IT-Sicherheit im Handwerk

Studie

Stand der IT-Sicherheit im Handwerk

Gefördert durch:

Bundesministerium
für Wirtschaft
und Technologie

aufgrund eines Beschlusses
des Deutschen Bundestages

TASK FORCE
IT-SICHERHEIT IN DER WIRTSCHAFT
Mehrwert und Schutz für Rechner.

Impressum

Autorin: Karen Bartelt

Master of Arts und
wissenschaftliche Mitarbeiterin am
Heinz-Piest-Institut für Handwerkstechnik
an der Leibniz Universität Hannover.

ISBN: 978-3-944916-00-2
1.Auflage

Herausgeber: Projekt „IT-Sicherheit im Handwerk“

Bearbeitung: Heinz-Piest-Institut für Handwerkstechnik
an der Leibniz Universität Hannover
Wilhelm-Busch-Str.18
30167 Hannover

Verlag: Handwerkskammer Rheinhessen,
Verlagsnummer: 978-3-944916
Kompetenzzentrum für IT-Sicherheit
und qualifizierte digitale Signatur
Dagobertstr.2, 55116 Mainz
Tel.: +49 (0) 6131/999261
E-Mail: j.schueler@hwk.de

Titelgestaltung: aviate Werbeagentur

Itb- Institut für Technik der Betriebsführung im Deutschen Handwerksinstitut e.V.

Heinz-Piest-Institut für Handwerkstechnik an der Leibniz Universität Hannover

Handwerkskammer Rheinhessen, Kompetenzzentrum für IT-Sicherheit und qualifizierte digitale Signatur

if(is) – Institut für Internet-Sicherheit der Westfälischen Hochschule

Inhaltsverzeichnis

Abkürzungsverzeichnis

BMWi	Bundesministerium für Wirtschaft und Technologie
BYOD	Bring your own device
IAO	Fraunhofer Institut für Arbeitswissenschaft und Organisation
IKT	Informations - und Kommunikationstechnologien
IT	Informationstechnik
KMU	Kleine und mittlere Unternehmen
ZDH	Zentralverband des deutschen Handwerks
VoIP	Voice over IP

1. Zusammenfassung

Die Studie „IT-Sicherheitsniveau im Handwerk“ betrachtet den Grad des Risikobewusstseins zu Fragen der Sicherheit von Informationstechnologien unter Betrieben des Handwerks auf Basis einer von November 2012 bis Januar 2013 durchgeführten empirischen Erhebung. Zusätzlich zu einer quantitativen Umfrage unter kleinen und mittleren Unternehmen (KMU) wurden Experteninterviews durchgeführt. In diesen Interviews haben neun Berater der Handwerkskammern ihren Eindruck zur Umsetzung von IT-Sicherheitsmaßnahmen beschrieben und auftretende Sicherheitsdefizite genannt.

Die Studie untersucht, inwieweit das Thema IT-Sicherheit im Handwerk präsent ist und auf welche Weise die verschiedenen Betriebe ihre IT schützen. Durch eine Differenzierung nach Betriebsgrößenklassen kann festgehalten werden, welche Betriebe im besonderen Maße auf fachmännische Beratung angewiesen sind und welche Probleme bezüglich der IT-Sicherheit bestehen. Daraus resultierend kann ein Ranking erstellt werden, an dem sich zukünftige für IT-Sicherheit sensibilisierende Maßnahmen orientieren können.

In den geführten Interviews sind sich die Experten einig, dass der Grad der IT-Sicherheit der Handwerksbetriebe von der jeweiligen Betriebsgröße abhängt. Häufig spielen Unwissenheit und fehlende Professionalität in Bezug auf IT-Sicherheit eine große Rolle. Das liegt zum einen an der kleineren IT-Infrastruktur und zum anderen an der geringeren Relevanz der IT-Sicherheit in kleineren Handwerksbetrieben.
Die Studie zeigt, dass abhängig von der Betriebsgröße IT-sicherheitsrelevante Themen bei größeren Unternehmen eine übergeordnete Rolle spielen. Bezüglich der Datensicherung, sicherer Passwörter und der Zugriffsrechte für Mitarbeiter bestätigt sich die Expertenmeinung, dass diese Betriebe der IT - Sicherheit höhere Priorität einräumen.

Insbesondere Betriebe mit weniger als 50 Mitarbeitern bedürfen daher einer Sensibilisierung. Die Studie zeigt darüber hinaus, dass dem Thema IT-Sicherheit seitens der Handwerksbetriebe insgesamt noch eine zu geringe Bedeutung zugeschrieben wird.

2. Einleitung

Informations- und Kommunikationstechnologien (IKT) haben in den letzten Jahren immer mehr an Bedeutung gewonnen und einen Strukturwandel in allen Teilen der Gesellschaft wie Wirtschaft, Wissenschaft und Politik ausgelöst.
Die weite Verbreitung der Informationstechnologien beeinflusst weitreichende Bereiche der Wirtschaft, woraus sich neue Formen der Geschäftsanbahnung und -abwicklung gebildet haben. Diese Veränderungen sind nicht nur in großen Unternehmen in den letzten Jahren weit vorangeschritten. Auch in den kleinen und mittleren Betrieben (KMU) des Handwerks ist die Informationstechnologie (IT) heute integraler Bestandteil der meisten Unternehmensprozesse und oftmals mit entscheidend für den Unternehmenserfolg. Häufig haben die Verantwortlichen nur die Vorteile und Chancen der neuen Möglichkeiten im Blick und vernachlässigen dabei die potenziellen Gefahren, die mit innovativen Technologien einhergehen können.

Die vom Bundesministerium für Wirtschaft und Technologie in Auftrag gegebene Studie „IT-Sicherheitsniveau in kleinen und mittleren Unternehmen“ aus dem Jahr 2012 hat ergeben, dass noch 24,6% der befragten Handwerksbetriebe der IT-Sicherheit insgesamt eine sehr geringe oder geringe Bedeutung zuweisen. Nur 22% der Befragten sehen ein hohes oder sehr hohes Risikopotenzial in Bezug auf die Informationstechnik (IT). Dies zeigt im Vergleich zu anderen Wirtschaftssektoren, dass die Gefahrenpotentiale im Handwerk noch nicht gänzlich erkannt werden (vgl. Büllingen/Hillbrand 2012, S. 63f.).
Angesichts der vielfältigen und wachsenden Risiken – verursacht durch den wachsenden Einsatz von Smartphones, der inzwischen verbreiteten Nutzung privater Endgeräte im dienstlichen Kontext (Bring your own Device - BYOD) oder der Anbindung von Produktionsmaschinen an das Internet - sowie der steigenden Abhängigkeit vom einwandfreien Funk-

tionieren der eingesetzten Technologien, gewinnt die IT-Sicherheit auch für Handwerksbetriebe zunehmend an Bedeutung.

Die vorliegende Analyse greift bereits gewonnene Erkenntnisse aus anderen Studien auf, erweitert diese durch den gezielten Blick auf den Sektor Handwerk und liefert hierdurch einen aktuellen Überblick über das IT-Sicherheitsniveau in dessen KMU. Die Erkenntnisse werden genutzt, um die typische IT-Infrastruktur in den Betrieben des Handwerks nachzuzeichnen, bestehende IT-Sicherheitslücken zu analysieren und zukünftige Handlungsfelder aufzudecken. Das Ziel der Studie ist die Darstellung des IST-Zustands der bereits erreichten IT-Sicherheit im Handwerk. Anhand der Ergebnisse wird der Handlungsbedarf sich strukturell ähnelnder Betriebe abgeleitet.

3. Erhebungsdesign

Die Erhebung startete Mitte November 2012 und endete Anfang Januar 2013.

Als Grundgesamtheit werden die Betriebe des zulassungspflichtigen und des zulassungsfreien Handwerks definiert, die sich formaljuristisch durch die Erfassung in den Anlagen A sowie B Abschnitt 1 der Handwerksordnung abgrenzen lassen. (vgl. Feuerhake 2012, S. 55).

Da keine genaue Auflistung dieser Betriebe zugänglich ist, kann keine zufällige Stichprobe aus dieser Grundgesamtheit gezogen werden.

Stattdessen wurde einerseits ein Online-Fragebogen zur Verfügung gestellt, der auf verschiedenen Wegen beworben wurde. Andererseits wurde eine Druckversion an die Beauftragten[1] für Innovation und Technologie der Handwerkskammern zur Weiterleitung an die von ihnen betreuten Handwerksbetriebe versendet. Insgesamt haben fast 400 Betriebe an der Befragung teilgenommen. Nach Bereinigung der Umfrage beläuft sich die Stichprobe auf 323 gültige Antworten. Durch die Selbstrekrutierung kann nicht vollständig gewährleistet werden, dass alle Befragten der Grundgesamtheit zugeordnet werden können. Um diese Problematik einzugrenzen, wurde die Stichprobe differenziert hinsichtlich der jeweiligen Betriebsgröße betrachtet.[2] Das Handwerk setzt sich aus kleinen und mittleren Betrieben zusammen. Im Folgenden wird eine Strukturierung der befragten Betriebe anhand verschiedener Größenklassen vorgenommen. Da sich auch eine geringe Anzahl an großen Unternehmen, die nicht dem Handwerk zuzuordnen sind, an der Befragung beteiligt haben, werden diese im Folgenden gesondert ausgewiesen und in Teilen zum direkten Vergleich den Handwerksbetrieben gegenübergestellt. In allen Gesamtberechnungen werden diese großen

[1] *Aus Gründen der Lesbarkeit wird im Folgenden auf eine geschlechtsneutrale Formulierung verzichtet. Es sind jedoch immer beide Geschlechter im Sinne der Gleichbehandlung angesprochen.*

[2] *Die Unternehmensgröße wird im Folgenden anhand der Mitarbeiterzahl definiert.*

Unternehmen nicht berücksichtigt, da ausschließlich ein Bild der Bedürfnisse des Handwerks gezeichnet werden soll.

Es besteht die Möglichkeit, dass auch nach Bereinigung andere KMU, die nicht dem Handwerk zuzuordnen sind, in die Stichprobe gelangt sind. Hierbei handelt es sich, aufgrund der gezielten Ansprache von Handwerksbetrieben, jedoch um Einzelfälle. Insgesamt soll die Befragung ausschließlich einen Überblick über die derzeitige IT-Sicherheitslage in Handwerksbetrieben geben.

Um die wichtigsten IT-Sicherheitslücken in den Betrieben des Handwerks zu identifizieren, wurden neben der Betriebsbefragung neun Experteninterviews durchgeführt.
Hierzu wurden Berater aus der Handwerkskammerorganisation interviewt, die aufgrund der Durchführung von Veranstaltungen zum Thema IT-Sicherheit oder durch gezielte Beratungen für Betriebe, weitreichende Erfahrungswerte zur IT-Sicherheitslage im Handwerk aufweisen.

Einerseits werden die Erkenntnisse aus diesen Interviews genutzt, um forschungsleitende Hypothesen zu generieren, die mithilfe der quantitativen Erhebung überprüft werden. Andererseits bietet die Einbeziehung der Berater darüber hinaus die Möglichkeit, die Selbsteinschätzung der Betriebe aus Expertensicht zu ergänzen und zu objektivieren. Durch diese duale Herangehensweise können Schwachstellen in den Handwerksbetrieben identifiziert und der Bedarf an Beratungsthemen abgeleitet werden.

3.1 Stichprobe

Im Folgenden wird die Zusammensetzung der vorliegenden Stichprobe abgebildet. Die vertretenen Betriebsgrößenklassen innerhalb der Stichprobe werden hierbei der Verteilung innerhalb der Grundgesamtheit vergleichend gegenüber gestellt.

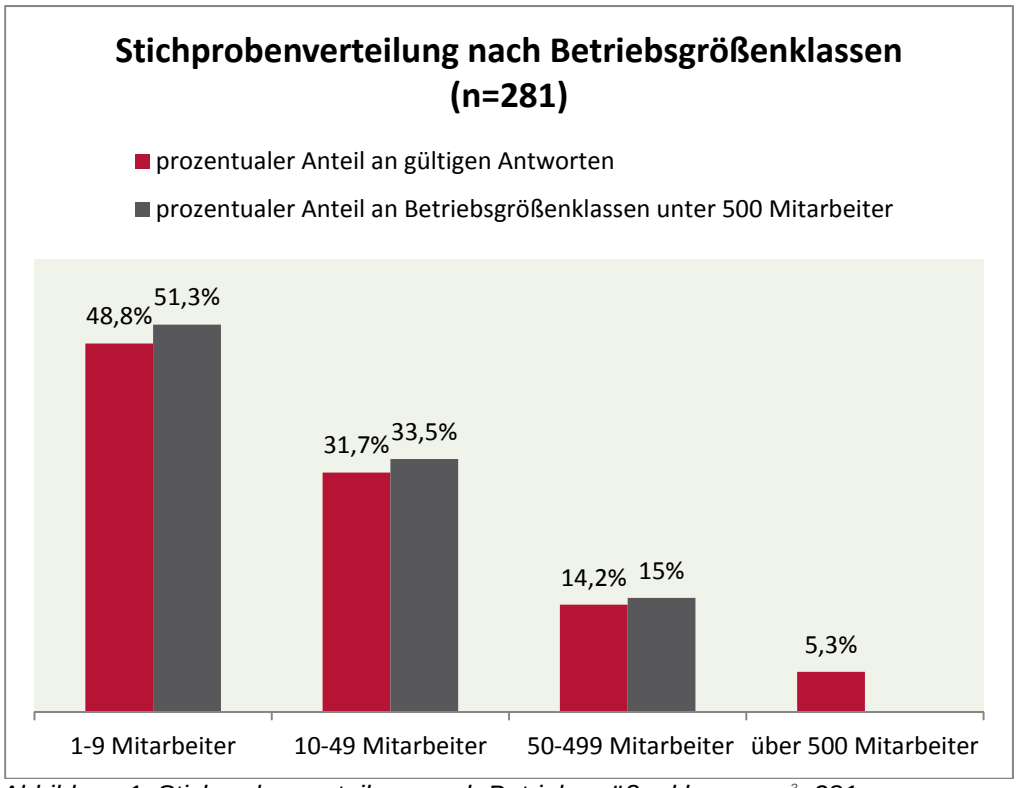


Abbildung 1: Stichprobenverteilung nach Betriebsgrößenklassen, n[3]=281

Die folgenden zwei Abbildungen stellen die Verteilungen der Betriebsgrößenklassen mit weniger als 500 Mitarbeitern, innerhalb der durchgeführten Studie zur IT-Sicherheit sowie die der Grundgesamtheit laut Angaben des Zentralverbands des deutschen Handwerks, dar. Die Verteilung der Betriebe nach Unternehmensgröße innerhalb der Stichprobe entspricht nicht der bundesweiten Verteilung (vgl. Abbildung 2 und 3).

[3] *Die Stichprobengröße variiert abhängig von den jeweils betrachteten Betriebsgrößenklassen und den gültigen Antworten der jeweiligen Frage.*

Der Anteil der Kleinstbetriebe in der vorliegenden Stichprobe (vgl. Abbildung 2) fällt geringer aus als bei der bundesweiten Vergleichsstatistik des Zentralverbands des deutschen Handwerks (ZDH) (vgl. Abbildung 3). Die Betriebsgrößenklassen sind innerhalb der vorliegenden Stichprobe ausgeglichener verteilt als innerhalb der Vergleichsstatistik. Während laut Angaben des ZDH nur 2% der Betriebe des Handwerks mehr als 49 Mitarbeiter beschäftigen, stellt diese Klasse innerhalb der Stichprobe 15,1% dar. Auch die Anteile der Betriebsgrößenklasse mit weniger als 5 Mitarbeitern weichen stark voneinander ab. Während diese Betriebe innerhalb der Grundgesamtheit 61% ausmachen, sind es innerhalb der Stichprobe nur knapp 28%.

Die Betriebsgrößenklasse von 5- 9 Mitarbeitern entspricht mit 23,4% grob dem Anteil in der Grundgesamtheit von 21%. Die Klassen 10- 19, 20- 49 sowie über 49 Mitarbeiter sind hingegen deutlich überrepräsentiert (vgl. Abbildungen 2 und 3).
Bei der Betrachtung der Betriebsgrößenverteilung innerhalb der Stichprobe fällt auf, dass die Betriebe ab 10 Beschäftigten im Vergleich zur Grundgesamtheit übermäßig stark vertreten sind. Einerseits wurde die Verteilung innerhalb der Stichprobe durch die Bewerbung des Fragebogens durch die beteiligten Berater beeinflusst, andererseits kann ein besonders starkes Interesse größerer Betriebe am Thema vermutet werden. Dementsprechend geringer sind die Beteiligung und das dadurch signalisierte Interesse der Betriebe mit weniger als 10 Mitarbeitern. Bereits hier wird die Notwendigkeit an Sensibilisierung und Information, insbesondere kleinerer Betriebe des Handwerks, deutlich.

