbereitschaft in unabhängige Dienstleistungen für Usability und/oder IT-Security laut den Befragten aus Softwareentwickler-Unternehmen

2.5.3 Kleine und mittlere Unternehmen

Bei 41% der Befragten aus KMU besteht in ihrem Unternehmen die Bereitschaft ihr eigenes Personal für die beiden Qualitätsthemen Usability und IT-Security zu schulen. 22% geben an, dass ihr Unternehmen bereit ist ihr Personal nur in IT-Security zu schulen, 5% nur in Usability. 32% der Unternehmen sind weder bereit ihr Personal in Usability noch in IT-Security zu schulen (siehe Abbildung 88). Daraus lässt sich erschließen, dass 68% der Befragten angeben, dass ihr KMU bereit ist Personal in Usability und/oder IT-Security zu schulen.

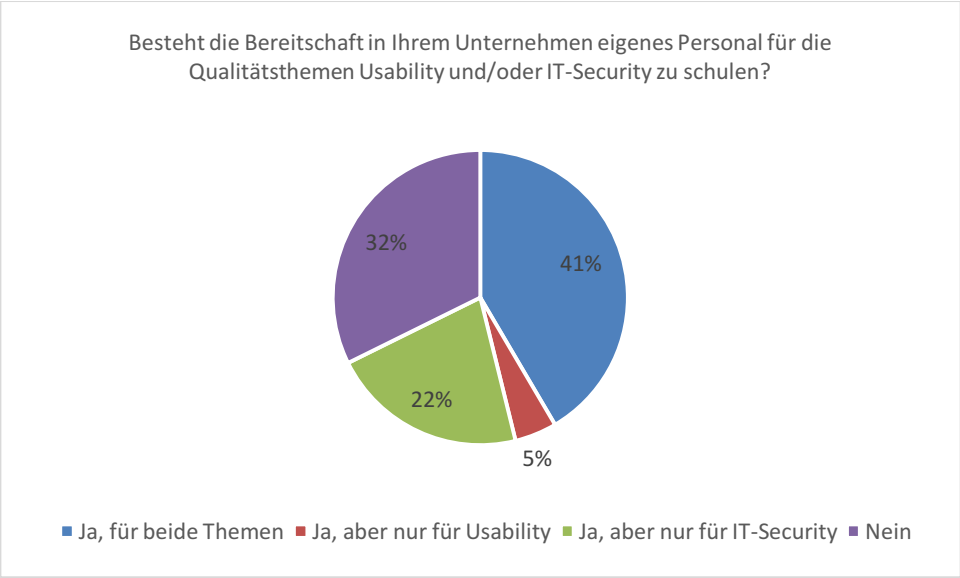

Abbildung 88: Investitionsbereitschaft in Schulungen vom eigenem Personal in Usability und/oder IT-Security laut den Befragten aus KMU

26% der Befragten aus KMU, die bereit sind ihr eigenes Personal in Usability und/oder IT-Security zu schulen, geben an, dass ihr Unternehmen bis zu 5 Tagen pro Jahr für die Schulung von Personal in Usability und/oder IT-Security einräumt. 22% geben 1 Tag an, jeweils 21% mehr als 5 Tage oder 2 Tage, 10% geben 3 Tage an. Folglich geben 78% an, dass ihr Unternehmen bereit ist mindestens 2 Tage pro Jahr für Schulungen in Usability und/oder IT-Security einzuräumen.

