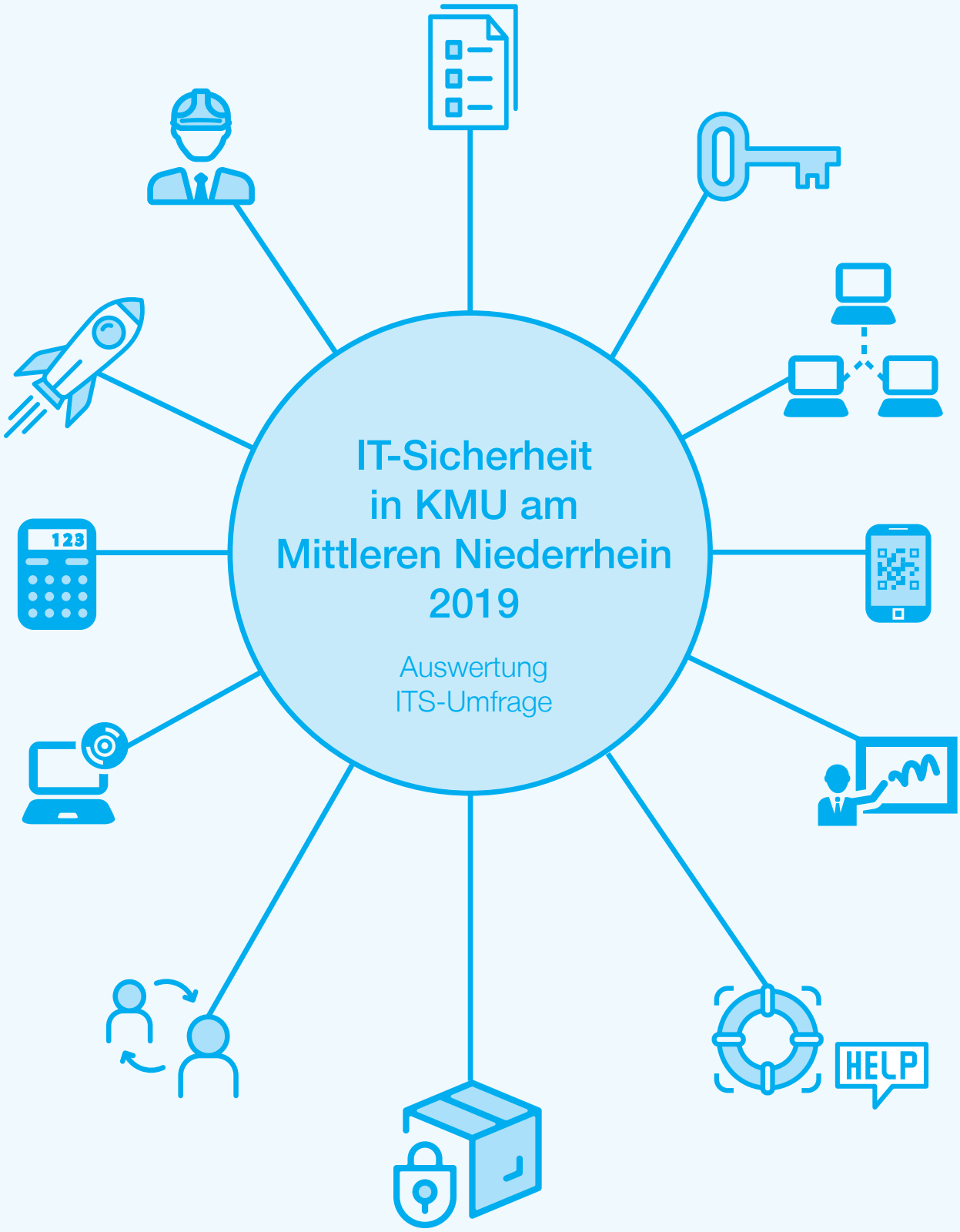

IT-Sicherheit in KMU am Mittleren Niederrhein 2019

Auswertung ITS-Umfrage

Durchgeführt von Kompetenzzentrum für Informationssicherheit der Hochschule Niederrhein Clavis