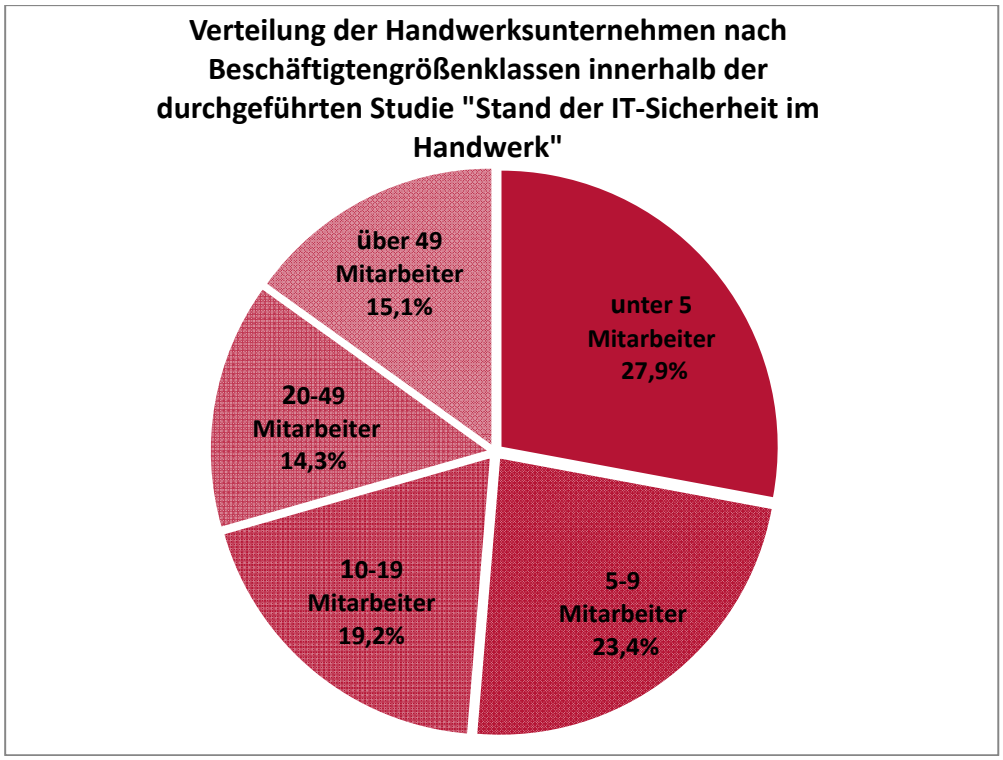


Abbildung 2: Verteilung der Handwerksunternehmen nach Beschäftigtengrößenklassen, prozentuale Anteile an Betrieben mit weniger als 500 Mitarbeitern.

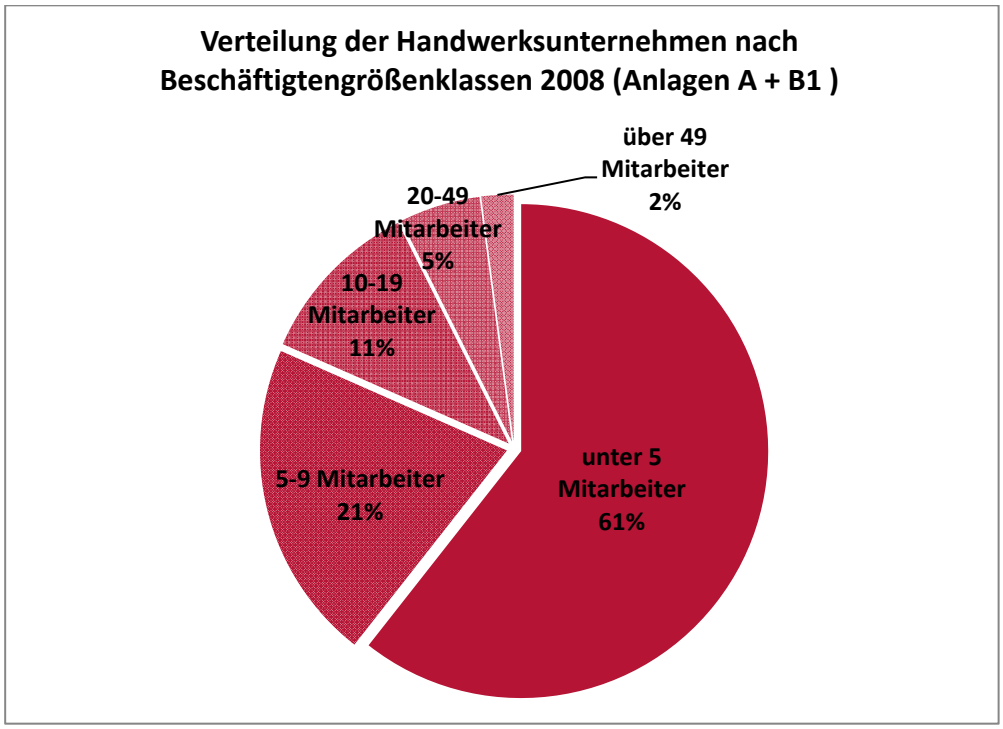


Abbildung 3[4]: Verteilung der Handwerksunternehmen nach Beschäftigtengrößenklassen 2009

[4] *Quelle: Handwerkszählung des statistischen Bundesamtes 2008, in Anlehnung an Darstellung des ZDH.*

Um die beschriebenen Abweichungen der Stichprobe von der Grundgesamtheit zu reduzieren, wird die Stichprobe für einige Berechnungen gewichtet. Für die Gewichtung wurden die Angaben aus der Grafik des ZDH (vgl. Abbildung 3) als Grundlage herangezogen. Alle Berechnungen, die ausschließlich den Vergleich zwischen den Betriebsgrößenklassen zum Ziel haben, sind hiervon unberührt geblieben, da in diesen Fällen der jeweilige prozentuale Anteil an der Gesamtstichprobe keinen Einfluss auf die Ergebnisse hat. Die Gewichtung spielt insbesondere dann eine Rolle, wenn Aussagen über die gesamte Stichprobe gemacht werden, ohne die Betriebsgrößenklassen zu differenzieren.

3.2 Wer hat den Fragebogen beantwortet?

Der größte Anteil der Fragebögen wurde von den Betriebsinhabern selbst ausgefüllt. 33,4% gaben an, sowohl Betriebsinhaber als auch Meister zu sein. 27,6% der Fragebögen wurden von Gesellen beantwortet. Circa jeder zehnte Fragebogen wurde von einem kaufmännischen Angestellten bearbeitet (10,4%). Selten hingegen haben Lehrlinge (3,2%), mitarbeitende Familienmitglieder (4,5%) oder angestellte Meister (8,1%) die Antworten gegeben.

Es ist positiv zu bewerten, dass sich insbesondere die Betriebsinhaber mit dem Fragebogen beschäftigt haben, was ihr Interesse am Thema IT-Sicherheit signalisiert. Der Inhaber muss als Entscheidungsperson, welche die Umsetzung von IT-Sicherheitsmaßnahmen anstößt, für die Risiken durch die eingesetzten Technologien sensibilisiert werden.

Es kann darüber hinaus angenommen werden, dass die Inhaber der Betriebe über die vorliegende Infrastruktur und die bereits eingesetzten Sicherheitsmaßnahmen voll informiert sind und somit zuverlässige Auskünfte über diese geben können.

3.3 Hypothese

Auf Basis der Ergebnisse der im Vorfeld erhobenen Interviews mit den Betriebsberatern werden im Folgenden forschungsleitende Hypothesen formuliert. Die Daten aus der Betriebsbefragung sollen dann hinsichtlich der aufgestellten Hypothesen ausgewertet werden.

Die befragten Berater sind sich einig darüber, dass der Grad der IT-Sicherheit in starker Abhängigkeit zur Betriebsgröße steht. Zum einen verfügen kleine Unternehmen über eine weniger ausgebaute IT-Infrastruktur, zum anderen messen diese dem Thema IT-Sicherheit eine geringere Bedeutung zu.

„Ja, je kleiner die Unternehmen sind, desto vernachlässigter ist das Ganze.“ (Nr.4, S.2)

„Also je größer der Betrieb ist, umso dessen bewusster ist er sich auch.“ (Nr.5, S.4)

„wenn der Betrieb größer ist, dann bemüht er sich und wenn da mehr PC - Arbeitsplätze vorhanden sind, dann ist natürlich auch [für] das Thema sensibilisiert.“ (Nr.8, S.2)

Darüber hinaus stehen weniger personelle Ressourcen innerhalb des Betriebs zur Verfügung, welche für den Bereich der IT und deren Sicherheit eingesetzt werden können.

„Wir haben es im Handwerk überwiegend mit sehr kleinen Unternehmen zu tun, die auch in der Regel keine eigene IT -Kompetenz im Hause haben.“ (Nr.9, S.1)5

Die Experten weisen darauf hin, dass weder das Gewerk ausschlagend für den Stand der IT-Sicherheit ist, noch ob die Wertschöpfung vorrangig durch Dienstleistungs- oder Produktionsmerkmale gekennzeichnet werden kann. Zwar stehen verschiedenen Gewerke, wie beispielsweise die Elektrotechnik, dem Thema IT-Sicherheit fachlich näher als andere,

[5] *Erläuterung der Ziffern: Laufende Nummer des Interviews, Seitenzahl.*

Hypothese:

Je mehr Mitarbeiter innerhalb eines Betriebs beschäftigt sind, desto näher kommt der Betrieb dem Ziel einer sicheren IT.

wie zum Beispiel die Handwerke für den privaten Bedarf. Hiermit erklären die Experten eine grundlegende Sensibilisierung in einigen Branchen. Trotzdem sind nach deren Aussagen die größten Differenzen in Bezug auf den erreichten IT -Grundschutz und das notwendige Bewusstsein für auftretende Gefahren hauptsächlich von der Betriebsgröße abhängig.

Die abgeleitete zu überprüfende Hypothese lautet somit:

Je mehr Mitarbeiter innerhalb eines Betriebs beschäftigt sind, desto näher kommt der Betrieb dem Ziel einer sicheren IT.

Die Implikation der Hypothese legt nahe, dass vergleichbar große Betriebe gemeinsame Interessenlagen teilen. Es ist daher sinnvoll Betriebsgrößenkategorien zu bilden und diese miteinander zu vergleichen, um differenzierte Aussagen zum Thema IT- Ausstattung und erreichte IT-Sicherheit treffen zu können.

Nachfolgend werden zur Darstellung erster Ergebnisse die Betriebe mit 1- 9 Mitarbeitern entgegen der Abbildungen 2 und 3 als Kleinstbetriebe zusammengefasst. Betriebe mit 10- 49 Mitarbeitern bilden im Folgenden ebenfalls eine Betriebsgrößenklasse. Zugunsten der Übersichtlichkeit wurden diese beiden Betriebsgrößenklassen, die ebenfalls in der bereits in Kapitel 2 zitierten Studie IT-Sicherheitsniveau in kleinen und mittleren Unternehmen verwendet werden, gewählt (vgl.Bünnig, Hillbrand 2012, S.15). Unter der Betriebsgrößenklasse der mittleren Unternehmen werden alle Betriebe ab 50 bis 499 Mitarbeitern gezählt. Da laut Darstellung des ZDH (vgl. Abbildung 3) nur ca. 2% der KMU des Handwerks mehr als 49 Mitarbeiter beschäftigen, wird auf eine stärkere Differenzierung verzichtet.

	Kleinstbetrieb	Kleinbetrieb	Mittlerer Betrieb
Mitarbeiteranzahl	1 - 9	10 - 49	50 - 499

Abbildung 4: Kategorisierung nach Betriebsgröße

Diese grobe Unterteilung soll zunächst dabei helfen, die Ergebnisse zu strukturieren und erste Tendenzen aufzuzeigen. Besonders aussagekräftige Ergebnisse werden im Folgenden herausgegriffen. Bei diesen wird eine weitere Unterteilung der Betriebsgrößenklasse unter 50 Mitar-

beitern in Anlehnung an Abbildung 2 und 3 vorgenommen, um differenziertere Aussagen über die, laut Hypothese, besonders gefährdete Zielgruppe der kleineren Betriebe treffen zu können.

4. Ergebnisse

4.1 Infrastruktur und Nutzungsverhalten

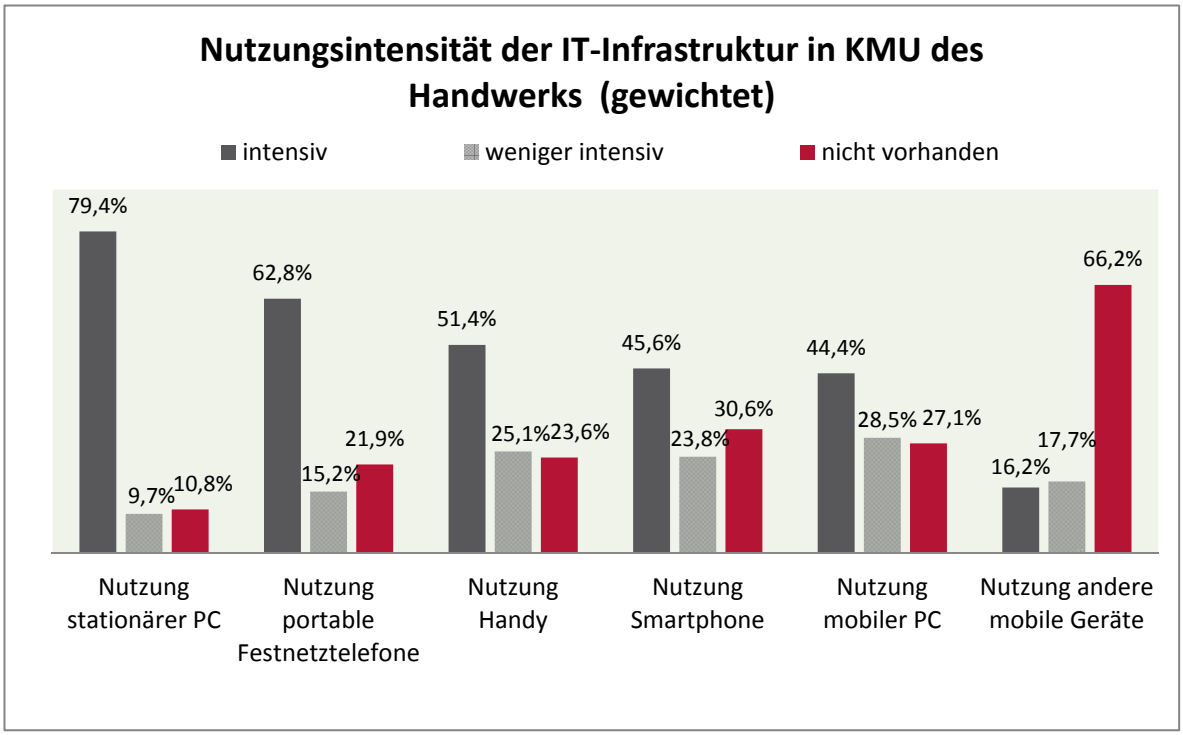


Abbildung 5: Nutzungsintensität der IT -Infrastruktur in KMU des Handwerks (gewichtet)[6]

Laut der zitierten Studie „IT-Sicherheitsniveau in kleinen und mittleren Unternehmen“ zeichnet sich der deutsche Mittelstand insgesamt durch eine hohe IT -Affinität aus. Von allen KMU setzten bereits 99,7% IT in ihren täglichen Geschäftsprozessen ein (vgl. Büllingen/Hillbrand 2012, S.2).

Zum Vergleich: Die im Rahmen dieser Erhebung befragten Betriebe nutzen in 89,1% der Fälle mindestens einen stationären PC. 2,2% der Befragten geben an, weder einen stationären PC noch ein mobiles Ge-

[6] *Keine einheitliche Angabe zu n möglich, da mehrere Fragen in der Abbildung dargestellt werden. Stichprobengröße variiert.*

rät wie Notebook oder Tablet -PC zu nutzen. Nur 1% der Befragten verfügt über kein internetfähiges Gerät.
Es kann festgehalten werden, dass in nahezu allen Betrieben des Handwerks eine IT-Grundausstattung vorhanden ist. Die Nutzungsintensität von stationären PCs, Notebooks oder anderen mobilen Geräten unterscheidet sich jedoch stark voneinander (vgl. Abbildung 5).