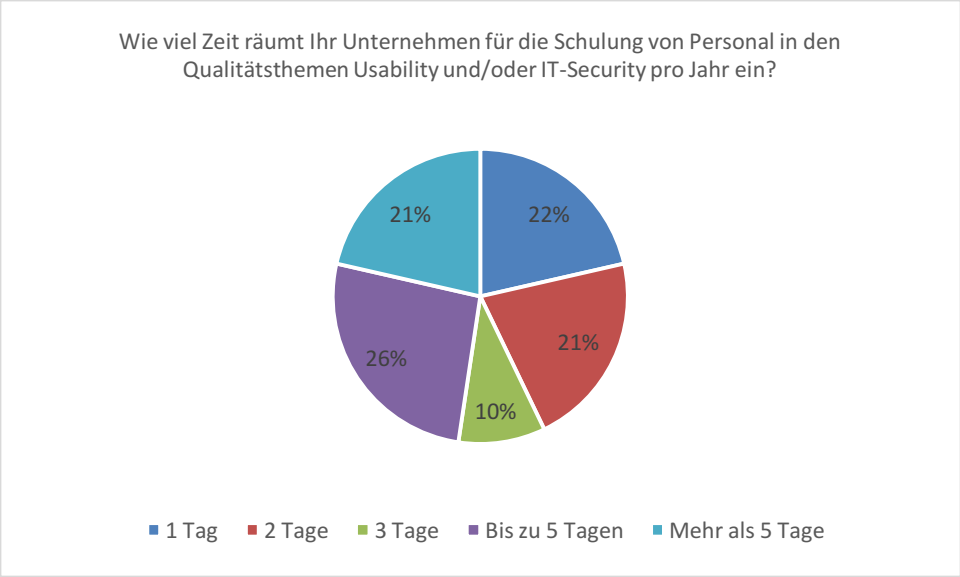

Abbildung 89: Investitionszeit in Schulungen von Personal in Usability und/oder IT-Security laut den Befragten aus KMU

51% der Befragten, die einer beruflichen Tätigkeit in einem KMU nachgehen, geben an, dass ihr Unternehmen bereit ist spezialisierte Werkzeuge für beide Qualitätsthemen Usability und IT-Security einzusetzen. 18% geben an, dass in ihrem Unternehmen nur die Bereitschaft besteht spezialisierte Werkzeuge für IT-Security einzusetzen, 3% bestätigen die Bereitschaft nur für Usability. 28% geben an, dass ihr Unternehmen bereit ist weder spezialisierte Werkzeuge für Usability noch für IT-Security einzusetzen. Folglich geben 72% der Befragten, die in einem KMU angestellt sind, an, dass bei ihrem Unternehmen die Bereitschaft besteht spezialisierte Werkzeuge für Usability und/oder IT-Security einzusetzen.

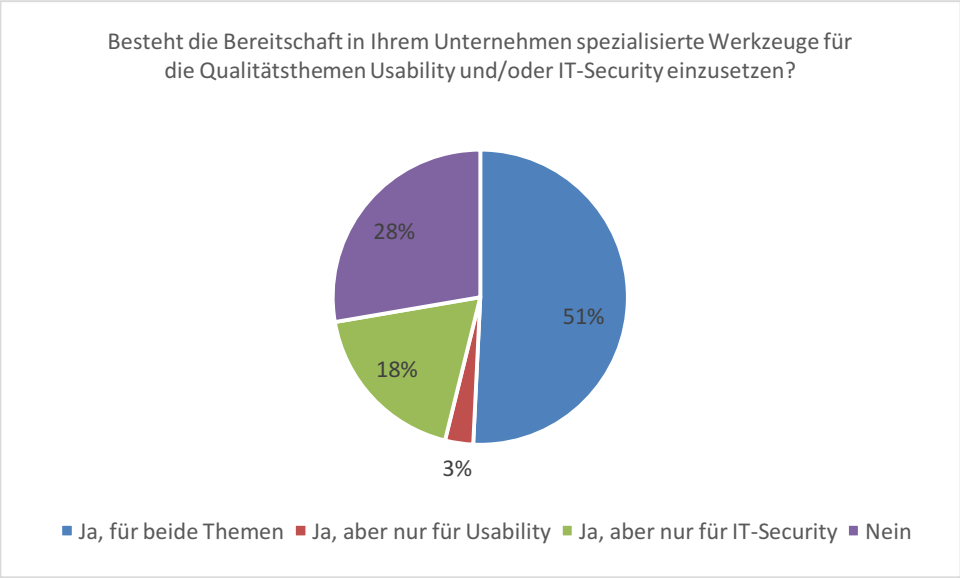

Abbildung 90: Investitionsbereitschaft in spezialisierte Werkzeuge für Usability und/oder IT-Security laut der Befragten aus KMU