Hochschule Niederrhein
University of Applied Sciences

Mitwirkende:
Prof. Dr. René Treibert (Leitung Clavis)
M. Sc. Philipp Schütz (Projektleitung)
Nils Leyers
Jonas Heimann

Im Auftrag der:

IHK Industrie- und Handelskammer Mittlerer Niederrhein

Inhaltsverzeichnis

1 Einleitung

Mit zunehmenden Digitalisierungsgrad in den Unternehmen, steigen auch die Anforderungen an die IT-Sicherheit. Diese wird oft als reiner Kostenfaktor wahrgenommen und die langfristen Vorteile werden insbesondere von kleinen und mittleren Unternehmen nicht richtig wahrgenommen. Dabei spielt die Verfügbarkeit der Daten und der IT-Systeme für die meisten Unternehmen eine kritische Rolle. Längere Ausfälle können schnell zu erheblichen Einbußen führen oder sogar den Betrieb zum Erliegen bringen. Die hierbei entstehenden Kosten sind oft weit höher als die Ausgaben für entsprechende IT-Sicherheitsmaßnahmen. Zusätzlich gilt es sich den regulatorischen Anforderungen, z.B. im Umgang mit personenbezogen Daten, bewusst zu sein. Eine hohe Datenqualität z.B. von Kundenstammdaten hat einen nicht unerheblichen Einfluss auf den Wert der eigenen Unternehmung. Genau wie Kundendaten, gehört das Knowhow im Betrieb zu den besonders schützenswerten Informationen. Die IT-Sicherheit trägt dazu bei, dass diese Information vertraulich bleiben und leistet somit einen wichtigen Beitrag zum nachhaltigen Erfolg der Betriebe. Nicht zuletzt bei dem Thema Unternehmensnachfolge spielt die Datenqualität eine immer größere Rolle.

Die Industrie- und Handelskammer Mittlerer Niederrhein (nachfolgend „IHK“ genannt) hat die Herausforderungen und Chancen in Bezug auf IT-Sicherheit schon seit langen erkannt und will mit dieser Befragung zum einen den regionsbezogenen Status Quo in der IT-Sicherheit der kleinen und mittleren Unternehmen (nachfolgend „KMU“ und „KMUs“ genannt) erheben. Zum anderen soll den KMU durch Teilnahme an der Befragung eine Möglichkeit zur Selbstreflektion und Einordnung gegeben werden. Daher hat die IHK Mittlerer Niederrhein Clavis, das Kompetenzzentrum für Informationssicherheit der Hochschule Niederrhein, mit der Durchführung der Befragung beauftragt.

2 Ziele

Das Ziel dieser Studie ist die systematische Erkennung, Erfassung und Bewertung des aktuellen Sachstandes zum Thema IT-Sicherheit in der Region Mittlerer Niederrhein. Betrachtet werden KMUs aus der Region. Die Bereiche Umsetzungsstand, Bedarf und weitere Einflussgrößen der IT-Sicherheit stehen im Vordergrund der Untersuchung. Die Auswertung unserer Untersuchung soll es Unternehmen und besonders deren Entscheidern ermöglichen, ihr eigenes IT-Sicherheitsniveau mit anderen Unternehmen zu vergleichen. Weiter sollen sie dazu angeregt werden, die Relevanz und Bedeutung der vorgestellten und untersuchten Sicherheitsmaßnahmen für ihr Unternehmen bewerten und – falls zutreffend – die entsprechenden Maßnahmen umsetzen zu können. Ein Teilziel ist es zudem Unternehmen für das Thema IT-Sicherheit zu sensibilisieren und darauf aufmerksam zu machen. Da IT-Sicherheitsvorfälle im Extremfall die Existenz bedrohen können und nicht mehr nur große Unternehmen die Ziele von Cyber-Kriminellen sind, sollten sich gerade kleine und mittlere Unternehmen vor den Gefahren schützen.