Der stationäre PC wird im Handwerk am intensivsten verwendet. 79,4% der KMU des Handwerks geben an, diesen sehr häufig bis häufig zu nutzen. 44,4 % der Betriebe nutzen einen mobilen PC, gefolgt von dem Tablet-PC, der schon in 33,9 % der Handwerksbetriebe Anwendung findet. Bereits zum Zeitpunkt der Befragung verwenden 16,2 % aller Handwerksbetriebe den Tablet-PC häufig bis sehr häufig.
Werden die verschiedenen Telefonarten betrachtet, wird die portable Festnetzvariante (DECT) von den befragten Betrieben am häufigsten benutzt. 62,8 % der Befragten geben an, sehr häufig oder häufig über einen portablen Festnetzanschluss zu telefonieren. In 51,4% aller Fälle werden nicht internetfähige Handys häufig bis sehr häufig genutzt. 45,6% aller Betriebe verwenden das Smartphone häufig bis sehr häufig. Laut unserer Umfrage steht in ca. 66 % aller Betriebe ein Smartphone zur Verfügung.

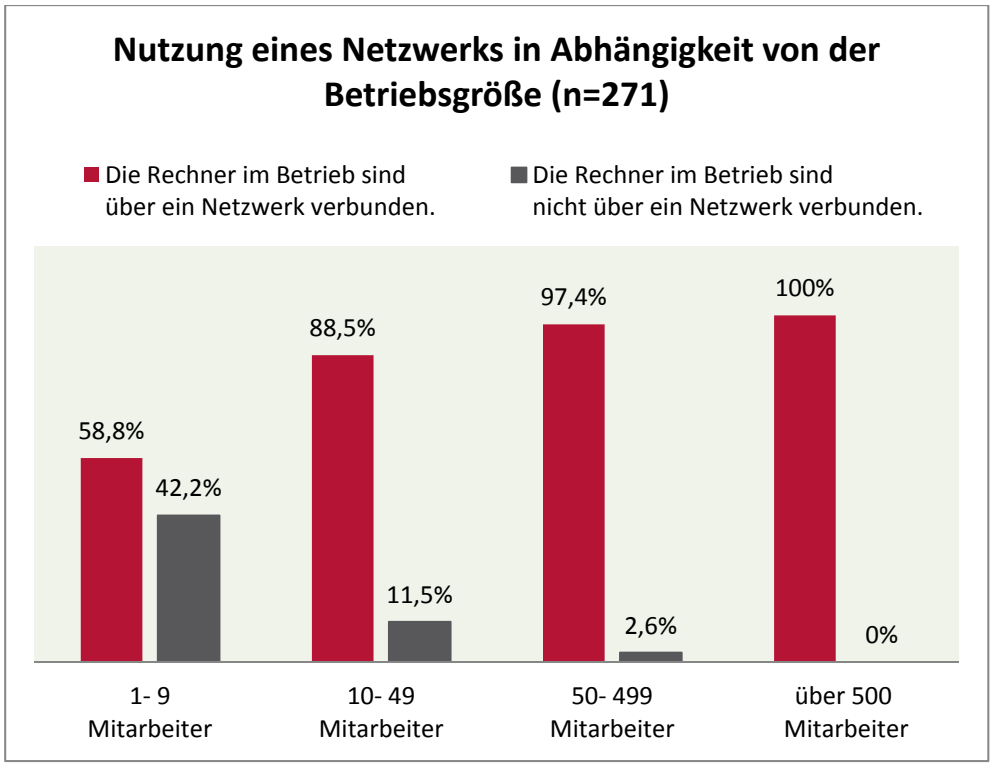


Abbildung 6: Nutzung eines Netzwerks in Abhängigkeit von der Betriebsgröße

Die Nutzung eines lokalen Netzwerkes steigt mit der Betriebsgröße, insbesondere ab 10 Mitarbeitern, stark an. Während die Betriebe mit unter zehn Mitarbeitern in nur 58,8% der Fälle ihre Rechner mit einem Netzwerk verbinden, sind es in der Kategorie 10 - 49 Mitarbeiter schon 88,5%. (vgl. Abbildung 6).

Es kann davon ausgegangen werden, dass Betriebe mit weniger als zehn Mitarbeitern auch über eine geringere Anzahl an Rechnern verfügen. Darüber hinaus kann in größeren Betrieben von einer differenzierteren Arbeitsteilung ausgegangen werden, die eine starke Vernetzung verschiedener Arbeitsbereiche notwendig macht. Dies deutet sich ebenfalls innerhalb der Infrastruktur an.

„In größeren Betrieben ist immer ein Netzwerk vorhanden. Wenn da mehrere Arbeitsplätze sind, sind die vernetzt. Das ist Standard.“ (Nr.2, S.4)

Ganz ähnlich verhält es sich mit der Nutzung eines Servers. Auch diese nimmt mit ansteigender Betriebsgröße zu. Während in der Kategorie 1-9 Mitarbeiter nur in 40,2% der Fälle ein Server vorhanden ist, ist der Verwendungsgrad in der Kategorie 10 - 49 Mitarbeiter mit 80,3% dop-

pelt so hoch. Alle Betriebe mit mehr als 49 Mitarbeitern geben an, einen Server zur Ablage ihrer Daten zu nutzen (vgl. Abbildung 7).

In 61,6% der Fälle haben die Mitarbeiter eines Betriebs dienstlich freien Zugang zum Internet. Insbesondere in diesen Fällen ist es notwendig, die Mitarbeiter für die Gefahren des Internets zu sensibilisieren. Darüber hinaus ist es sinnvoll, die Verantwortlichen innerhalb eines Betriebs über Beschränkungsmöglichkeiten der Internetnutzung aufzuklären und aufzuzeigen, welche Regeln den Mitarbeitern hierbei vorgegeben werden sollten.

In gut 70% der Betriebe sind die Rechner über ein Netzwerk verbunden. Auf dieses Netzwerk kann in 28,4% der Fälle von außerhalb des Betriebsgeländes zugegriffen werden. Durch das Risiko eines unberechtigten Zugriffs auf interne IT-Strukturen besteht die Gefahr der Manipulation von Daten und der Maschinensteuerungen sowie des Abrufens sensibler Firmeninformationen.
53,3% der Betriebe nutzen einen zentralen Server zur Datenablage. In 16,2% dieser Fälle haben die Mitarbeiter des Betriebs uneingeschränkten Zugriff auf die zentral gespeicherten Daten.
In 12,7% der befragten Betriebe sind Maschinen oder Steuerungen über einen Rechner erreichbar. Von diesen Rechnern mit Maschinenanbindung haben 74,3% Zugriff auf das Internet. Das heißt in 9,4% der befragten Betriebe sind Maschinen mit dem Internet vernetzt und somit besonders gefährdet für Angriffe von außen.

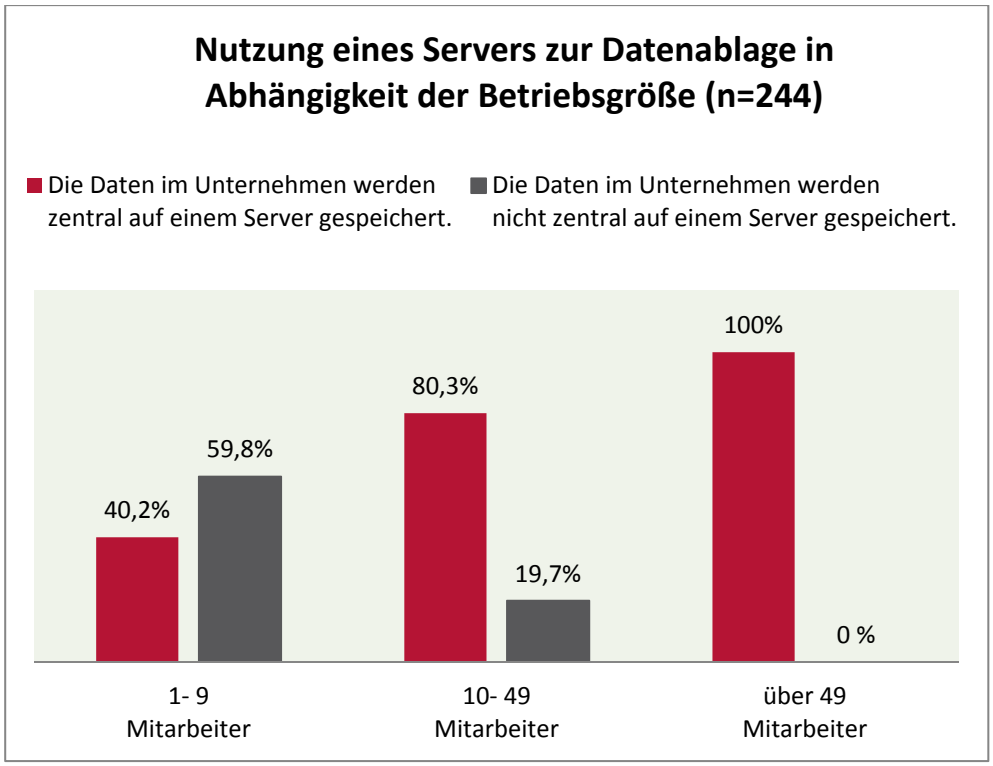


Abbildung 7: Nutzung eines Servers zur Datenablage in Abhängigkeit der Betriebsgröße

4.2 Nutzung innovativer Informationstechniken am Beispiel von Cloud-Computing und mobilen Anwendungen

Laut der Veröffentlichung „IT-Sicherheitslage im Mittelstand 2012“, einer Studie von „Deutschland sicher im Netz“ von Brandl und Böhme, geht der Trend auch in kleinen und mittelständischen Unternehmen hin zur Mobilität. Bei diesem Update zur Studie von 2011 wird festgehalten, dass Notebooks bereits in 64% (2011: 60%) der KMU genutzt werden. Vergleicht man dieses Ergebnis mit der vorliegenden Befragung, so wird deutlich, dass auch bei der ausschließlichen Betrachtung des Handwerks die Nutzung von Notebooks bereits weit verbreitet ist. 77,7% der befragten Handwerksbetriebe geben an, ein Notebook zu verwenden. Immerhin 44,4% der Handwerksbetriebe innerhalb der Stichprobe tun dies häufig oder sehr häufig. Andere mobile Geräte

werden von rund einem Drittel (33,9%) der befragten Betriebe in Anspruch genommen.
Eine weitere zukunftsträchtige Entwicklung stellt das Cloud-Computing dar. Cloud-Computing bietet die Möglichkeit einer weitgehend automatisierten Datensicherung mithilfe einer internetbasierten Anwendung. Laut dem Bundesamt für Sicherheit der Informationstechnik wird Cloud-Computing wie folgt definiert:
„Cloud-Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT- Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud-Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur […]Plattformen […]und Software […].“ (Bundesamt für Sicherheit und Informationstechnik 2012, S. 15f.)

Auch die Anwenderstudie „Potenziale von Cloud-Computing im Handwerk“ des Fraunhofer Instituts für Arbeitswissenschaft und Organisation (IAO) beschäftigt sich intensiv mit dem Thema Cloud-Computing, wobei das Augenmerk hierbei insbesondere auf der aktuellen und der zukünftigen Bedeutung der Technologie für die Betriebe des Handwerks und deren Einstellung zu den sich daraus ergebenden Möglichkeiten liegt. Laut der Studie des Fraunhofer IAO wurden Anfang 2011 in rund 16% der Handwerksbetriebe die Möglichkeiten des Cloud-Computings genutzt. Die Studie prognostiziert jedoch insbesondere für größere Betriebe des Handwerks eine Bedeutungssteigerung des Cloud Computings (vgl. Kasper, Kett, Weisbecker 2012, S .43).

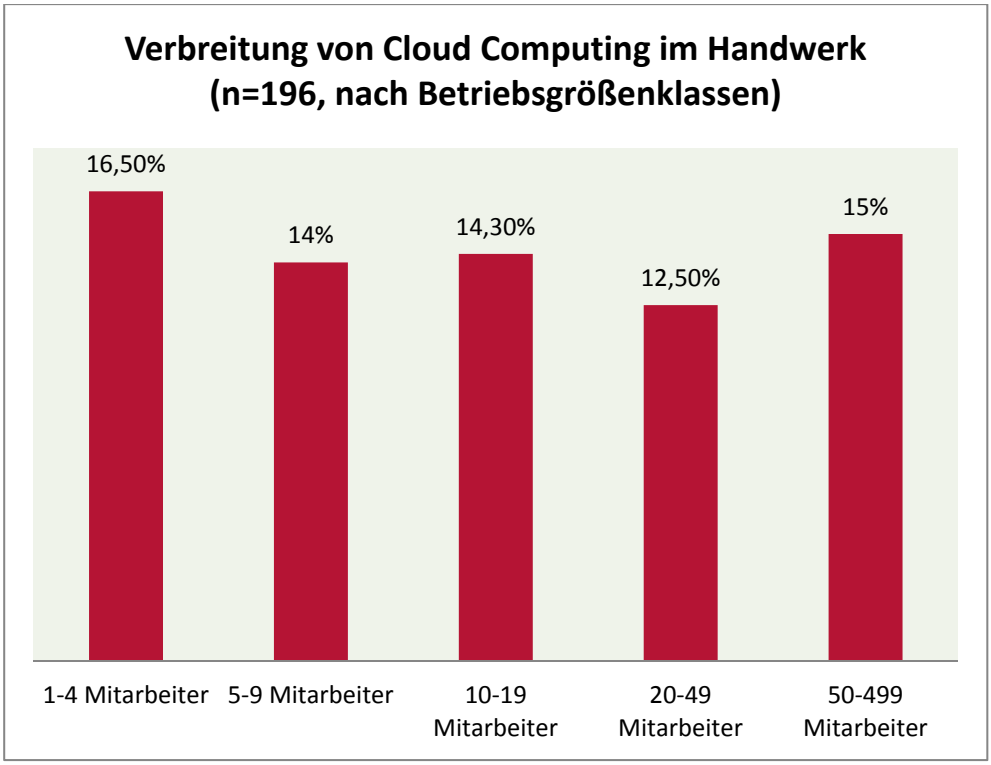


Abbildung 8: Verbreitung von Cloud Computing im Handwerk (nach Betriebsgrößenklassen)

Auf Basis dieser Befragung können weder betriebs - größen - noch branchen -spezifische Präferenzen für die Nutzung einer Cloud bestätigt werden.

Die bisher gering verbreitete Nutzung des Cloud-Computing im Handwerk wird durch die hier vorliegende Befragung unterstützt. Nur 10,2% der Betriebe geben an, von Cloud-Computing-Technologien Gebrauch zu machen. Die Ergebnisse dieser Untersuchung zeigen ebenfalls, dass sich der derzeitige Nutzungsgrad des Cloud-Computing zwischen den Betriebsgrößenklassen kaum unterscheidet. Kleinstbetriebe mit weniger als fünf Mitarbeitern nutzen im Schnitt mit 16,5% am häufigsten eine Cloud. Betriebe mit fünf bis neun Mitarbeiter und die Betriebe mit zehn bis weniger als 20 Mitarbeiter verwenden in rund 14% der Fälle bereits die Möglichkeit des Cloud Computing. Innerhalb der Betriebsgrößenklasse von 20 bis weniger als 50 Mitarbeiter geben 12,5% der Befragten an, Daten in einer Cloud abzulegen. Die mittleren Betriebe bis unter 500 Mitarbeiter nutzen diese Möglichkeit in 15% der Fälle (vgl. Abbildung 8). Eine Präferenz abhängig von der Betriebsgröße kann folglich bei den von uns befragten Betrieben nicht festgestellt werden. Auch branchenspezifische Unterschiede sind nicht erkennbar.