28% der Teilnehmer aus KMU geben an, dass ihr Unternehmen bereit ist für beide Qualitätsthemen Usability und IT-Security unabhängige Dienstleistungen einzusetzen. 20% geben an, dass bei ihrem Unternehmen die Bereitschaft besteht nur für IT-Security unabhängige Dienstleistungen zu verwenden. Bei 3% sind die Unternehmen nur bereit für Usability unabhängige Dienstleistungen einzusetzen. 41% geben an, dass bei ihrem Unternehmen weder die Bereitschaft besteht unabhängige Dienstleistungen für Usability noch für IT-Security zu verwenden (siehe Abbildung 91). Folglich sind 51% der Unternehmen bereit unabhängige Dienstleistungen für Usability und/oder IT-Security einzusetzen.

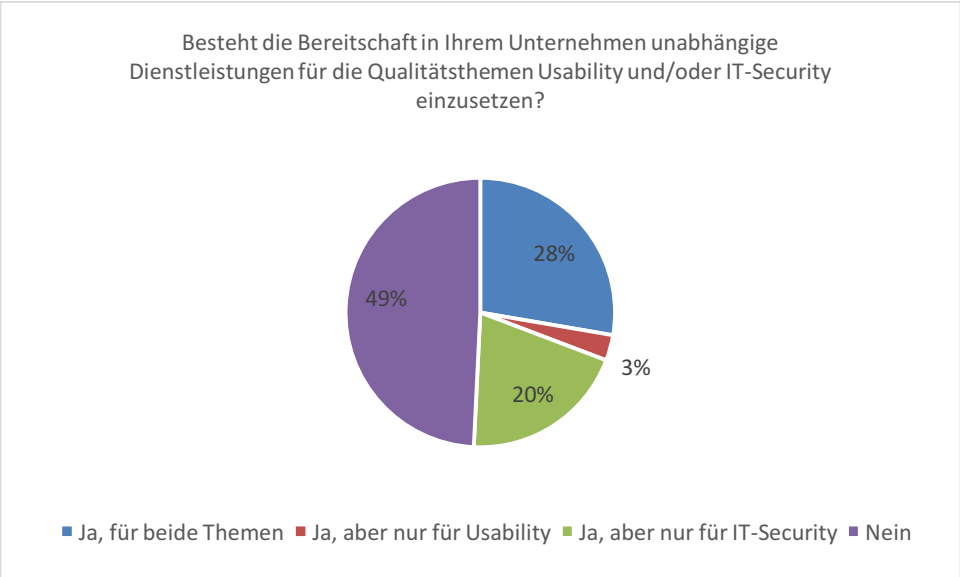

Abbildung 91: Investitionsbereitschaft in unabhängige Dienstleistungen für Usability und/oder IT-Security laut den Befragten aus KMU

2.5.4 Großunternehmen

49% der Befragten aus GU geben an, dass ihr Unternehmen bereit ist eigenes Personal in beiden Qualitätsthemen Usability und IT-Security zu schulen. Bei 21% besteht in den jeweiligen Unternehmen die Bereitschaft eigenes Personal nur in IT-Security zu schulen. 6% geben an, dass ihr Unternehmen bereit ist ihr eigenes Personal nur in Usability zu schulen. Bei 24% sind die Unternehmen weder bereit ihr eigenes Personal in Usability noch in IT-Security zu schulen (siehe Abbildung 92). Folglich geben 76% der Befragten, die in einem GU angestellt sind, an, dass ihr Unternehmen bereit ist ihr eigenes Personal in Usability und/oder IT-Security zu schulen.