3 Ergebnisse

In diesem Abschnitt sind die Ergebnisse der Studie zur Ermittlung des aktuellen Standes der IT-Sicherheit kleiner und mittlerer Unternehmen (KMUs) in der Region Mittlerer Niederrhein aufgeführt. Die Ergebnisse sind in die folgenden Kategorien unterteilt: Strukturdaten, Infrastruktur, Sicherheitskonzept, IT-Sicherheitsbeauftragter, Verschlüsselung, Mobilgeräte, Mitarbeitersensibilisierung, Datensicherung, Notfallbehandlung und Datenschutz. Im ersten Unterkapitel (Kapitel 3.1) wird auf Strukturdaten der Teilnehmer und deren Einschätzungen eingegangen. Die Ergebnisse der Kernbereiche der Studie werden in den nachfolgenden Kapiteln (Kapitel 3.2 bis 3.10) behandelt. Zusätzlich werden in Kapitel 4 zu den jeweiligen Abschnitten Handlungsempfehlungen für Unternehmen in der Region ausgesprochen.

3.1 Strukturdaten

Dieser Abschnitt thematisiert die befragten Unternehmen und den Stellenwert, der IT-Sicherheit zugeschrieben wird. Die insgesamt 115 befragten Unternehmen wurden in zwei Kategorien unterteilt. Die Unternehmen wurden in „kleine KMUs“ (1 – 49 Mitarbeiter) und „große und mittlere KMUs“ (50 – 499 Mitarbeiter)[1] zusammengefasst. Wird ein Vergleich der Angaben anhand dieser Unterteilung vorgenommen, wird dies in den Abbildungsbeschriftungen durch „gruppiert nach Größe“ gekennzeichnet. Die nachfolgenden Abbildungen veranschaulichen die Mitarbeiterzahlen, Branchen, Jahresumsätze und geplanten Investitionen in IT-Sicherheit der befragten Unternehmen.

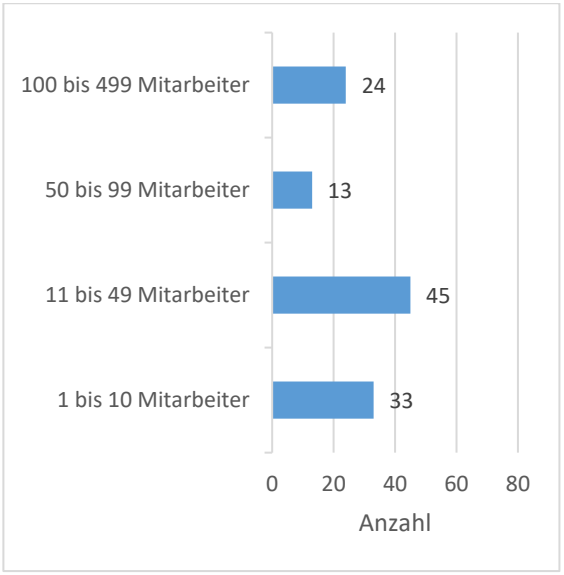

Abbildung 1: Mitarbeiteranzahl befragter Unternehmen

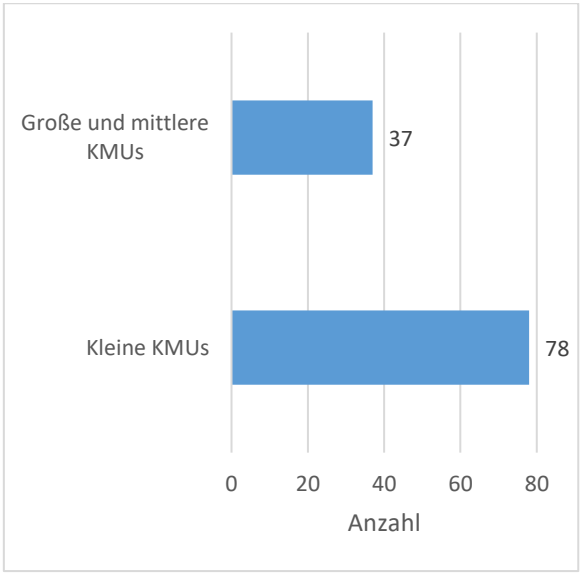

Abbildung 2: Verteilung der Größenkategorien

[1] Gruppierung der Unternehmensgrößen basierend auf der KMU-Definition des Instituts für Mittelstandsforschung (IfM) Bonn, Stand 2016.