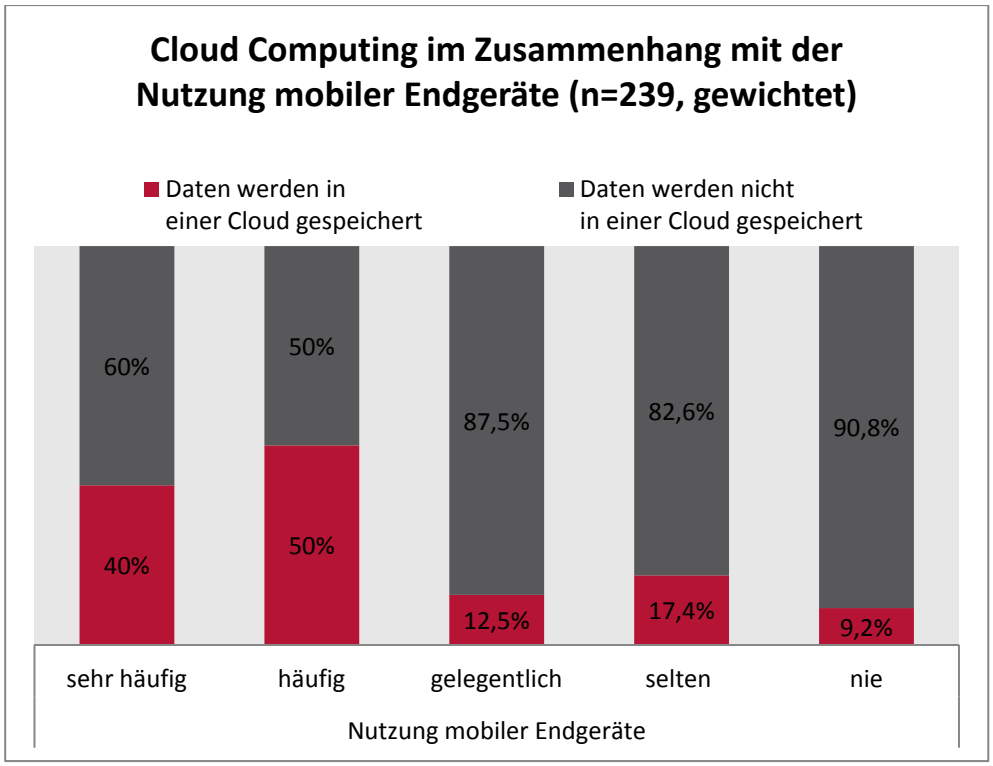


Abbildung 9: Cloud -Computing im Zusammenhang mit der Nutzung mobiler Endgeräte (n= 239, gewichtet)

Auf Basis dieser Befragung können weder Betriebsgrößen- noch branchenspezifische Präferenzen für die Nutzung einer Cloud bestätigt werden. Betrachtet man jedoch unabhängig von Größe und Branche die Betriebe in Bezug auf die Nutzung mobiler Endgeräte (ausgeschlossen Laptops) werden charakteristische Unterschiede in der Anwendung des Cloud-Computing deutlich. Die 10,2% derjenigen Betriebe, die Daten in einer Cloud speichern, nutzen mobile Geräte häufiger, als jene Betriebe, die das Cloud-Computing bisher nicht in Anspruch nehmen (vgl. Abbildung 9). Die Erklärung kann aus verschiedenen Perspektiven erfolgen. Sowohl beim Cloud-Computing, als auch bei den mobilen Anwendungen handelt es sich um relativ junge Technologien, deren Nutzung im Handwerk bisher nicht weit verbreitet ist. Der Gebrauch dieser Technologien spricht folglich für eine besondere Zukunftsorientierung des Betriebsinhabers. Betriebe, die sich als zukunfts- und innovationsorientiert ansehen, sind daher generell aufgeschlossener gegenüber mobilen Lösungen, die sowohl das Cloud-Computing, als auch mobile Endgeräte bieten.

Das Cloud-Computing birgt den Vorteil, dass Daten mobil bereitgestellt werden können und so ein weltweiter Zugriff auf diese möglich wird. Der Nutzen einer Cloud wird folglich insbesondere dann für einen Betrieb verstärkt, wenn dessen Beschäftigte häufig mit mobilen Endgeräten von außerhalb des Betriebsgeländes auf ihre Daten zugreifen müssen.
Auch die Studie des Fraunhofer IAO sieht die Nutzung mobiler Geräte als geeigneten Einstieg in das Cloud-Computing (vgl. Kasper, Kett, Weisbecker 2012, S.43).

4.3 IT-Sicherheitslücken im Handwerk und der Einsatz von Sicherheitsmaßnahmen

4.3.1 Gefährdungspotentiale laut eigener Aussage

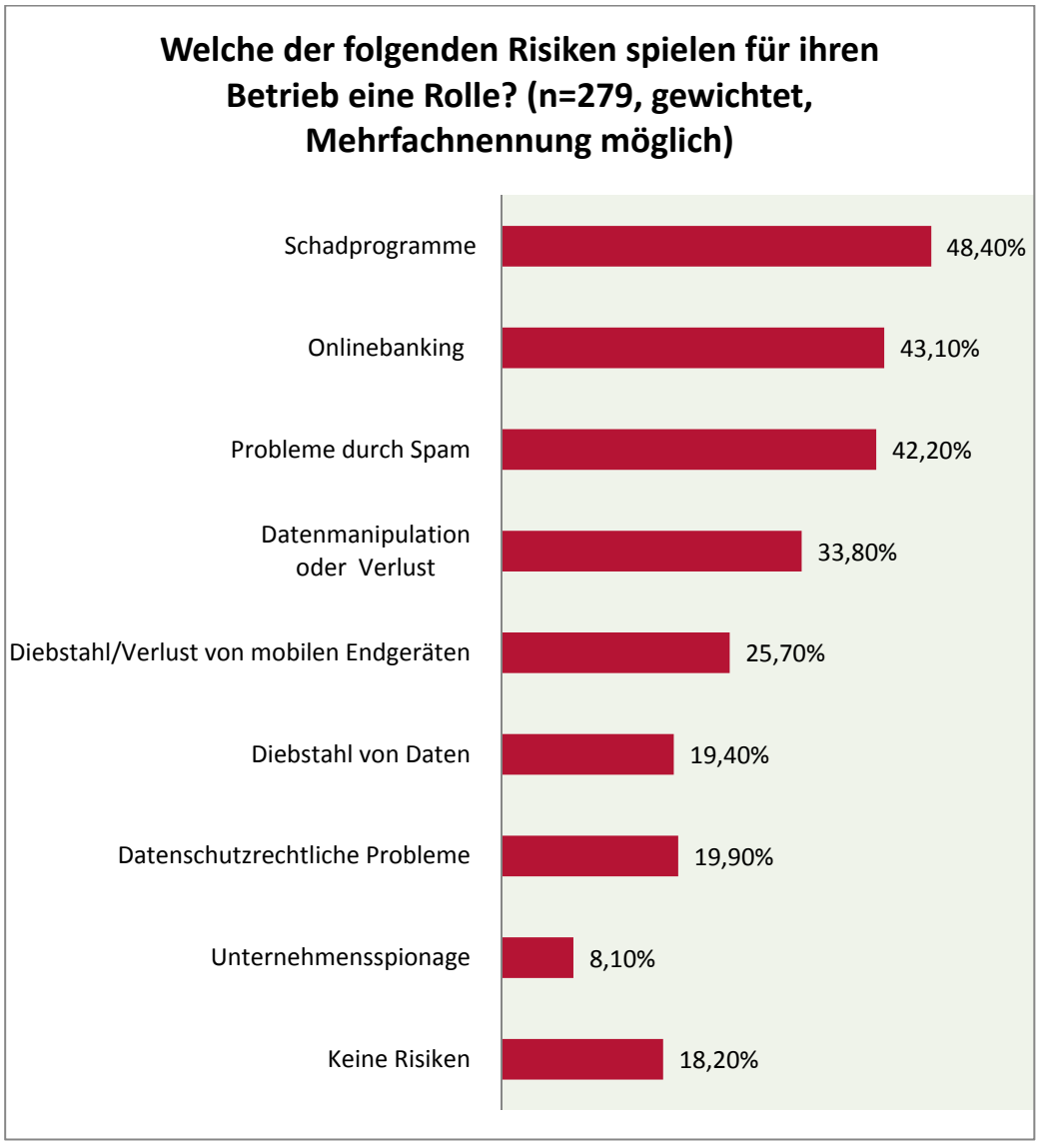


Abbildung 10: Welche der folgenden Risiken spielen für ihren Betrieb eine Rolle? (gewichtet, Mehrfachnennung möglich)

Im Rahmen der Befragung wurde erhoben, welche IT-bezogenen Risikofelder im betrieblichen Alltag eine Rolle spielen: Das Ranking der

Risikofaktoren kristallisiert vier Themenbereiche als besonders relevant heraus.
Mit 48,4% beurteilen die Betriebe Schadprogramme wie Würmer, Viren und Trojaner als den größten Risikofaktor, gefolgt vom Onlinebanking mit 43,1% der Nennungen.

Auch Probleme durch Spam stellen ein wichtiges Themenfeld dar. Im Schnitt geben 42,2% der Betriebe Spam als potenzielles Risiko an. Der Bereich Manipulation oder Verlust von Daten wird immerhin von 33,8% der Befragten als Risikofaktor angegeben (vgl. Abbildung 10). Wie bereits in anderen Studien (vgl. BMWi 2010, S. 42f.) ausgewiesen, spielt Unternehmensspionage eine untergeordnete Rolle. Nur 8,1% der befragten Handwerksbetriebe befürchtet eine gezielte Spionage. Auch der Diebstahl von Daten (19,4%) und datenschutzrechtliche Probleme (19,9%) werden als eher nachrangig empfunden. Rund ein Viertel der Befragten gibt an, dass der Verlust mobiler Endgeräte als IT-Sicherheitsrisiko eine Rolle spielt. Immerhin knapp jeder fünfte Handwerksbetrieb gibt an, mit keinem der aufgeführten Risiken konfrontiert zu sein (vgl. Abbildung 10).
Alle der vier am häufigsten genannten Risikofelder werden von mindestens ⅓ der befragten Betriebe als relevant eingestuft. Inbesondere in den Bereichen Schadprogramme, Onlinebanking, Spam und Datenverlust bestehen Wunsch und Bedarf an Information und müssen daher in verschiedenen Veranstaltungsformaten thematisiert werden.

Die befragten Handwerksbetriebe sehen insbesondere die Risiken als relevant an, die ihre täglichen Arbeitsabläufe gefährden. Weniger häufig werden Fragen des Datenschutzes als relevant bewertet, da diese bei Nichtbeachtung nicht zwangsläufig mit sofortigen Konsequenzen einhergehen. Insbesondere wegen der fehlenden Sensibilität für dieses Thema, ist die Aufklärung über datenschutzrechtliche Regelungen unvermeidbar.

Laut Hypothese nimmt der Gefährdungsgrad eines Betriebes mit sinkender Betriebsgröße zu. Es wird davon ausgegangen, dass insbesondere kleinere Betriebe mit weniger als 50 Mitarbeitern häufig zu wenig über die Risiken der Informationstechnologien informiert sind. Daher werden im Folgenden noch einmal die wichtigsten vier Risikofelder nach Betriebsgrößenklassen unter 50 Mitarbeitern differenziert, um die jeweiligen Gefährdungsschwerpunkte hervorzuheben.

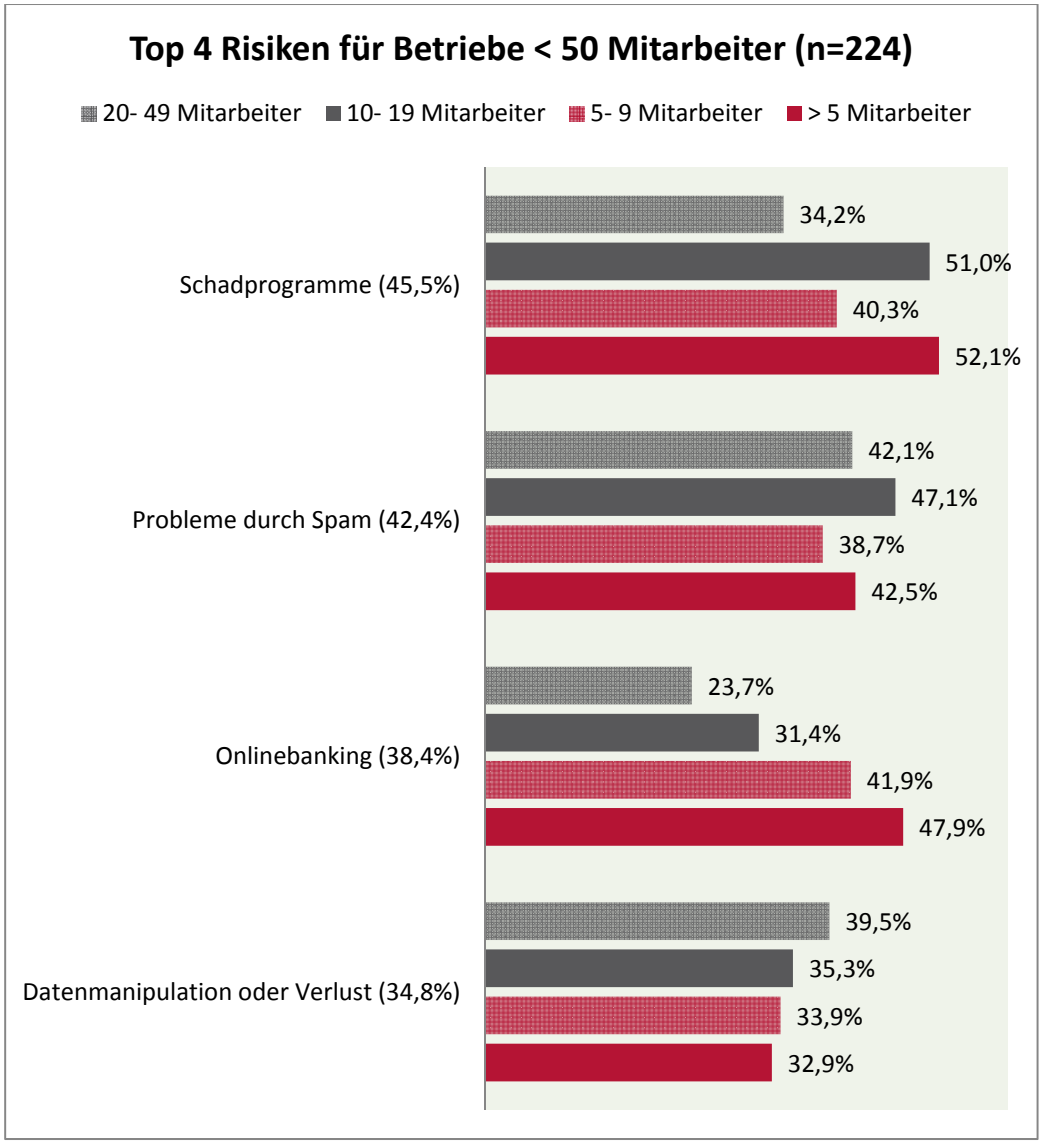


Abbildung 11: Top 4 Risiken für Betriebe < 50 Mitarbeiter
Lesebeispiel: 34,8% aller befragten Betriebe geben an, Risiken in Bezug auf Datenmanipulation oder Datenverlust zu sehen. 32,9% aller befragten Betriebe mit weniger als fünf Mitarbeitern sehen Datenmanipulation oder Datenverlust als potenzielles Risiko.

Werden die Betriebe mit weniger als 50 Mitarbeitern verglichen, fallen die größten Unterschiede in der Beurteilung des Onlinebankings auf. Je kleiner der Betrieb ist, desto risikoreicher wird dieser Bereich eingeschätzt. Trotz rechtlicher Regelungen zum Schutz von Onlinebanking-Nutzern, stehen insbesondere kleinere Betriebe diesem skeptisch gegenüber, 47,9% der Betriebe mit weniger als 5 Mitarbeitern sehen Onlinebanking als Risikofaktor für ihren Betrieb an.
Relativ homogen wird der Bereich Verlust oder Manipulation von Daten bewertet. Rund ⅓ der Befragten sehen dies als potenzielles Risiko, wobei der Anteil mit der Betriebsgröße leicht ansteigt. Keine klaren Tendenzen sind im Bereich der Risikofelder Schadprogramme und Spam zu erkennen.

4.3.2 Aktivitäten zur Herstellung von Datensicherheit

Um die im vorangegangenen Kapitel genannten Risiken zu minimieren, existieren verschiedene Möglichkeiten. Innerhalb der Befragung wurde die Verbreitung von Aktivitäten erhoben, die der Herstellung von Datensicherheit im Unternehmen dienen. Hierzu zählen beispielsweise regelmäßige Backups und die Überprüfung der gesicherten Daten auf Vollständigkeit und Verfügbarkeit. Darüber hinaus muss sowohl die Hard- als auch die Software durch das Einspielen von Schutzprogrammen und regelmäßigen Updates der Programme geschützt werden. Auch weitere Sicherheitsmechanismen, wie die Verwendung sicherer Passwörter und die Einschränkung von Zugangsrechten, sind zum Schutz betrieblicher Daten notwendig.

Abbildung 12: Aktivitäten zur Herstellung von Datensicherheit im Überblick

Die Umfrage unter den Betrieben des Handwerks zeigt, dass einige Maßnahmen zur Herstellung einer sicheren IT und zum Schutz der eigenen Daten im Handwerk bereits vorhanden sind.

Insbesondere Schutzsoftware wie Firewalls, Virenscanner etc. werden in den meisten Betrieben verwendet. 86% der Befragten geben an, diese immer oder weitestgehend einzusetzen. 12,3% wissen jedoch nicht, ob und wie häufig Schutzsoftware zum Einsatz kommt. Immerhin 77% der Befragten geben an, ihre Daten regelmäßig zu sichern, 8% hingegen erledigen dies nicht regelmäßig und gut 15% haben keinen Überblick über die Datensicherung in ihrem Betrieb.