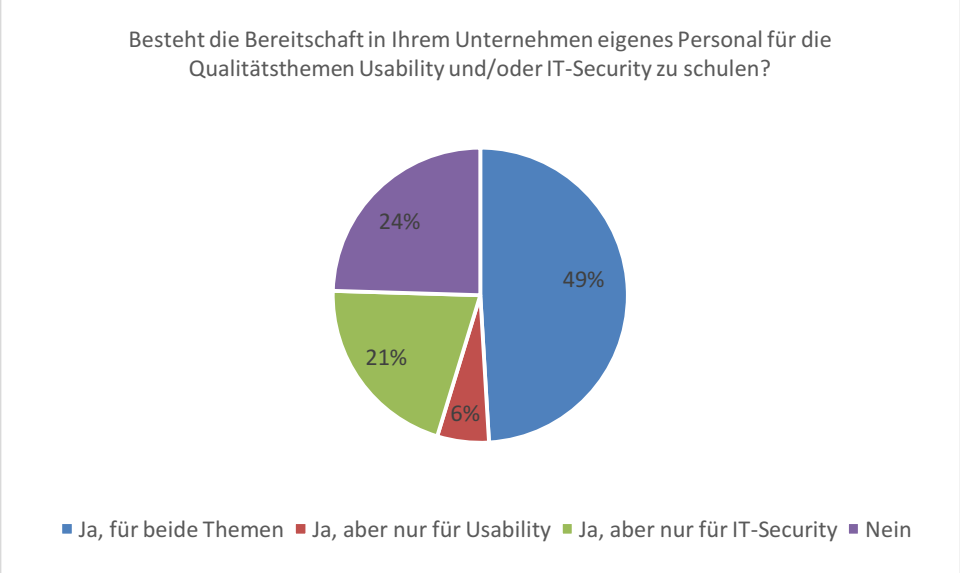

Abbildung 92: Investitionsbereitschaft in Schulungen vom eigenem Personal in Usability und/oder IT-Security laut den Befragten aus GU

Jeweils 26% der Befragten aus GU, die bereit sind ihr eigenes Personal in Usability und/oder IT-Security zu schulen, geben an, dass ihr Unternehmen 1 Tag bzw. bis zu 5 Tage pro Jahr für Schulungen von Personal in Usability und/oder IT-Security einräumt. Bei 23% räumen die Unternehmen 2 Tage pro Jahr ein, bei 20% mehr als 5 Tage, bei 5% 3 Tage (siehe Abbildung 93). Folglich geben 74% der Befragten, die eine berufliche Tätigkeit in einem GU ausüben, an, dass ihr Unternehmen mindestens 2 Tage pro Jahr für die Schulung von Personal in Usability und/oder IT-Security einräumt.

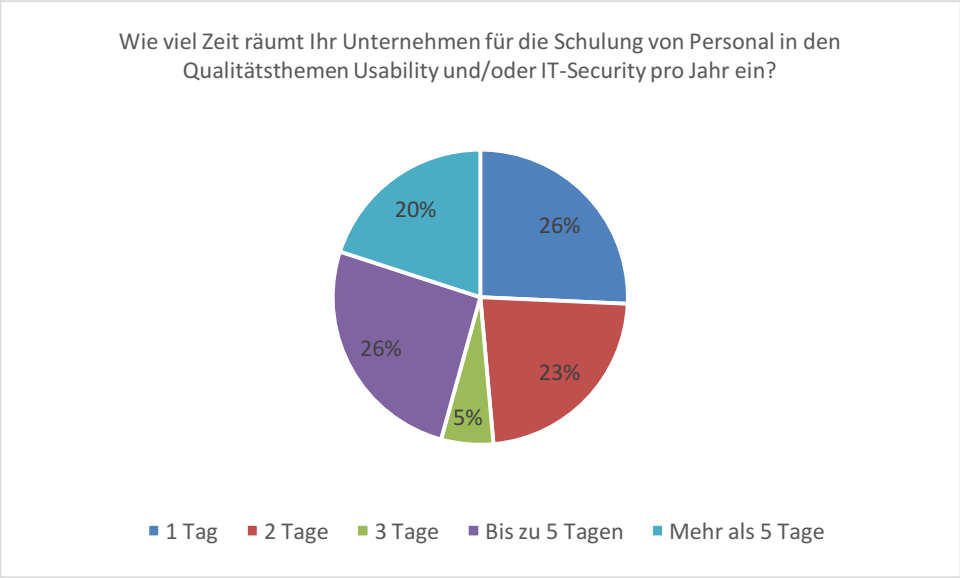

Abbildung 93: Investitionszeit in Schulungen von Personal in Usability und/oder IT-Security laut den Befragten aus GU