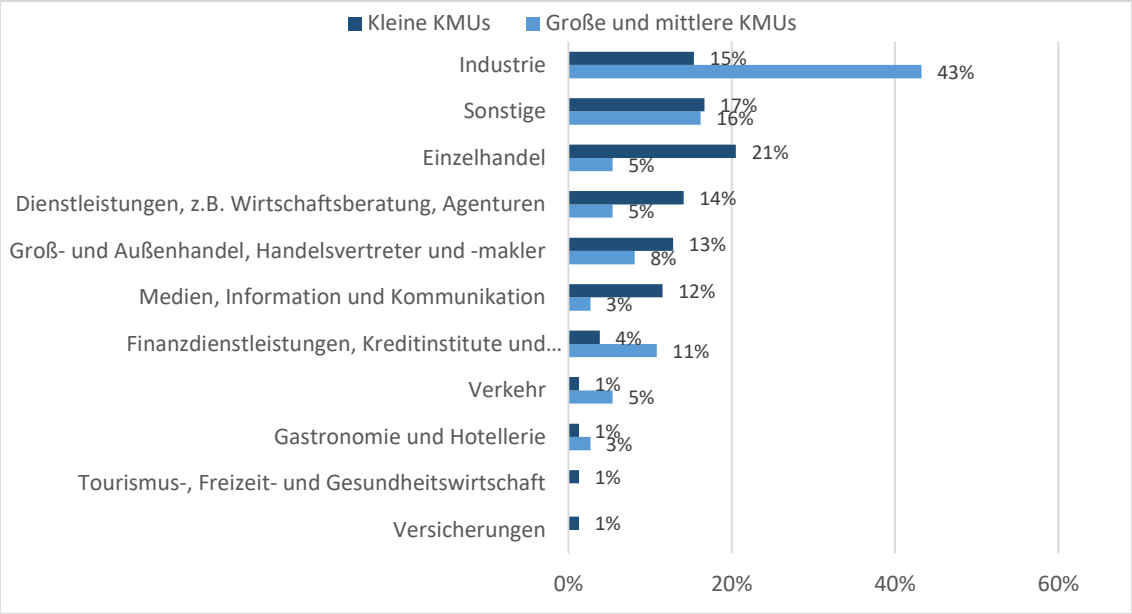

Abbildung 3: Branchenübersicht gruppiert nach Größe

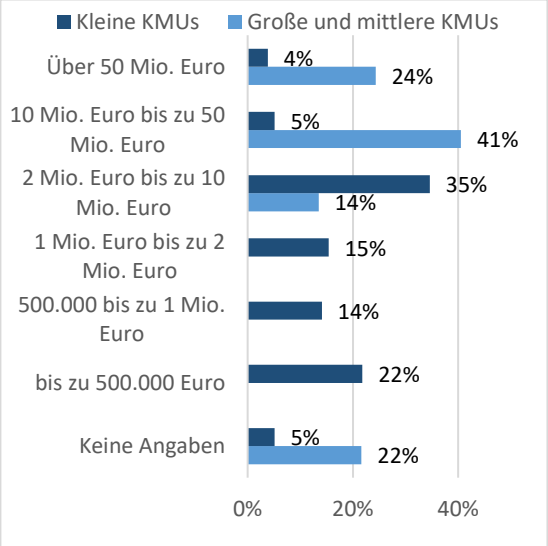

Abbildung 4: Jahresumsatz befragter Unternehmen gruppiert nach Größe

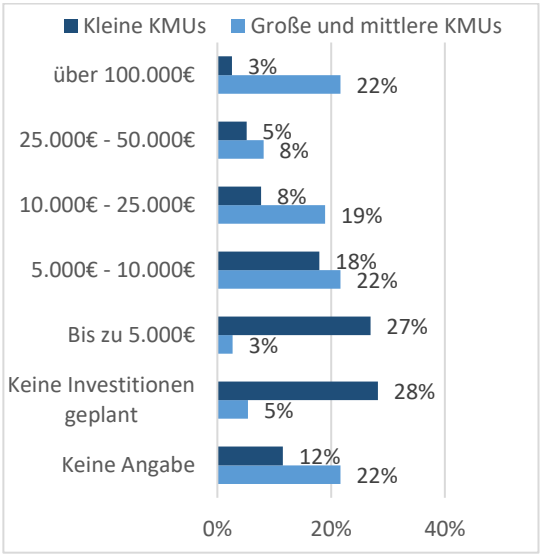

Abbildung 5: Geplante Investitionen in IT-Sicherheit gruppiert nach Größe

76%[2] der befragten Unternehmen gaben an, für das kommende Jahr Investitionen in IT-Sicherheit zu planen. Die in Unternehmen am häufigsten eingesetzte Informations- und Kommunikationstechnologie (kurz: „IKT“) sind PC-Arbeitsplätze mit Zugang zum Internet (96%) und mobile Endgeräte (86%), wie z.B. Laptops oder Smartphones. PC-Arbeitsplätze ohne Zugang zum Internet (17%) werden deutlich seltener eingesetzt.