Ähnlich verhält es sich mit dem Einspielen von Sicherheitsupdates der verwendeten Software (Betriebssystem und Applikationen). Auch hier

geben rund ¾ der Betriebe an, diese immer oder weitestgehend umzusetzen.
Deutlich problematischer verhält es sich mit den Themen Passwörter, Überprüfung gesicherter Daten und Datenverschlüsselung. Hier zeigen sich große Lücken in der IT-Sicherheit der befragten Betriebe.
Sichere[7] Passwörter kommen nur in 55% der befragten Betriebe regelmäßig zum Einsatz. Gut 27% der Betriebe geben an, diese nur teilweise, selten oder gar nicht zu verwenden. Die durch Backups gesicherten Daten werden nur von gut der Hälfte der Betriebe regelmäßig auf Vollständigkeit und Verfügbarkeit überprüft. Bisher kaum beachtet wird die Funktion der Verschlüsselung. Nur rund 27% der befragten Betriebe verschlüsseln regelmäßig ihre Daten, beispielsweise vor dem Versenden sensibler Inhalte via E -Mail.
Insbesondere die gängige Schutzsoftware wie Virenscanner und Firewall wird in den meisten Betrieben des Handwerks eingesetzt (vgl. Abbildung 12).

Um jedoch einen angemessenen Basisschutz zu gewährleisten, müssen regelmäßig Sicherheitsupdates, insbesondere beim Betriebssystem und der Schutzsoftware sowie auch bei sämtlichen installierten Anwendungen und Erweiterungen, wie zum Beispiel Java oder Adobe Flash, eingespielt werden. Rund ¼ der Befragten gibt entweder an, diese Aktualisierungen nicht regelmäßig durchzuführen oder keine Kenntnisse zur Aktualität der installierten Software zu haben.
Im Folgenden sollen einzelne Maßnahmen herausgegriffen und nach Betriebsgröße differenziert werden. Der Fokus liegt hierbei einerseits auf bisher von den Betrieben eher vernachlässigten Themen, wie dem Einsatz sicherer Passwörter. Andererseits werden grundlegende Maßnahmen zur Datensicherung genauer betrachtet, da grobe Defizite in diesem Bereich von den befragten Experten diagnostiziert werden.

[7] *Generell gilt ein Passwort als relativ sicher, wenn Folgendes beachtet wird: Mehr als zehn Zeichen, Verwendung von Sonderzeichen und Zahlen, sowie Groß - und Kleinbuchstaben und sinnfreie Zusammensetzung.*

4.3.3 Datensicherung und Überprüfung der gesicherten Daten

Um Daten, beispielsweise im Fall eines Hardwaredefekts, vor Verlust zu schützen, sind regelmäßige Backups notwendig. Hier können rund ¼ der Befragten entweder keine Auskunft zum Stand der Datensicherung erteilen oder geben an, dass diese nicht regelmäßig durchgeführt wird (vgl. Abbildung 12).

Jeder der neun Berater weist auf eine mangelhafte Datensicherung als verbreitetes Phänomen im Handwerk hin. Die meisten sehen die Mängel beim Backup und der dazugehörigen Rücksicherung als größtes IT-Sicherheitsrisiko für die Betriebe des Handwerks. Da insgesamt von einer schlechteren IT-Sicherheitslage in kleineren Betrieben ausgegangen wird, soll zunächst die Sicherung von Daten im Zusammenhang mit der Betriebsgröße betrachtet werden.

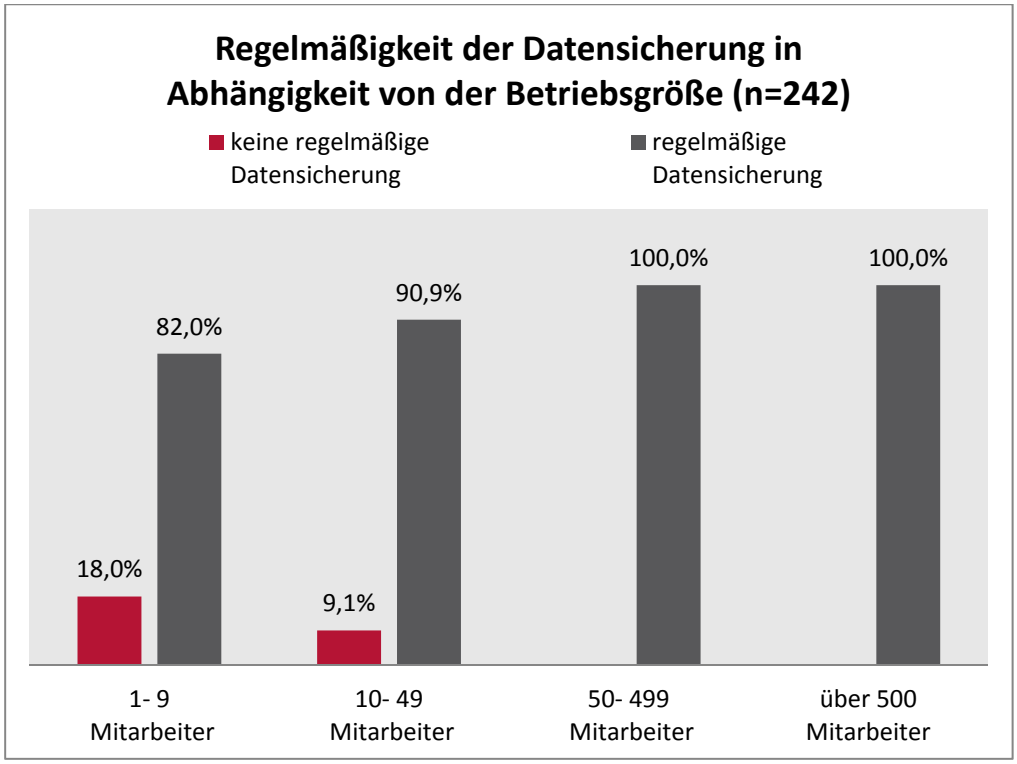
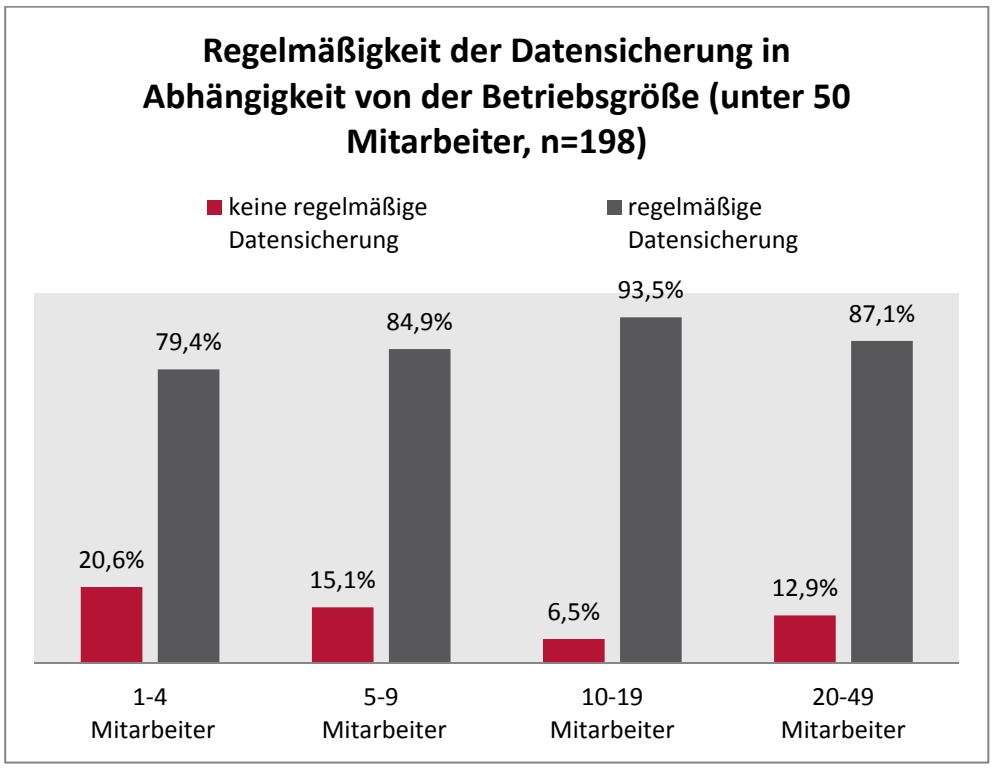


Abbildung 13: Regelmäßigkeit der Datensicherung in Abhängigkeit von der Betriebsgröße

Es werden klare Unterschiede zwischen den Betriebsgrößenklassen in Bezug auf die Regelmäßigkeit der Datensicherung deutlich. Alle befragten Betriebe mit mehr als 49 Mitarbeitern geben an, regelmäßig[8] ihre Daten zu sichern. Von den Betrieben mit weniger als 50 Mitarbeitern sichern im Schnitt nur gut 86% der Betriebe regelmäßig ihre Daten. Wobei auch hier Unterschiede zwischen den Betriebsgrößenklassen festzustellen sind. Die Betriebe mit weniger als zehn Mitarbeitern führen in 18% der Fälle keine regelmäßigen Backups durch. Bei den Betrieben zwischen 10 - 49 Mitarbeitern sind es rund 9% (vgl. Abbildung 13). Die dargestellten Differenzen untermauern somit die Hypothese, dass der Grad der erreichten IT-Sicherheit mit zunehmender Betriebsgröße ansteigt.

Mängel beim Backup und der dazugehörigen Rücksicherung können als eines der größten IT-Sicherheitsrisiken für die Betriebe des Handwerks angesehen werden.



[8] *Die Regelmäßigkeit der Datensicherung wurde durch eine Selbsteinschätzung abgefragt. Als regelmäßige Datensicherung werden die Items immer und weitgehend verstanden. Keine regelmäßige Datensicherung gilt, wenn diese teilweise, kaum oder gar nicht durchgeführt wird.*

Abbildung 14: Regelmäßigkeit der Datensicherung in Abhängigkeit von der Betriebsgröße (unter 50 Mitarbeiter)

Insbesondere die Betriebe mit weniger als 50 Mitarbeitern sind gefährdet und benötigen vertiefte Beratungsangebote.

Betrachtet man die Betriebe mit weniger als 50 Mitarbeitern differenzierter, kann zwar eine leicht ansteigende Tendenz der Backups mit zunehmender Betriebsgröße festgestellt werden (vgl. Abbildung 14), die größten Differenzen in Bezug auf die Sicherung von Daten finden sich jedoch zwischen den Betrieben mit weniger als 50 Mitarbeitern und den Betrieben ab 50 Mitarbeitern (vgl. Abbildung 13).

Das regelmäßige Sichern von Daten ist bisher in den Kleinst- und Kleinbetrieben noch nicht selbstverständlich. Noch deutlicher werden Defizite, wenn es um die regelmäßige Überprüfung dieser gesicherten Daten geht. Hier manifestiert sich erneut die These, dass vor allem in den Kleinst- und Kleinunternehmen weiterhin Sensibilisierungsbedarf zum Thema Datensicherheit besteht.

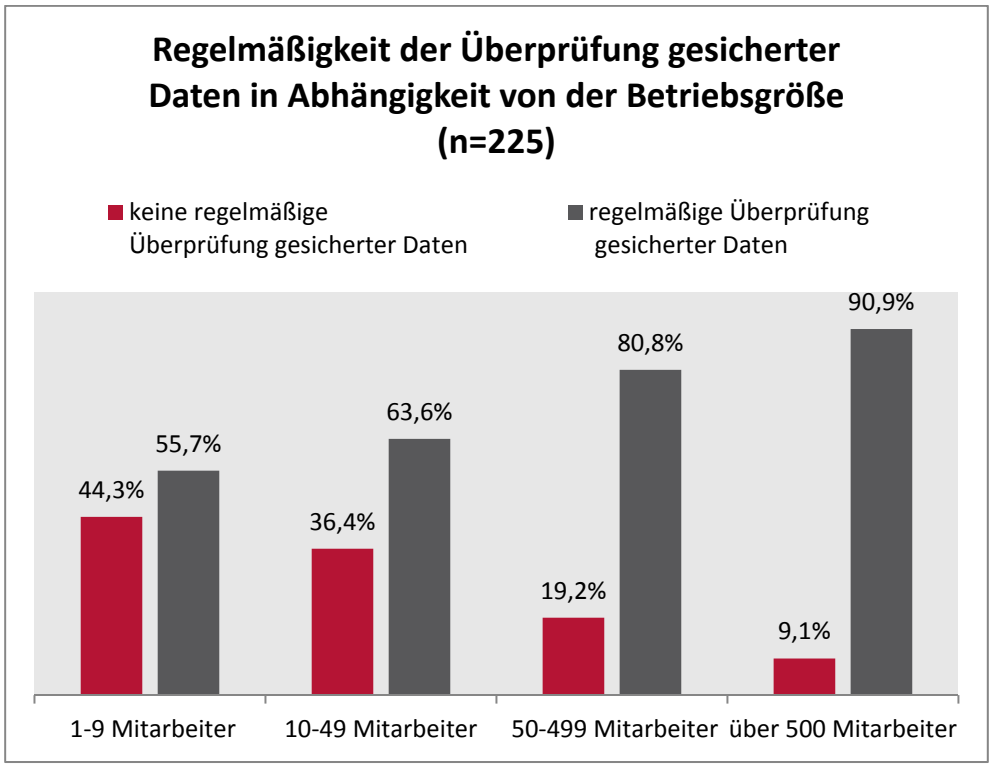


Abbildung 15: Regelmäßigkeit der Überprüfung gesicherter Daten in Abhängigkeit von der Betriebsgröße

Nur in etwa jeder zweite Betrieb mit weniger als zehn Mitarbeitern gibt an, seine gesicherten Daten auch regelmäßig zu überprüfen. Ein vollständiges Datensicherungskonzept beinhaltet die Überprüfung gesicherter Daten. Wird das Backup nicht regelmäßig auf Vollständigkeit und Wiederherstellbarkeit überprüft, kann im Fall des Verlusts der Originaldaten nicht gewährleistet werden, dass diese durch die Sicherung ersetzt werden können.

Innerhalb der Betriebsgrößenklasse von zehn bis unter 50 Mitarbeitern geben rund 36% an, ihre gesicherten Daten nicht regelmäßig zu prüfen. Deutlich stärker sensibilisiert scheinen die Betriebe ab 50 Mitarbeitern. Hier findet eine regelmäßige Überprüfung in gut 80% der Fälle statt. Zieht man zum Vergleich auch die großen Unternehmen mit mehr als 500 Mitarbeitern heran, werden die Unterschiede noch deutlicher. Gut 90% der Befragten aus dieser Gruppe geben an, ihre Backups regelmäßig zu prüfen (vgl. Abbildung 15).
Erkennbare Unterschiede zwischen den Betriebsgrößenklassen sind vorhanden und untermauern somit erneut die These der Bedeutung des Themas IT-Sicherheit bei ansteigender Betriebsgröße.
Betrachtet man die Betriebe mit weniger als 50 Mitarbeitern differenzierter, werden kaum Unterschiede deutlich. Der Anteil der regelmäßigen Überprüfung von gesicherten Daten liegt zwischen 55% und rund 66%, wobei ein leichter Anstieg mit zunehmender Betriebsgröße zu verzeichnen ist.
Dies zeigt erneut, dass insbesondere die Betriebe mit weniger als 50 Mitarbeitern als gefährdet zu betrachten sind und vertiefte Beratungsangebote zum Thema benötigen.

4.3.4 Passwörter und Zugriffsrechte

Beim Einsatz sicherer Passwörter verhält es sich ähnlich wie bei dem Themenkomplex Datensicherung. Mit steigender Anzahl an Mitarbeitern steigt auch die Nutzung sicherer Passwörter. Lediglich 45,9% der Betriebe mit weniger als zehn Mitarbeitern geben an, auf den ständigen Einsatz sicherer Passwörter zu achten. Bei den Betrieben von 10- 49 Mitarbeitern sind es 67,6% und in der Kategorie 50 und bis unter 500 Mitarbeitern bereits 78,1%. Im Vergleich hierzu schützen sich große Unternehmen deutlich besser. 86,7% der Befragten dieser Kategorie geben an, immer oder häufig sichere Passwörter zu verwenden(vgl. Abbildung 16). Zwar wurde im Fragebogen eine Definition sicherer Passwörter vorgegeben (vgl. Fußnote 5), trotzdem kann die subjektive Einschätzung der Befragten zum Thema Passwortsicherheit stark hiervon abweichen. Es kann somit davon ausgegangen werden, dass die tatsächliche Anwendung der Regeln zur Passwortsicherheit geringer ausfällt als in Abbildung 16 dargestellt.