Bei 58% der Befragten aus GU besteht bei ihrem Unternehmen die Bereitschaft spezialisierte Werkzeuge für beide Qualitätsthemen Usability und IT-Security einzusetzen. Bei 19% sind die Unternehmen bereit nur spezialisierte Werkzeuge für IT-Security zu verwenden. Bei 4% besteht bei den Unternehmen die Bereitschaft spezialisierte Werkzeuge nur für Usability einzusetzen. 19% geben an, dass ihr Unternehmen weder bereit ist spezialisierte Werkzeuge für Usability noch für IT-Security einzusetzen (siehe Abbildung 94). Folglich geben 81% der Befragten, die in einem GU angestellt sind, an, dass ihr Unternehmen bereit ist spezialisierte Werkzeuge für Usability und/oder IT-Security einzusetzen.

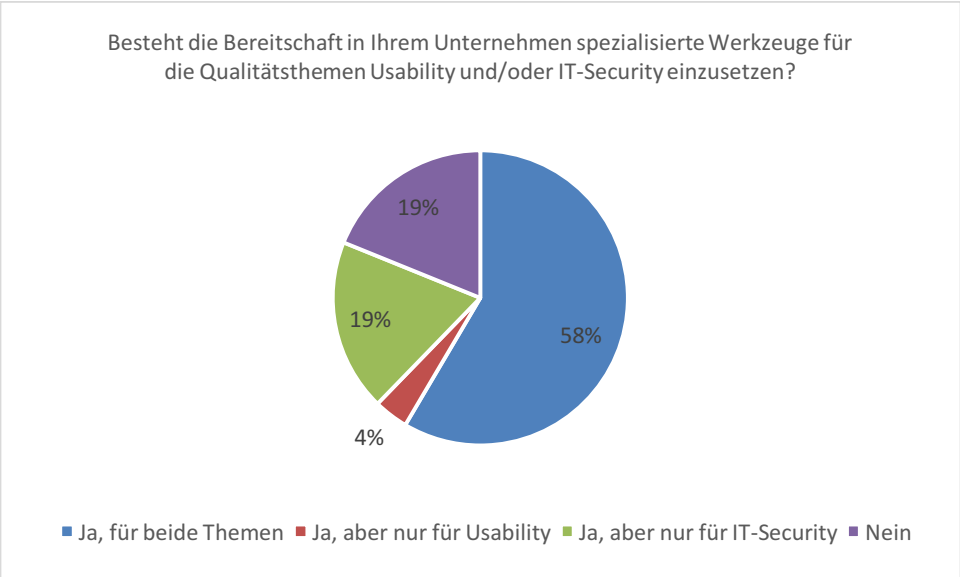

Abbildung 94: Investitionsbereitschaft in spezialisierte Werkzeuge für Usability und/oder IT-Security laut der Befragten aus GU

40% der Befragten, die in einem GU beschäftigt sind, geben an, dass ihr Unternehmen bereit ist unabhängige Dienstleistungen für beide Qualitätsthemen Usability und IT-Security einzusetzen. Bei 15% sind die Unternehmen bereit unabhängige Dienstleistungen nur für IT-Security einzusetzen. Bei 4% besteht bei den Unternehmen die Bereitschaft unabhängige Dienstleistungen nur für Usability zu verwenden (siehe Abbildung 95). Folglich geben 59% der Befragten, die eine berufliche Tätigkeit in einem GU ausüben, an, dass ihr Unternehmen bereit ist unabhängige Dienstleistungen für Usability und/oder IT-Security einzusetzen.