Geräte mit Zugang zum Internet sind einer Vielzahl an Gefahren ausgesetzt und benötigen entsprechenden Schutz. Wird ein Gerät für Aufgaben eingesetzt, deren

[2] Unternehmen die keine Angaben machten wurden herausgerechnet und nicht berücksichtigt.

Erfüllung kein Internet benötigt, kann durch eine Abkapselung verhindert werden, dass Angreifer dieses als Eintrittstor in das Unternehmensnetzwerk nutzen.

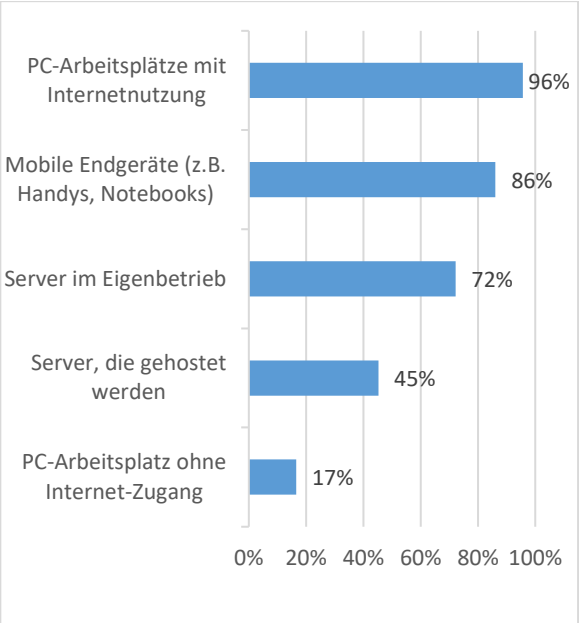

Abbildung 6: Eingesetzte IKT-Ausstattung

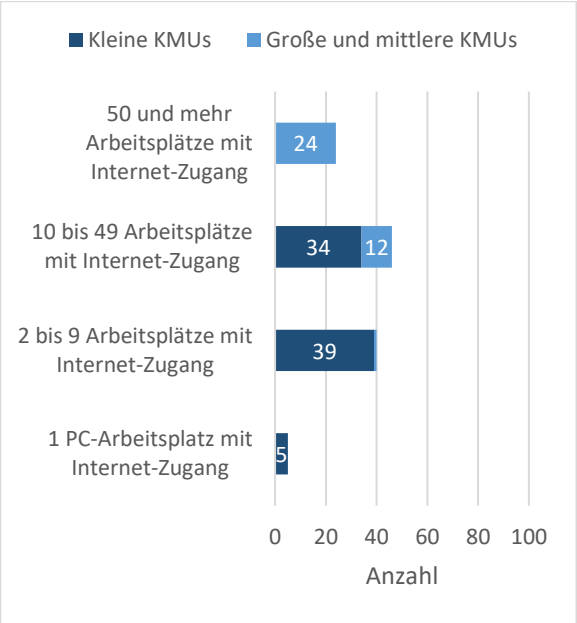

Abbildung 7: Einsatz von PCs gruppiert nach Größe

Die Unternehmen der Region betreiben ihre Server meistens selbst (72%), während durch externe Firmen gehostete Server in 45% der Unternehmen eingesetzt werden. Hybride Systeme aus Servern im Eigenbetrieb und extern gehosteten Server werden in 35% der Unternehmen eingesetzt. 17% setzen gar keine Server ein.