> „In den meisten Fällen sind es die Namen von irgendwelchen Familienmitgliedern. Aber wissen Sie selber, alle 6 Wochen ein anderes Passwort vergeben, das macht keiner.“ (Interview 2, S.2)

Eine Möglichkeit, um Daten gegen unbefugte Zugriffe (auch betriebsintern) zu schützen, ist die differenzierte Vergabe von Zugriffsrechten. Je größer ein Unternehmen ist, desto mehr schränkt es die Zugriffsrechte für Mitarbeiter ein. Alle befragten Großunternehmen geben an, die Zugriffsrechte ihrer Mitarbeiter zu limitieren.

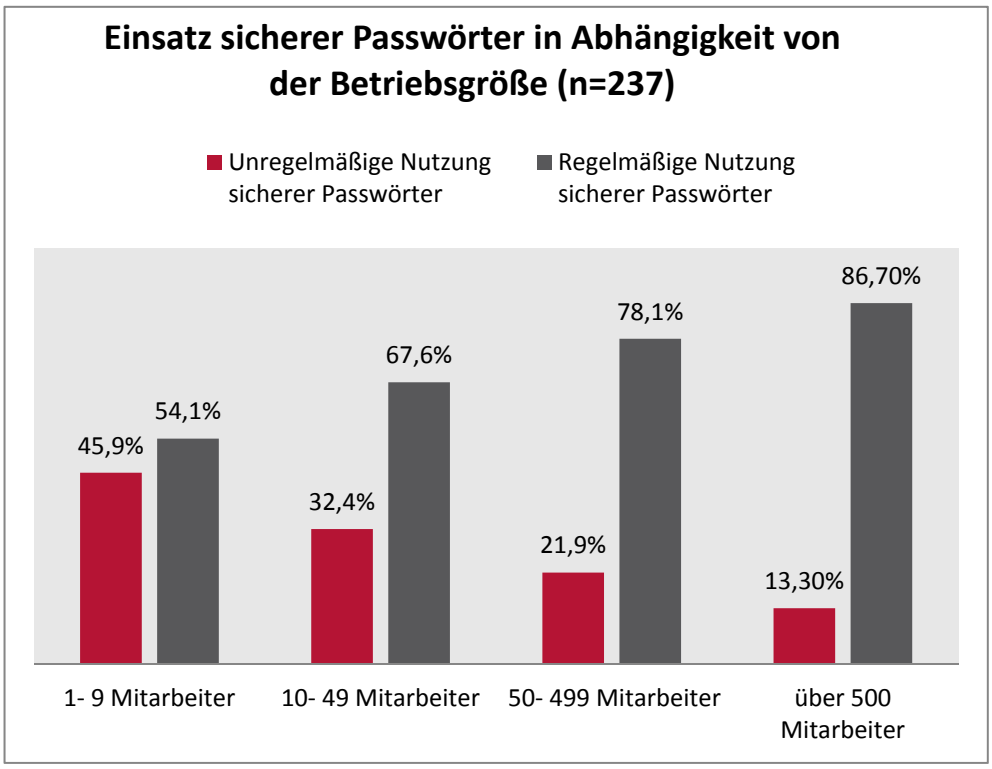


Abbildung 16: Einsatz sicherer Passwörter in Abhängigkeit von der Betriebsgröße

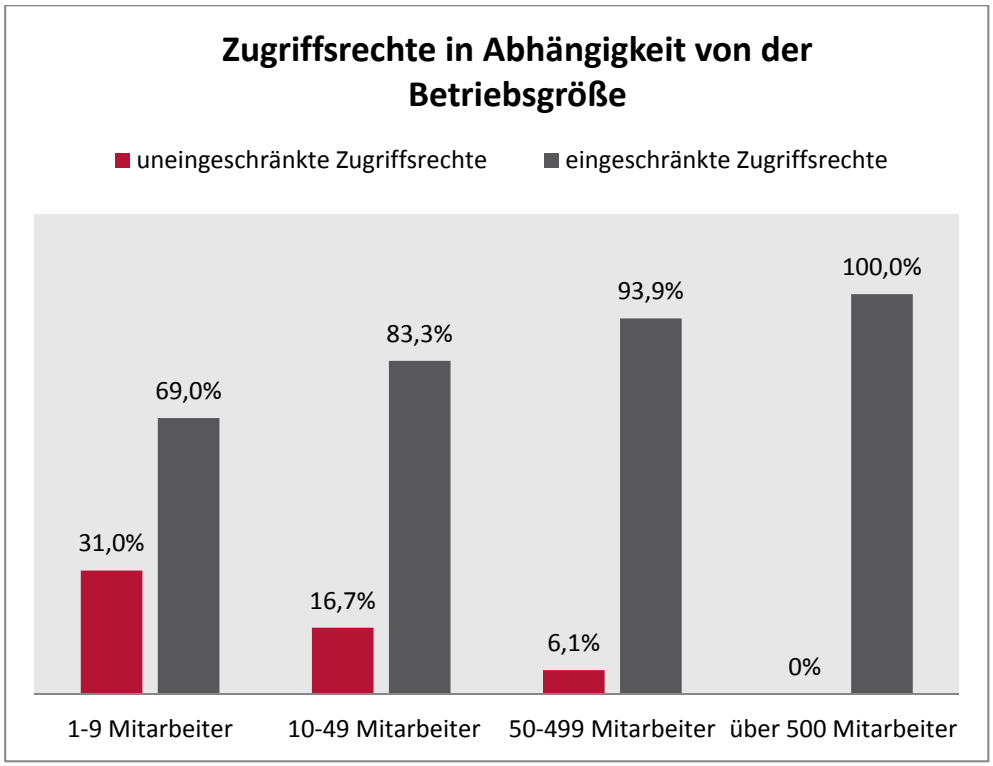


Abbildung 17: Zugriffsrechte in Abhängigkeit von der Betriebsgröße

Die mittleren Betriebe des Handwerks schränken in 93,9% der Fälle die Zugriffsrechte ihrer Mitarbeiter ein. Die Betriebe von 10- 49 Mitarbeitern erteilen in 83,3% der Fälle eingeschränkte Zugriffsrechte. Bei den Betrieben mit weniger als zehn Mitarbeitern sind es nur 69% (vgl. Abbildung 17). Es gibt einen deutlichen Zusammenhang zwischen der Einschränkung von Zugriffsrechten und der Betriebsgröße.

Betriebe mit weniger als 50 Mitarbeitern sollten aufgrund ihres akuten Gefährdundspotentials auf kostenlose Beratungen und Informations-veranstaltungen zurück greifen können.

„Das heißt, oft ist das so, dass alle volle Rechte haben am PC. Damit sind natürlich die Unternehmer letzten Endes gefährdet, weil die Unternehmerinnen oder die Ehefrauen, oder welche Mitarbeiter auch immer das sein mögen, nicht mit eigenen Benutzerkonten arbeiten, sondern meistens mit der Kennung des Chefs.“ (Interview 6, S.1f.)

Laut Einschätzung der befragten Experten werden die Möglichkeiten verschiedener Benutzerkonten und der dazugehörigen Rechte in den Betrieben des Handwerks kaum genutzt.

Es kann daher davon ausgegangen werden, dass auch die Daten in Abbildung 17 eine positivere Selbstbewertung der angewendeten Sicherheitsmaßnahmen im eigenen Betrieb darstellen, als die tatsächlichen Aktivitäten erlauben würden.

Insbesondere die Erfahrungen der Experten zeigen, dass auch in Bezug auf diesen Themenkomplex starker Sensibilisierungs- und Informationsbedarf besteht.

4.4 Selbsteinschätzung zum IT-Sicherheitsniveau

Im Folgenden wird die Selbsteinschätzung der befragten Betriebe zum Stand ihrer IT-Sicherheit dargestellt und deren Bedeutung innerhalb des Betriebs aufgezeigt.

4.4.1 Stellenwert der IT-Sicherheit im Betrieb

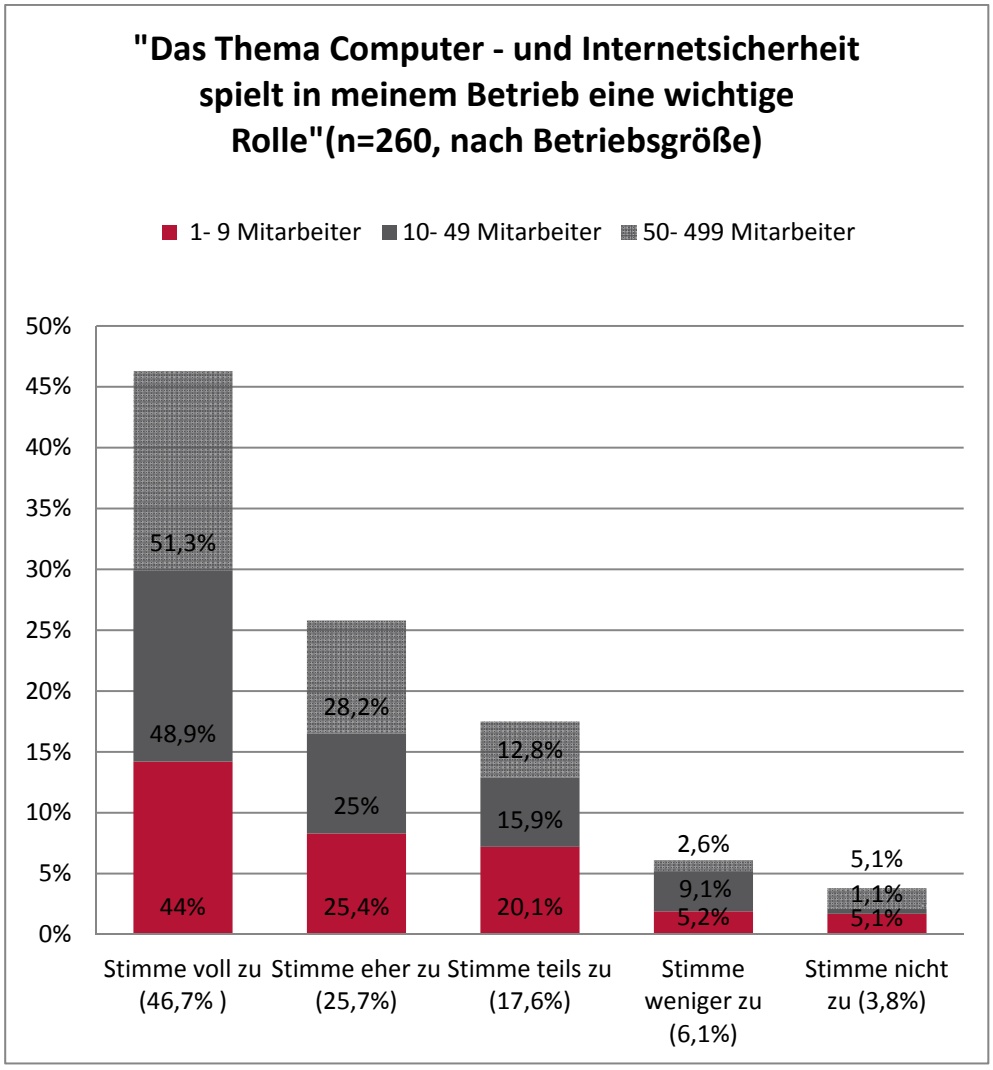


Abbildung 18: Zustimmung zur Aussage "Das Thema Computer - und Internetsicherheit spielt in meinem Betrieb eine wichtige Rolle" nach Betriebsgröße aufgeteilt.

Lesebeispiel: 44% der Betriebe mit weniger als zehn Mitarbeitern stimmen der Aussage voll zu. Insgesamt stimmen 46,7% der befragten Handwerksbetriebe der Aussage voll zu.

Es wird angenommen, dass mit steigender Mitarbeiteranzahl dem Thema IT-Sicherheit mehr Gewicht beigemessen sowie der Stand der Umsetzung von Sicherheitsmaßnahmen positiver beurteilt wird.
Die Zustimmung zur Aussage „Das Thema Computer- und Internetsicherheit spielt in meinem Betrieb eine wichtige Rolle“ steigt zwar in Abhängigkeit zur Betriebsgröße leicht an, ist jedoch auch insgesamt über alle Betriebsgrößenklassen hinweg sehr hoch (vgl. Abbildung 18).
Immerhin fast 70% der Befragten aus Kleinstbetrieben stimmen der Aussage voll oder eher zu. In der Betriebsgrößenklasse von 10 - 49 Mitarbeitern sind es knapp 74%, in den mittleren Betrieben fast 80%. Der Zusammenhang zwischen Unternehmensgröße und der attestierten Bedeutung des Themas IT-Sicherheit ist bei dem Vergleich der Betriebe mit weniger als 500 Mitarbeitern nur sehr gering. Werden das vorangegangene Kapitel und die darin aufgezeigten umgesetzten Aktivitäten betrachtet, wird deutlich, dass die in Abbildung 18 dargestellte Selbsteinschätzung der Betriebe positiver ausfällt als die Realität erlauben würde. Dies wird auch durch die Aussagen der Experten unterstrichen.

4.4.2 Verantwortungsbewusster Umgang mit der IT –Infrastruktur

„Und ansonsten haben sie dafür eigentlich gar keine Zeit. Weil sie sich damit noch nicht identifizieren können. Das ist für die halt alles schwarze Magie. Das ist ne Black -Box.“ (Interview 6, S.5)

„Das Thema ist nicht richtig greifbar für die. Da wissen sie zu wenig. So richtig interessiert es nicht, solange sie nicht betroffen sind davon Da muss man wirklich denen alles aus der Nase ziehen, was denn nun an Sicherheitsmaßnahmen überhaupt umgesetzt wird in den Firmen.“ (Interview 7, S.2)

Auch die Kompetenzen der eigenen Mitarbeiter in Bezug auf den Umgang mit Computer und Internet wird mit ansteigender Betriebsgröße positiver bewertet. Die Befragten aus Betrieben mit unter 10 Mitarbeitern stimmten der Aussage „Die Mitarbeiter in meinem Unternehmen sind im verantwortungsbewussten Umgang mit dem Computer und dem Internet geschult“ in nur 42,1% der Fälle zu. In Betrieben zwischen 10-

49 Mitarbeitern sind es 44,2%, in der Betriebsgrößenklasse von 50- 499 Mitarbeitern geben 48,7% der Befragten an, dass die Mitarbeiter ausreichend geschult sind (vgl. Abbildung 19).

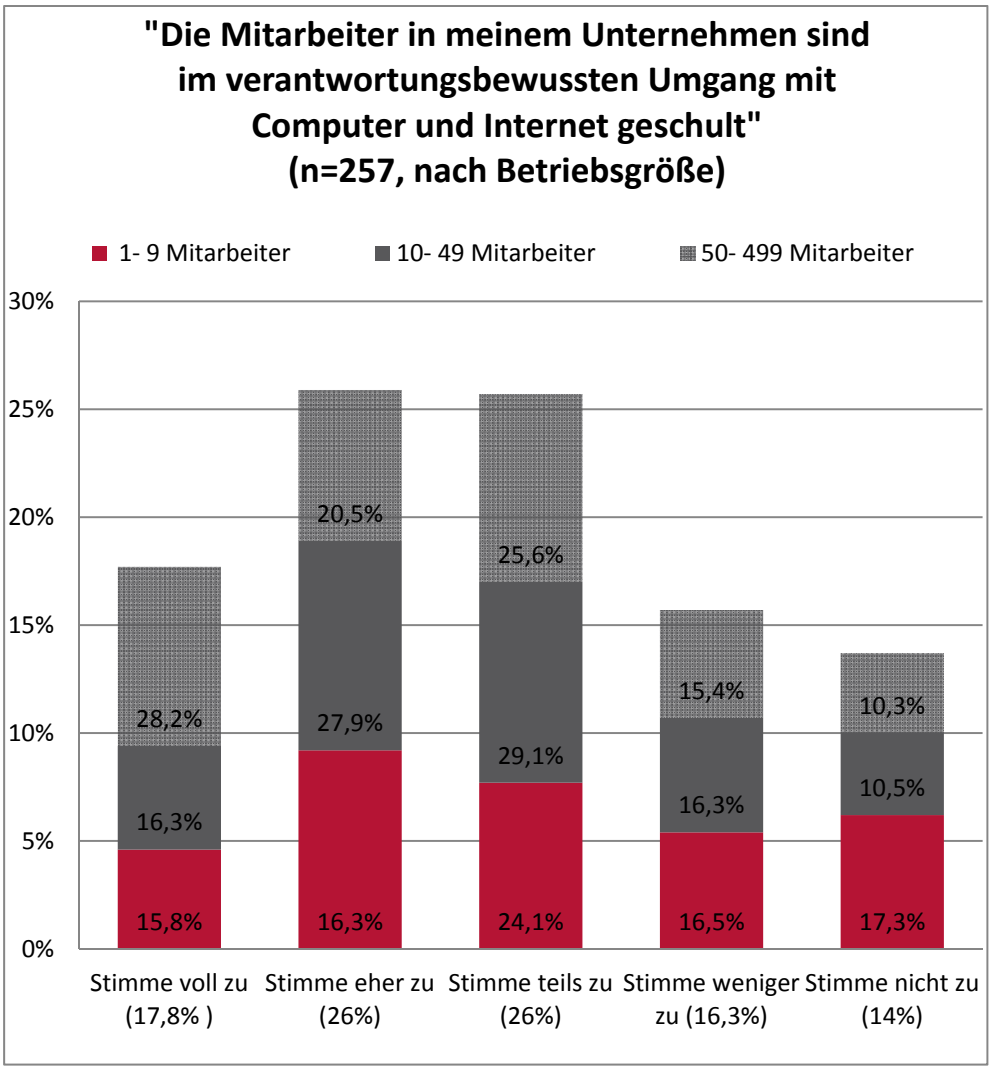


Abbildung 19: Zustimmung zur Aussage: "Die Mitarbeiter in meinem Unternehmen sind im verantwortungsbewussten Umgang mit Computer und Internet geschult."