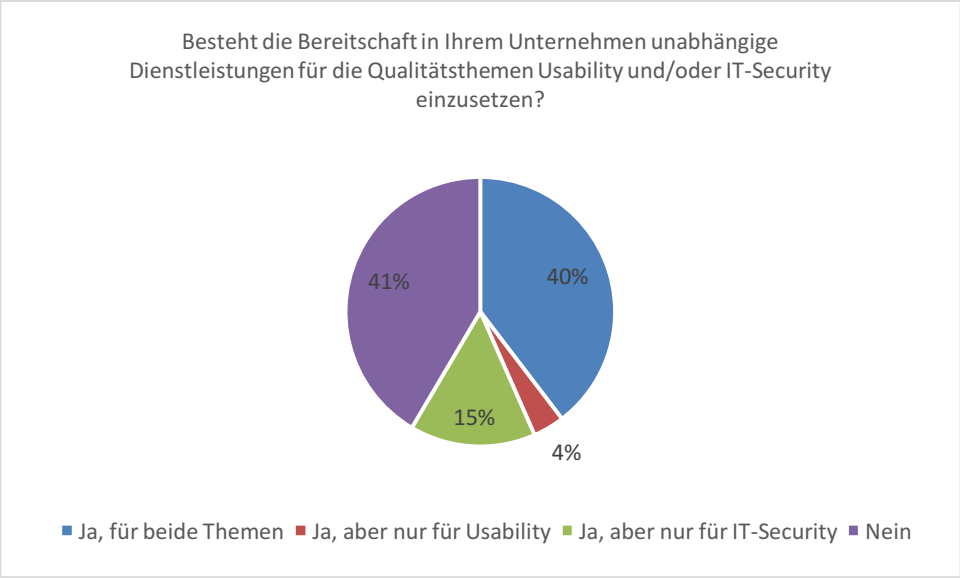

Abbildung 95: Investitionsbereitschaft in unabhängige Dienstleistungen für Usability und/oder IT-Security laut den Befragten aus GU

3 Fazit

Ein Großteil der Befragten ist in der Lage die Qualitätseigenschaften hinter den Begriffen Usability und IT-Sicherheit zu verstehen und zu definieren. Somit kann gesagt werden, dass Usability und IT-Sicherheit sowohl bei den Befragten aus Softwareanwender- als auch Softwareentwickler-Unternehmen und aus KMU sowie GU bekannte Qualitätsmerkmale sind.

Ebenfalls kann festgestellt werden, dass mindestens 85% der Befragten aus den jeweiligen Unternehmensgruppen die Relevanz von Usability und IT-Sicherheit hoch oder sogar sehr hoch einschätzen. Daraus lässt sich ableiten, dass Usability und IT-Sicherheit auch als wesentliche Qualitätsmerkmale in Software-Produkten wahrgenommen werden.

Der hohe Stellenwert von Usability und IT-Sicherheit kann nochmals untermauert werden, da 94% bzw. 95% der Befragten aus Softwareentwickler-Unternehmen angeben, dass Usability-Engineering bzw. Security-Engineering Bestandteil des Softwareentwicklungsprozesses ist. Hierbei gibt es zwischen Softwareentwickler-KMU und Softwareentwickler-GU keine großen Unterschiede.

Obwohl ein Großteil der Befragten sowohl Usability als auch IT-Sicherheit als zwei wesentliche Qualitätsmerkmale in Software-Produkten erachten und Usability- sowie Security-Engineering Bestandteil vieler Softwareentwickler-Unternehmen sind, sind beide Qualitätsmerkmale bei der Mehrheit der Teilnehmer aus Softwareanwender-Unternehmen

nicht das erste oder zweite Auswahlkriterium für Software. Für 74% steht die Funktionalität im Vordergrund. Nur bei 5% ist Usability bzw. Sicherheit das erste Auswahlkriterium. Bei Softwareanwender-KMU ist die Auswahl von Usability und Sicherheit als erstes Kriterium ähnlich niedrig. Bei Softwareanwender-GU liegt die Auswahl sogar bei 0%. Auch als zweites Auswahlkriterium stimmten nur 26% aller Befragten für Usability und 21% für Sicherheit. Bei den Befragten aus Softwareanwender-KMU stimmten 35% für Usability und 25% für Sicherheit als zweites Kriterium. Nur 14% der Teilnehmer aus Softwareanwender-GU wählten jeweils Usability und Sicherheit als zweites Auswahlkriterium.