Tabelle 1: Verwendete Betriebsarten für Server

	Gehostete Server	*Keine gehosteten Server*	*Gesamt*
Keine Server im Eigenbetrieb	20	12	32
Server im Eigenbetrieb	43	40	83
Gesamt	63	52	115

Der Einsatz von Servern bringt verschiedene Vor- und Nachteile mit sich. Aus größeren Netzwerken sind sie jedoch nicht mehr wegzudenken. Server sind leistungsstarke Computer, die für andere Geräte (auch „Clients“ genannt) sowohl Daten als auch Anwendungen bereitstellen und verbundene Geräte verwalten können. Es gibt verschiedene Server-Typen, wie zum Beispiel Webserver, File-Server, Mailserver und Datenbankserver, die für spezielle Aufgaben eingesetzt werden. Die verschiedenen Server-Typen besitzen hinsichtlich der IT-Sicherheit verschiedene Vor- und Nachteile, da sie eine gewisse Angriffsfläche bieten, aber auch weiterführende IT-Sicherheitsmaßnahmen ermöglichen.

Beispiel: Ein zentraler File-Server kann alle für das Unternehmen relevanten Daten speichern, die dann in einer zentralen Datensicherung gespeichert und sicher aufbewahrt werden können. So können Daten im Fall eines Systemausfalls widerhergestellt und Stillstände vermieden werden. Gelangt ein Angreifer jedoch an eine

nicht-verschlüsselte Datensicherung, kann er die Daten des Unternehmens widerherstellen und stehlen.

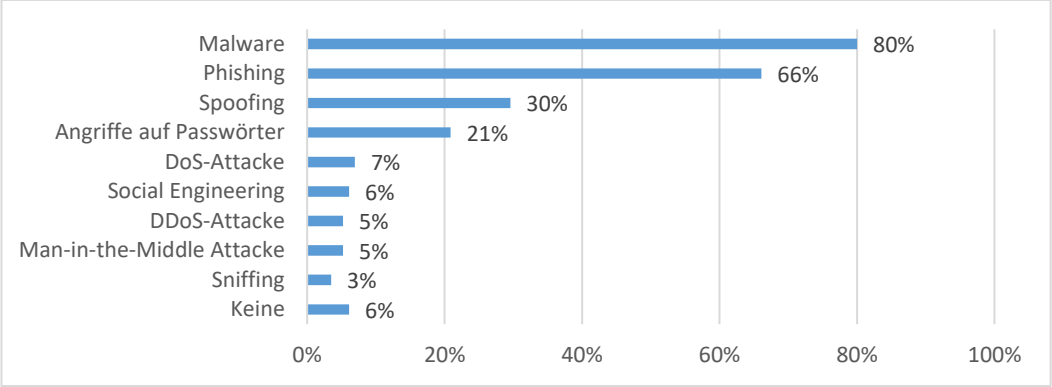

Abbildung 8: Erfahrung mit Cyber-Angriffen

Malware und Phishing sind die häufigsten Cyber-Angriffe, von denen Unternehmen bislang betroffen waren. Spoofing (Verschleierung der Identität, Vortäuschung anderer Identität) und Angriffe auf Passwörter sind weitere Angriffsarten, mit denen circa jedes vierte Unternehmen Erfahrung gemacht hat.

Nur weil ein Angriff nicht bemerkt wurde bedeutet es nicht, dass kein Angriff stattgefunden hat. Um mit der wachsenden Anzahl und dem wandelnden Vorgehen von Angreifern mithalten zu können sollten sich Unternehmen über „generelle Neuigkeiten“ aus dem Bereich IT-Sicherheit und insbesondere über neue Angriffsarten informieren. Für regelmäßige Informationen – beispielsweise als Newsletter – gibt es zahlreiche kostenlose und kostenpflichtige Anbieter im Internet. Erkennen kommt von kennen. Demnach gilt: Um die Gefahr erkennen zu können, sollte man die Gefahr kennen.

In der Region zeichnet sich bei den Unternehmen ein positives und einsichtiges Bild hinsichtlich des Verbesserungsbedarfs des IT-Sicherheitsniveaus. Insgesamt 82% sehen einen teilweisen bis starken Verbesserungsbedarf.