Die Differenzen zwischen den drei Betriebsgrößenklassen sind nur geringfügig. Werden zum Vergleich die großen Unternehmen ab 500 Mitarbeitern betrachtet, werden starke Unterschiede deutlich. 80% der Befragten aus diesen Unternehmen stimmen voll oder eher zu, dass die Mitarbeiter im verantwortungsbewussten Umgang mit Internet und Computer geschult sind.

Betrachtet man ausschließlich die im Handwerk besonders relevanten Betriebe mit weniger als 500 Mitarbeitern, lässt sich festhalten, dass mehr als die Hälfte der Befragten der Aussage zum sensiblen Umgang der Mitarbeiter mit den betrieblichen Informations- und Kommunikationstechnologien nur teilweise bis gar nicht zustimmen. Hier besteht offenkundig noch zielgruppenspezifischer Sensibilisierungs- und Qualifizierungsbedarf. Neben einer Basisqualifizierung zur Nutzung des Internets sollte der Schwerpunkt auf der Einbindung externer Geräte (BYOD) und von Maschinen liegen.

4.4.3 Selbsteinschätzung zum Stand der IT-Sicherheit im eigenen Betrieb

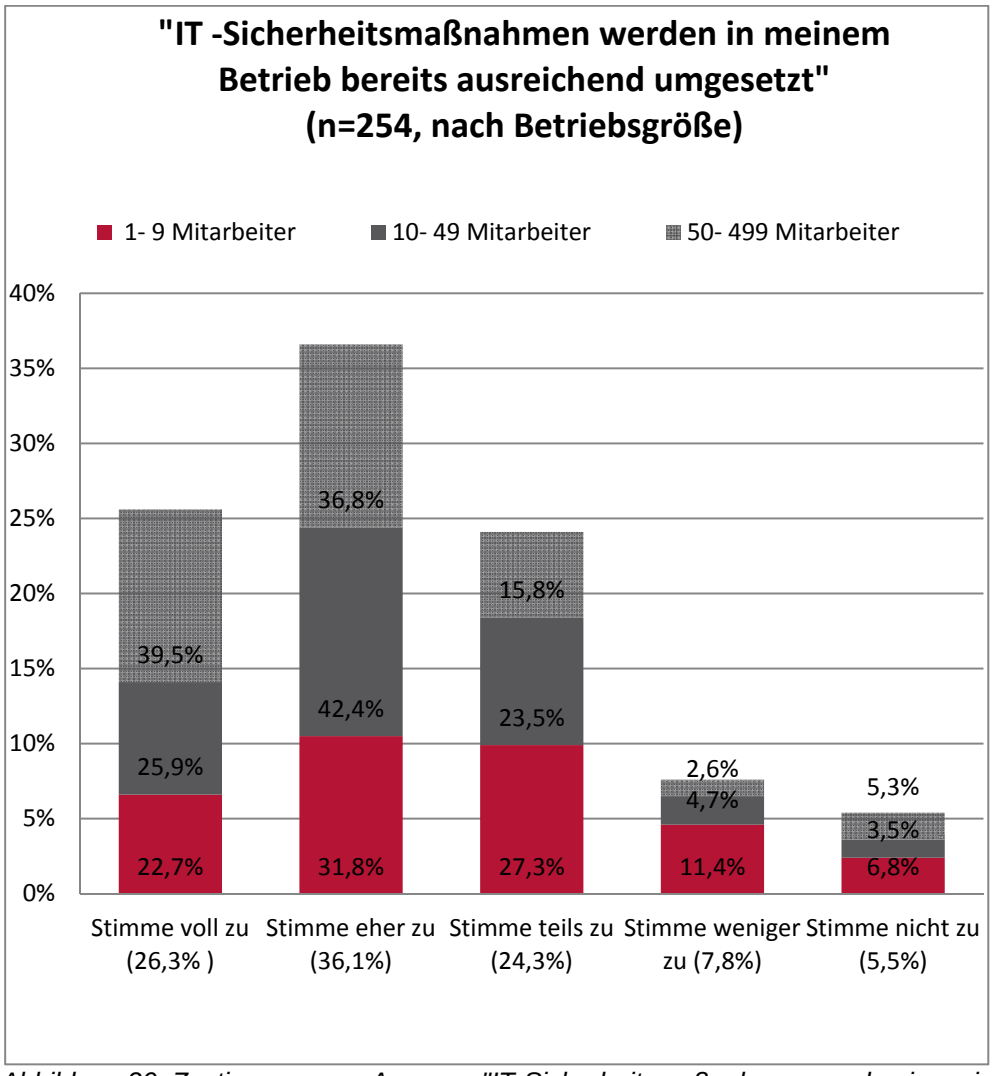


Abbildung 20: Zustimmung zur Aussage "IT-Sicherheitsmaßnahmen werden in meinem Betrieb bereits ausreichend umgesetzt" nach Betriebsgröße aufgeteilt

Inwieweit beurteilen die befragten Betriebe, die bei sich bestehenden Maßnahmen in Bezug auf das Thema IT-Sicherheit als ausreichend? Zur Klärung dieser Frage wurde die Zustimmung zur Aussage „IT-Sicherheitsmaßnahmen werden in meinem Betrieb bereits ausreichend umgesetzt“ abgefragt. Dieser Aussage stimmen rund 62% der Befragten voll oder eher zu. Nur rund 13% stimmen weniger oder gar nicht zu (vgl. Abbildung 20).

Es zeigt sich, dass die eigene IT-Infrastruktur als relativ sicher eingeschätzt wird. Betrachtet man jedoch die im vorherigen Kapitel aufgezeigten Sicherheitslücken und die Aussagen der Experten, wird der Nachholbedarf insbesondere in Betrieben mit weniger als 50 Mitarbeitern deutlich.

Die Einschätzung der Sicherheit der eigenen IT-Infrastruktur nimmt zwar nur leicht mit ansteigender Betriebsgröße zu, wie jedoch im vorherigen Kapitel dargestellt, wird die IT mit zunehmender Betriebsgröße tatsächlich besser geschützt. Man kann folglich festhalten, dass insbesondere die Betriebe ab 50 Mitarbeitern ihre IT-Sicherheitslage relativ realistisch einschätzen. Anders verhält es sich mit den Betrieben unter 50 Mitarbeitern. Diese überschätzen die Sicherheit ihrer IT-Infrastruktur. Knapp 55% der Betriebe mit weniger als 10 Mitarbeitern schätzen ihre IT als weitgehend sicher ein, innerhalb der Betriebsgrößenklasse von 10 - 49 Mitarbeitern sind es 68,3%. Im Vergleich zu den tatsächlichen Aktivitäten zeigen sich hier noch Diskrepanzen, die durch tiefergehende Sensibilisierungen aufgehoben werden müssen.

„Außer dem Virenscanner haben die nichts drauf. Und die einzige Firewall ist quasi die Firewall im Router des Providers.“ (Interview 1, S.2)

„Eine Firewall und ein Anti -Viren Programm, kann man eigentlich sagen, haben so ziemlich alle. Die Frage ist nur wie man damit umgeht. Was viele nicht kennen, sind die Sicherheitsupdates von Windows.“ (Interview 6, S.1)

„Es muss im Handwerk auch wehtun. Die Wenigsten nehmen bestimmte Risiken so richtig wahr.“ (Interview 7, S.3)

4.4.4 Bedarf an Beratungsleistungen nach eigenen Angaben

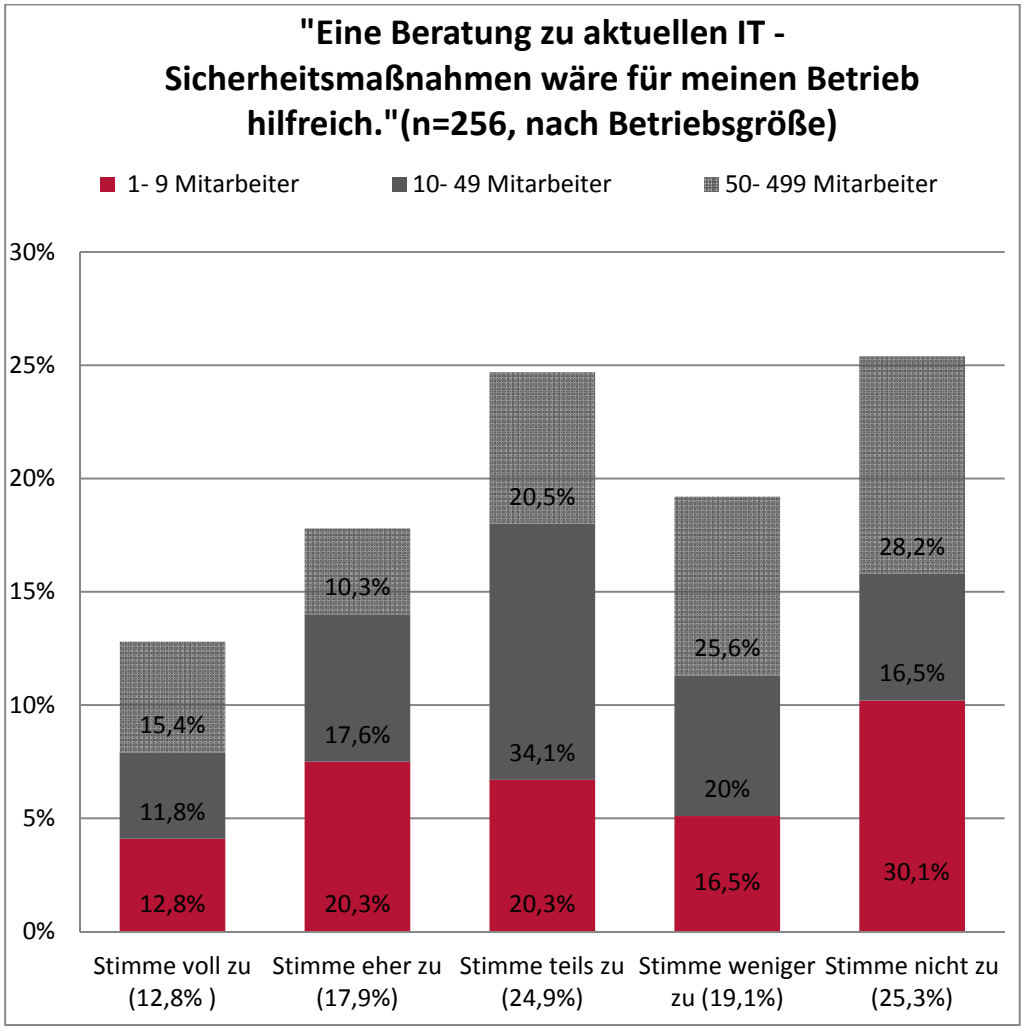


Abbildung 21: Zustimmung zur Aussage: "Eine Beratung zu aktuellen IT-Sicherheitsmaßnahmen wäre für meinen Betrieb hilfreich."

Nur knapp ein Drittel der Betriebe hält eine Beratung zum Thema IT-Sicherheit für hilfreich. Gut 46% aller Befragten stimmen der Aussage, dass eine Beratung hilfreiche wäre, weniger oder sogar gar nicht zu. Eher unentschlossen sind rund ⅕ der Befragten.

Von den befragten Betrieben mit 1 - 9 Mitarbeitern hält nur gut ⅓ eine Hilfestellung für vollständig oder eher sinnvoll. Der größte Anteil (46,5%) stimmt der Aussage weniger oder nicht zu und sieht dementsprechend Beratungen zum Thema nicht als hilfreich an.

Der Vergleich zwischen den Betriebsgrößenklassen lässt keine deutlichen Tendenzen erkennen. Alle Betriebe neigen eher dazu, eine Beratung als nicht sinnhaft einzuordnen. Die mittlere Kategorie von 10 - 49 Mitarbeitern ist jedoch mit 34,1% eher unentschlossen. Besonders negativ fällt die Bewertung der Betriebe von 50 bis 499 Mitarbeitern aus (vgl. Abbildung 21). Dies verwundert weniger, da diese Betriebe ihre aktuelle Sicherheitslage besonders positiv einschätzen und somit weniger auf externe Hilfestellungen angewiesen sind.
Obwohl die kleineren Betriebe weitreichende Defizite in puncto IT-Sicherheit haben, besteht noch wenig Interesse an einer Hilfestellung zu aktuellen Problemstellungen.

„Die haben das Bewusstsein nicht. Die meinen keiner will etwas von ihnen und bei denen sei doch noch nichts passiert. Die haben das nur nicht mitbekommen. Wir haben ja mal ne Zeit lang kostenlos Seminare angeboten, theoretisch müssten die einem die Bude einrennen. Machen die aber nicht.“ (Interview 1, S.5)

„Das Thema IT-Sicherheit ist im Handwerk kein beliebtes Thema, kein Massenthema, das heißt wenn ich das Thema IT-Sicherheit hab, dann sind die Besucherzahlen oder die Teilnehmerzahlen eher begrenzt. IT-Sicherheit wird ziemlich Stiefmütterlich behandelt.“ (Interview 3, S.1)

5. Fazit

„Und IT-Sicherheit brennt in der Regel in dieser Phase noch nicht, außer man hat da halt mal nen Schaden, dann wird‘s zum aktuellen Thema.“ (Interview 8, S.3)

„Die haben dafür eigentlich gar keine Zeit. Weil sie sich damit noch nicht identifizieren können. Das ist für die halt alles schwarze Magie. Das ist ne Black -Box..“ (Interview 6, S.5)

Abschließend kann festgehalten werden, dass die Betriebsgröße das ausschlaggebende Differenzierungskriterium in Bezug auf den Stand der IT-Sicherheit ist: Nicht nur bei der Selbsteinschätzung des Stands der IT-Sicherheit im eigenen Betrieb, sondern auch bei den tatsächlich umgesetzten Aktivitäten zur Herstellung einer sicheren IT zeigen sich in einigen Bereichen große Differenzen. So wird sowohl die Datensicherung als auch die Überprüfung gesicherter Daten sowie die Nutzung sicherer Passwörter mit steigender Mitarbeiteranzahl regelmäßiger durchgeführt.

Die Umfrage hat insgesamt gezeigt, dass insbesondere in den kleineren Betrieben mit unter 50 Mitarbeitern die Aktivitäten zur Herstellung einer sicheren IT-Infrastruktur ausbaufähig sind und weitreichender Sensibilisierungsbedarf besteht. Es wird jedoch auch deutlich, dass die generelle Bedeutung des Themas IT-Sicherheit noch nicht im Handwerk angekommen ist. Somit besteht die Herausforderung, die Sinnhaftigkeit von Beratungsleistungen an die Betriebe zu vermitteln, um sie für das Thema zu sensibilisieren.

6. Ausblick

Um den betrieblichen Gegebenheiten Rechnung zu tragen, soll mit handhabbaren Mitteln ein ausreichender Schutz der vorhandenen IT hergestellt werden. Hierbei sind die Betriebe des Handwerks grundlegend für die Risiken von Informationstechnologien zu sensibilisieren und bei der Herstellung eines Basisschutzes zu unterstützen. Ziel ist es, in allen erreichten Betrieben einen Schutz herzustellen, der alle grundlegenden Bereiche wie Browsersicherheiten, Virenschutz, den verantwortungsbewussten Umgang mit sozialen Medien sowie die Kommunikation über E-Mail etc. umfasst. Um hierbei die Bedürfnisse der einzelnen Betriebe zu berücksichtigen, kann bei einer grundlegenden Aufklärung auf die in Abbildung 23 dargestellte Themen zurückgegriffen werden, die sowohl die wichtigsten Sicherheitslücken, als auch die für die unterschiedlichen Betriebsgrößenklassen relevanten Themenschwerpunkte aufgreift.