Auch eine hohe Investitionsbereitschaft in Usability und IT-Sicherheit kann anhand der Ergebnissen der Online-Studie festgestellt werden. 71% der Befragten geben an, dass ihr Unternehmen bereit ist ihr Personal in Usability und/oder IT-Sicherheit zu schulen, 45% sogar für beide Qualitätsthemen. 77% davon geben an, dass in ihrem Unternehmen die Bereitschaft besteht mindestens 2 Tage pro Jahr für Schulungen in diesen Bereichen einzuräumen. Bei den Befragten aus Softwareentwickler-Unternehmen, Softwareentwickler-KMU und Softwareentwickler-GU sind die Prozentsätze ähnlich. Bei den Teilnehmern aus Softwareanwender-KMU liegt der Prozentsatz etwas niedriger. Hier geben nur 59% an, dass ihr Unternehmen bereit ist für Schulungen in Usability und/oder IT-Sicherheit zu investieren. Von diesen 59% besteht nur bei 46% die Bereitschaft mindestens 2 Tage pro Jahr für Schulungen in Usability und IT-Sicherheit einzuräumen.

Des Weiteren besteht auch eine hohe Investitionsbereitschaft in spezialisierte Werkzeuge für Usability und IT-Sicherheit. 76% aller Befragten geben an, dass ihr Unternehmen bereit ist spezialisierte Werkzeuge für Usability und/oder IT-Security einzusetzen, 54% sogar für beide Qualitätsthemen. Bei den Befragten aus Softwareentwickler-Unternehmen bzw. Softwareentwickler-GU sind es sogar 85% bzw. 81%. Bei den Teilnehmern aus KMU liegt der Prozentsatz bei 72%. Auch hier liegt der Prozentsatz mit 56% bei den Befragten aus Softwareanwender-Unternehmen niedriger als bei den anderen Unternehmensgruppen. Als adäquate Methoden und Werkzeuge bei Softwareentwickler-Unternehmen werden hier am häufigsten Vorgehensmodelle, Patterns, Guidelines, Checklisten und Tools angesehen. Dienstleistungen und Online-Services werden allerdings als weniger adäquat angesehen. Dies ist sowohl bei Softwareentwickler-KMU und Softwareentwickler-GU ähnlich.

Die Feststellung, dass Dienstleistungen und Online-Services als weniger adäquate Werkzeuge und Methoden betrachten werden, kann möglicherweise mit der Fragestellung nach der Investitionsbereitschaft in unabhängige Dienstleistungen in Verbindung gebracht werden. Hier geben nur um die 50% der Befragten an, dass ihr Unternehmen bereit ist solche Dienste einzusetzen.

Nichtsdestotrotz kann festgehalten werden, dass bei dem Großteil der Befragten eine Investitionsbereitschaft in spezialisierte Werkzeuge, Schulungen und unabhängige Dienstleistungen für Usability und IT-Sicherheit besteht. Die hohe Investitionsbereitschaft in spezialisierte Werkzeuge und Schulungen gehen mit den Zielen das USecureD-Projekts einher, da es beabsichtigt grundlegende Methoden, Musterlösungen und Werkzeuge zu entwickeln und zu evaluieren, um Unternehmen – insbesondere KMU – die Implementierung von sicherer und zugleich benutzerfreundlicher Software zu vereinfachen. Die Erhebung, dass Vorgehensmodelle, Patterns, Guidelines, Checklisten und Tools am häufigsten als adäquate Werkzeuge und Methoden empfunden werden, sowie die Feststellung, dass Usability- und Security-Engineering bei 90% Bestandteil des Softwareentwicklungsprozesses

ihres Unternehmens ist, entspricht den Anforderungen der zu entwickelnden USecureD-Plattform. In dieser Plattform werden Patterns, Principles, Guidelines, Metriken und Best Practices in einer zentralen Umgebung gebündelt, um mittelständischen Softwareentwickler-Unternehmen eine günstige Möglichkeit anzubieten, diese Methoden und Werkzeuge in den Usability- sowie Security-Engineering-Prozess zu integrieren oder beide Prozesse sogar zu verzahnen. Für mittelständische Softwareanwender-Unternehmen dient die USecureD-Plattform als Anlaufpunkt, ihre Softwareprodukte fundiert und umfangreich nach dem Qualitätsmerkmal Usable Security zu evaluieren.

Zudem kann aus den Ergebnissen der Online-Studie entnommen werden, dass in vielen Bereichen Bedarf an gebrauchstauglichen Sicherheitsmechanismen existiert. Hierbei stachen insbesondere die Bereiche E-Mail-Sicherheit und Mobile Security heraus. Der Handlungsbedarf in vielen Bereichen ist vor allem damit zu kennzeichnen, dass 65% der Teilnehmer bis zu 1 Stunde pro Tag für Sicherheitsmechanismen aufwenden müssen, 4% sogar bis zu 2 Stunden. Der letztere Prozentsatz ist bei den Teilnehmern aus Softwareanwender-Unternehmen sogar noch höher. Hier benötigen 9% bis zu Stunden pro Tag für Verwendung von Sicherheitsmechanismen.

Diesen Aufwand zu minimieren gehört ebenfalls zu den Zielen von USecureD, indem die entwickelten Werkzeuge des Projekts dazu beitragen Geschäftsprozesse effizienter, effektiver, zufriedenstellend und zugleich sicherer zu gestalten.

Die meist gewählten Anforderungen, um gebrauchstaugliche Sicherheitsmechanismen zu gestalten sind laut den Befragten Transparenz (65%), Nachvollziehbarkeit (75%) und einfache Anwendbarkeit (83%). Nur ungefähr ein Drittel der Teilnehmer (35%) fordert, dass gebrauchstaugliche Sicherheitseigenschaften im Verborgenen gestaltet werden sollen. Diese Anforderungen sind unter den Teilnehmern aus Softwareanwender-, Softwareentwickler-Unternehmen, KMU und GU ähnlich.

Aus den Ergebnissen der Online-Studie sind neue wissenschaftliche Erkenntnisse über das Verständnis, die Bedürfnisse, die Anforderungen und die Investitionsbereitschaft von Usability, IT-Sicherheit und Usable Security gewonnen worden. Dennoch gab es einige Aspekte, die nicht erschlossen werden können. Zu diesen gehören das Verständnis und die Relevanz von Usable Security. In der Studie wurde nur nach dem Verständnis und der Relevanz von Usability und IT-Sicherheit gefragt. Außerdem kann nicht festgestellt werden, wie belastend sich spezifische Sicherheitskomponenten auf die tägliche Arbeit bzw. das Nutzerverhalten auswirken. In der Online-Studie wurde lediglich nach dem Belastungsgrad von Sicherheitsmechanismen allgemein gefragt. Des Weiteren wurden bei der Frage nach den Auswahlkriterien für Software nur Teilnehmer aus Softwareanwender-Unternehmen befragt. Da Softwareentwickler-Unternehmen auch Software-Produkte verwenden, hätte diese Frage auch allen Befragten gestellt werden können. Ein weiterer Aspekt, der nicht untersucht werden kann, ist, warum die Befragten aus Softwareanwender-Unternehmen Usability oder Sicherheit nicht als erstes oder zweites Auswahlkriterium für Software-Produkte erachten. Zudem kann nicht erörtert werden, warum eine geringere Bereitschaft für den Einsatz unabhängiger Dienstleistungen besteht als für die Verwendung von Schulungen und spezialisierte Software für Usability und/oder IT-Sicherheit. In diesem Zusammenhang fehlt auch eine Untersuchung, warum die Befragten aus Softwareentwickler-Unternehmen Online-Services und Dienstleistungen als weniger adäquat ansehen als Vorgehensmodelle, Patterns, Guidelines, Checklisten oder Tools.

Diese fehlenden Erkenntnisse gilt es in einer weiteren Studie zu untersuchen, um die Anforderungen, Bedürfnisse und das Verständnis über Usable Security noch genauer evaluieren zu können.

4 Quellen

[DIN EN ISO 9241-11:1999-01] DIN Deutsches Institut für Normung e. V. (1999): Ergonomische Anforderungen für Bürotätigkeiten mit Bildschirmgeräten - Teil 11: Anforderungen an die Gebrauchstauglichkeit; Leitsätze (ISO 9241-11:1998); Deutsche Fassung EN ISO 9241-11:1998

[EU-Kommission 2003] Kommission der Europäischen Gemeinschaften (2003): Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, Aktenzeichen K(2003) 1422, Amtsblatt der Europäischen Union. Verfügbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32003H0361&from=EN

[Sorge et al. 2013] Christoph Sorge, Nils Gruschka und Luigi Lo Iacono (2013): „Sicherheit in Kommunikationsnetzen“, Oldenbourg Verlag.