Aufbauend sollen Betriebe, die über Netzwerk und Serverstrukturen verfügen, zu notwendigen Sicherheitsmaßnahmen informiert werden, die Möglichkeiten zum Schutz bieten. Darüber hinaus ist, wenn nötig, zu Themen wie Mobile Security (BYOD), Cloud-Computing oder VoIP zu informieren.
Mögliche Chancen, die mit der Nutzung des Cloud-Computing einhergehen wurden bereits in Kapitel 3.2 dargestellt. Zwar macht bisher nur ein geringer Teil der Handwerksbetriebe von diesen Möglichkeiten Gebrauch, die zukünftige verstärkte Anwendung ist aber auch laut den Aussagen der befragten Experten zu erwarten. Insbesondere im Zusammenhang mit der vermehrten Verwendung mobiler Endgeräte im Handwerk wird die Bedeutung des Cloud-Computing in der Zukunft ansteigen. Hierbei birgt auch der Bereich BYOD (Bring your own device) ein potenzielles Handlungsfeld. BYOD bezeichnet die Nutzung privater, mobiler Endgeräte wie Tablet- PCs oder Smartphones im Geschäftsall-

tag. Neben den Chancen (Kostenersparnis, Flexibilität) birgt dieser Trend jedoch auch Risiken: Da mittels dieser mobilen Endgeräte durch den Zugriff auf das betriebliche Netzwerk oftmals betriebsinterne Daten gespeichert und verarbeitet werden, müssen hier auch die im Unternehmensnetzwerk gültigen Bestimmungen und Sicherheitsrichtlinien Anwendung finden. Gerade kleine und mittlere Unternehmen haben in diesem Bereich ein noch nicht ausreichend ausgebildetes Problembewusstsein: Laut einer Studie des IT-Dienstleisters Datagroup verfügt ein großer Teil der kleinen Unternehmen über keine Konzepte zum Umgang mit privaten mobilen Endgeräten (vgl. www.datagroup.de). Oftmals werden auch die Risiken von BYOD nicht wahrgenommen. Hier besteht neben dem Sensibilisierungsbedarf auch eine Notwendigkeit spezieller, auf die Charakteristika von Handwerksbetrieben ausgerichteter Konzepte, die die strukturellen Besonderheiten der Zielgruppe berücksichtigen und adäquat durch geeignete Kanäle vermittelt und ggf. auch im Betrieb implementiert werden müssen.

Auch das sogenannte „Voice over Internet Protocol“ (kurz VoIP) hat für kleine und mittelständische Unternehmen große Vorteile und muss daher Gegenstand der Veranstaltungen rund um das Thema IT-Sicherheit werden. Durch die Nutzung des Internetzugangs für Telefongespräche können sich Unternehmen die Kosten für einen herkömmlichen Festnetzanschluss sparen und auch die Flexibilität erhöhen, unter anderem weil Rufnummern unabhängig von Standorten genutzt werden können. Es ist zu beachten, dass bei VoIP das Internet als gemeinsam genutzter Kanal für die Übertragung der Gesprächsdaten verwendet wird. Aus diesem Grund ist es essenziell, dass bei einer Entscheidung für VoIP die IT-Sicherheitsmaßnahmen im Fokus stehen. Ziel sollte es sein, dass Gespräche nicht durch einen unbekannten Dritten abgehört werden können. Dies müssen VoIP-Anbieter mittels adäquaten Verschlüsselungsmechanismen gewährleisten. In der Praxis nutzen kleinere Betriebe häufig einen softwarebasierten VoIP- Dienst. Größere Unternehmen verwenden hingegen sogenannte VoIP- Gateways, auf denen sich alle Mitarbeiter von unterwegs aus mit einer Software oder unternehmensintern mit einem VoIP- fähigen Telefon verbinden können. Bei der

Auswahl eines VoIP- Anbieters sollten Verantwortliche darauf achten, dass eine Gesprächsverschlüsselung angeboten wird. Beispiele hierfür sind das sogenannte „Virtual Private Network“ (kurz VPN) oder ein „SSL/TLS“ -gestützter Verschlüsselungsmechanismus. Letzteres beschreibt zwei Verschlüsselungsstandards, welche beispielsweise zum Schutz vor unberechtigtem Zugriff auf private Daten durch Dritte dienen.

Einzelne Betriebe, deren Maschinen über ihre IT gesteuert werden oder die mit sogenannten kritischen Infrastrukturen (vgl. folgenden Absatz) in Berührung kommen, müssen auf vertiefendem Level über Sicherheitsmaßnahmen und den sensiblen Umgang mit diesen Strukturen geschult werden (vgl. Abbildung 22).

Heizungs- und Alarmanlagen, Aufzugsteuerungen und die Gebäudeleittechnik bis hin zu Großanlagen sind mittlerweile über das Internet erreichbar. Diese werden von Handwerksbetrieben installiert, konfiguriert und gewartet. Schon die Tatsache, dass die Anlagen direkt über das Internet erreichbar sind, stellt ein Problem dar, ebenso wie die Gegebenheit, dass derartige Embedded-Server selten mit Sicherheits-Patches versorgt werden.

Durch unberechtigte Zugriffe bestehen u.a. Manipulationsmöglichkeiten der Betriebsparameter von Wärmenetzen, Heizzentralen und Feuerungsanlagen, die zu Ausfällen und Zerstörung der Systeme führen können.

Handwerksbetrieben, die im „Haus der Zukunft“ bzw. an kritischen Infrastrukturen arbeiten, müssen künftig in der Lage sein, durch Einhaltung von Mindeststandards solche Systeme sicher zu konfigurieren, Schwachstellen zu erkennen und zu vermeiden, damit die Sicherheit informationstechnischer Systeme erhöht wird.

Alle Sensibilisierungsmaßnahmen, ob es um Basisinformationen, problemgerichtete Beratungen bestimmter Betriebe oder die Aufklärung zu den Gefahren eingerichteter Infrastrukturen geht, können am effektivsten von bereits etablierten Beratern durchgeführt werden, die sich die Betriebszugänge bereits erschlossen haben.

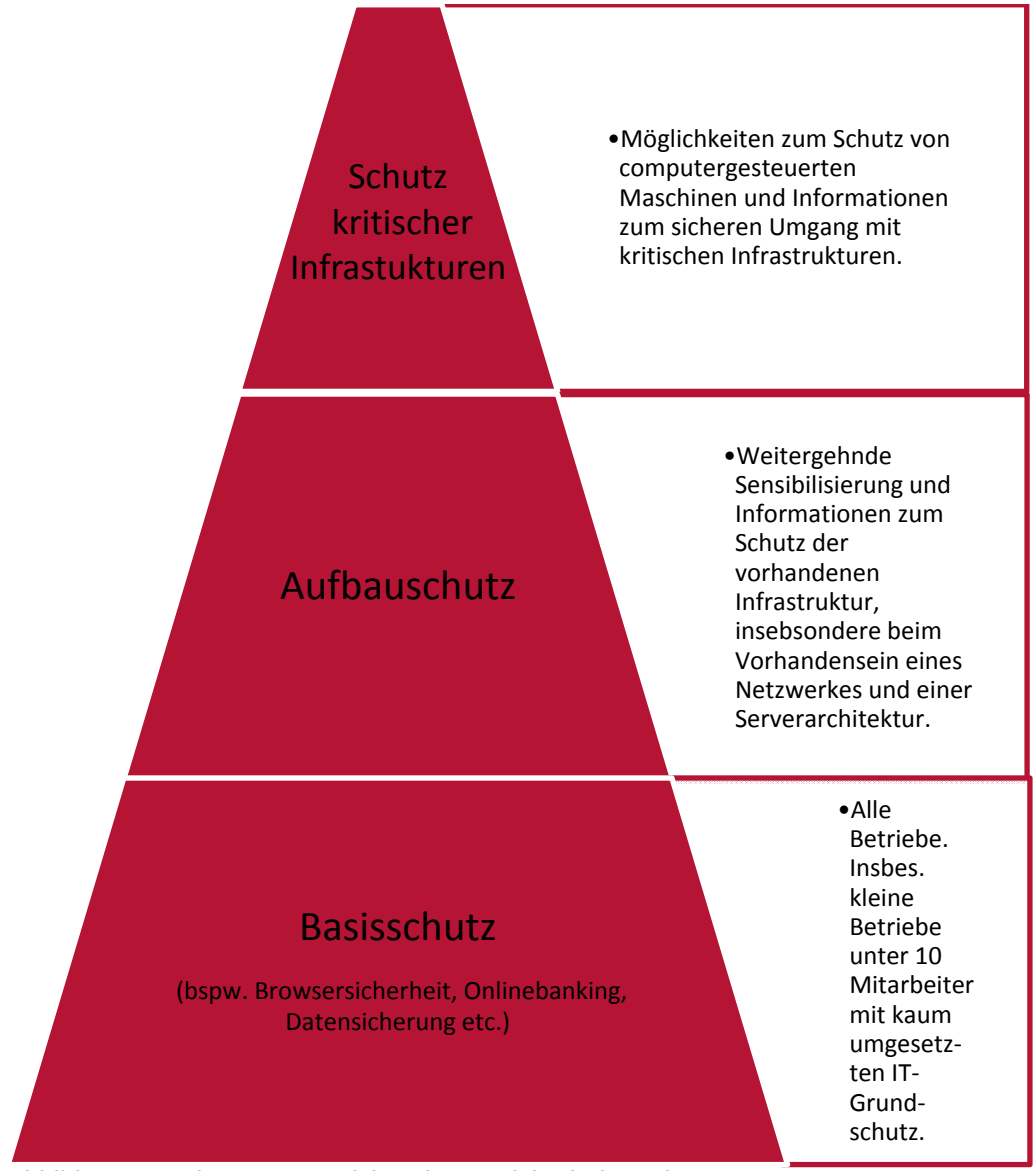


Abbildung 22: Cluster zu erreichender IT-Sicherheitsstufen

Cluster	TOP 3 Risiken	Sicherheitslücken
1-5 Mitarbeiter	1.Schadprogramme	stark gefährdet: Keine regelmäßige Datensicherung
	2.Onlinebanking	keine regelmäßige Überprüfung gesicherter Daten
	3. Probleme durch Spam	knapp 50% unsichere Passwörter
5-9 Mitarbeiter	1.Onlinebanking	stark gefährdet: Keine regelmäßige Datensicherung
	2.Schadprogramme	keine regelmäßige Überprüfung gesicherter Daten
	3.Probleme durch Spam	knapp 50% unsichere Passwörter
10-19 Mitarbeiter	1.Schadprogramme	gefährdet: nicht immer regelmäßige Datensicherung
	2.Probleme durch Spam	keine regelmäßige Überprüfung gesicherter Daten
	3.Datenmanipulation oder Verlust von Daten	1/3 unsichere Passwörter
20-49 Mitarbeiter	1.Probleme durch Spam	gefährdet: nicht immer regelmäßige Datensicherung
	2.Datenmanipulation oder Verlust von Daten	keine regelmäßgie Überprüfung, gesicherter Daten 1/3 unsichere Passwörter
	3.Schadprogramme	

Abbildung 23: Themen für den Basisschutz besonders gefährdeter Betriebsgrößen-klassen

7. Glossar

Adobe Flash	Ein Programm, welches unter Anderem die Darstellung interaktiver Inhalte ermöglicht.
Backups	Die Sicherung der Daten eines Computers, in der Regel auf externen Datenträgern.
Branchensoftware	Computerprogramme, die auf bestimmte Unternehmen in einer Branche abgestimmt sind. Zum Beispiel gibt es speziell für Handwerksbetriebe optimierte Software.
BYOD	(kurz für: Bring your own device) steht für die Nutzung privater Geräte zu dienstlichen Zwecken.
Client	Beschreibt die Verteilung von Aufgaben und Dienstleistungen innerhalb eines Netzwerks. Hierbei kommunizieren Client und Server miteinander. Der Client fordert vom Server Dienste an, der Server stellt diese bereit.
DECT	Standard für Schnurlostelefone.
Firewall	Schranke zwischen dem zu schützenden und dem unsicheren Netz. Kontrolliert den Datenverkehr zwischen den Netzen, erkennt Angriffe aus Netzen und wehrt diese ab.

Hardware	Mechanische und elektronische Komponenten eines Systems (bspw. Laufwerke, Festplatte, Drucker und Tastatur).
Java	Plattformunabhängig Programmiersprache. Viele Anwendungen und Websites können nur vollständig geladen werden, sofern die Java-Laufzeitumgebung (JRE) installiert wurde
Malware	Oberbegriff für Schadprogramme wie Viren, Würmer und Trojaner, welche entwickelt wurden, um nicht erwünschte und/ oder funktionsschädigende Folgen bei einem IT-Endgerät zu bewirken. Angreifer nutzen Software-Schwachstellen z. B. zum Auslesen von Informationen oder zur Spam-Verteilung aus.
Nutzungsrechte	Befugnis für eine Person, auf die für sie vorgesehenen internen Daten oder Programme zugreifen zu können.
Restore -Test	Testlauf, um herauszufinden, ob die Datensicherung erfolgreich war und wie lange die Wiederherstellung einzelner Daten dauert.
Sicherheitsupdate	Sicherheitsrelevante Produktaktualisierung für Anwendungsprogramme, Betriebssystem und spezielle Sicherheitssoftware.

Smartphone	Mobilfunkgerät, das die Funktionen von Handcomputern (PDA) und Handys miteinander verknüpft.
Spam	Unverlangt zugesandte E-Mails, häufig genutzt für Werbezwecke oder zur Verbreitung von Malware.
Software	Gegenteil von Hardware. Alle ausführbaren Programme werden als Software bezeichnet.
Server	Rechner, der den anderen Rechnern seines Netzes Informationen und Dienste zur Verfügung stellt.
Trojaner	(Kurz für: Trojanisches Pferd.) Unerwünschtes Programm, welches zur Familie der Malware gehört und verborgene Funktionalitäten besitzt, die dem Anwender nicht bekannt sind.
Update	Produktaktualisierung
Virus	Schädliches Computerprogramm aus der Familie der Malware, welches sich unbemerkt in andere Programme kopieren kann und zu einem definierten Zeitpunkt meist zerstörerische Aktivitäten ausführt.
Virenscanner	Programm zur Erkennung, Blockierung und Entfernung von Malware auf dem laufenden Betriebssystem. Regelmäßige Updates der Virensignatu-

	ren sind erforderlich, um auch neue Malware zu erkennen.
VoIP -Telefonie	Internet-Telefonie über Computer-netzwerke.
Zugriffsrechte/Zugangsrechte	Über Zugriffsrechte/Zugangsrechte kann unter anderem gesteuert wer-den, wer auf die gesamten Daten eines PCs oder Netzwerks zugreifen kann.
Peer to Peer	Peer-to-Peer, kurz: P2P, Architektur-Modell, in welchem alle Rechner gleichberechtigt verbunden sind, so-mit können alle Dienste gemeinsam zur Verfügung gestellt und genutzt werden.

8. Abbildungsverzeichnis

9. Literaturverzeichnis

Büllingen, Franz/Hillbrand, Annette (2012): IT-Sicherheitsniveau in kleinen und mittleren Unternehmen im Auftrag des Bundesministeriums für Wirtschaft und Technologie, Bad Honnef.

Brandl, Stefan/Böhme, Katrin (2012): IT-Sicherheitslage im Mittelstand 2012. Eine Studie von Deutschland sicher im Netz, Berlin.

Bundesamt für Sicherheit und Informationstechnik (2011): Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen. Grad der Sensibilisierung des Mittelstandes in Deutschland.

Bundesamt für Sicherheit und Informationstechnik (2012): Eckpunktepapier. Sicherheitsempfehlungen für Cloud Computing Anbieter. Mindestanforderungen in der Informationssicherheit.

Bundesministerium für Wirtschaft und Technologie (2010): Elektronischer Geschäftsverkehr in Mittelstand und Handwerk 2010. Ergebnisse einer Untersuchung des Netzwerks Elektronischer Geschäftsverkehr.

Feuerhake, Jörg (2012): Handwerkszählung 2008. In: WiSta 1/2012, S. 51 ff.

Günterberg, Brigitte/Wolter, Hans -Jürgen (2002): Unternehmensgrößenstatistik 2001/2002 –Daten und Fakten -. Hrsg. Institut für Mittelstandsforschung, Bonn.

Kasper, Harriet/Kett, Holger/Weisbecker, Anette (2012): Potentiale für Cloud Computing im Handwerk. Aktuelle IT -Unterstützung und Anforderungen an Internet -basierte IT -Lösungen, Fraunhofer Verlag, Stuttgart.

http://www.zdh-statistik.de/application/index.php?mID=3&cID=47
(Stand 13.05.2013)

www.datagroup.de/datagroup/uber -uns/news -events/news -details/article/datagroup -trendmonitor -2012 -kleine -und -mittlere -unternehmen -gehen -derzeit -noch -defensiv -mit -byod -um.html, (Stand 10.05.2013)

ISBN:978-3-944916-00-2