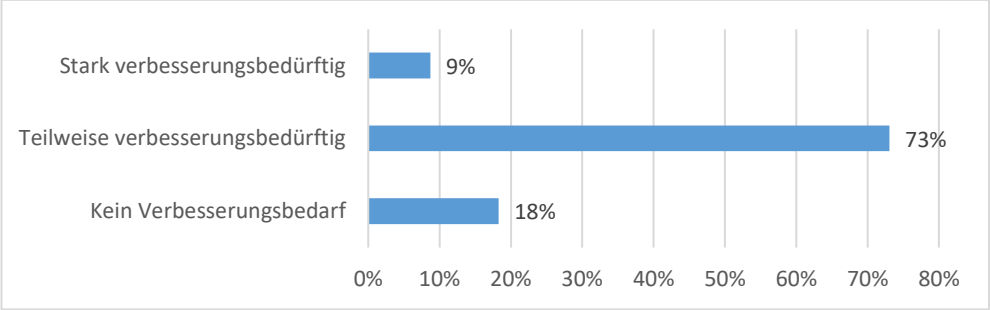

Abbildung 9: Einschätzung des Verbesserungsbedarfs des eigenen IT-Sicherheitsniveaus

Unternehmen, die diesen Bedarf nicht sehen, sollten prüfen ob ihre Sicherheitsmaßnahmen für aktuelle Sicherheitsrisiken ausreichend sind. Da IT-Sicherheitsvorfälle im Extremfall die Existenz des Unternehmens und seiner Angestellten gefährden können, ist eine generelle Unterlassung von Schutzmaßnahmen bedenklich.

Schutzmaßnahmen für IT-Systeme können mit den Funktionen von ESP (elektronisches Stabilitätsprogramm) und Airbags in Autos verglichen werden. Während die Einen verhindern, dass das Unternehmen ins Schleudern gerät, dämpfen Andere die Schwere im Schadensfall ab.

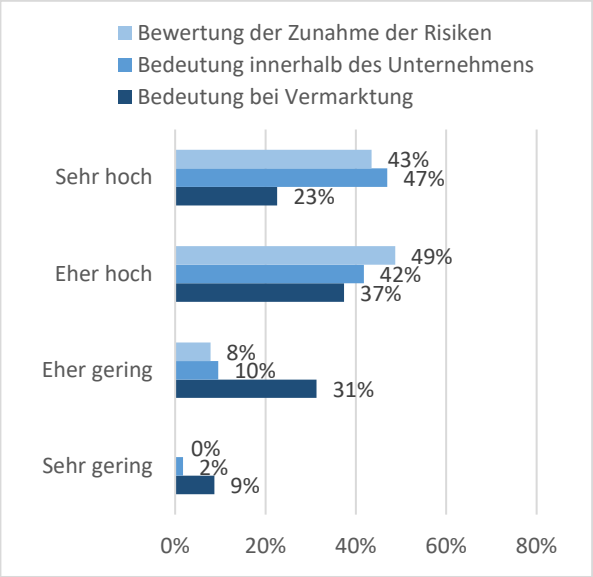

Abbildung 10: Bewertung der Informationssicherheit

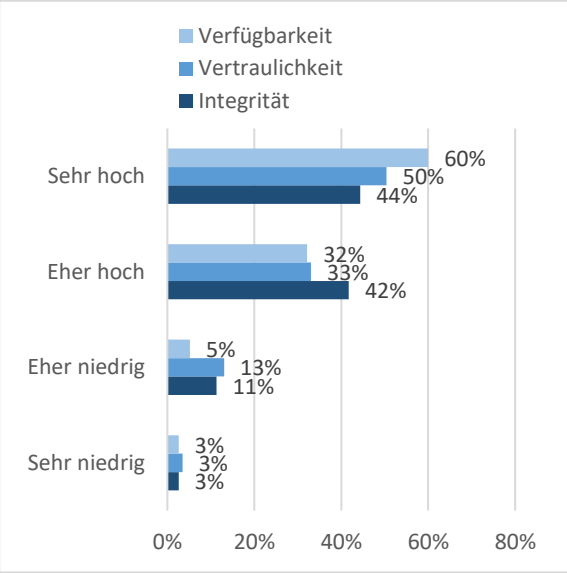

Abbildung 11: Bewertung des Schutzbedarfs hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität von Daten und IT

Neben dem individuellen Verbesserungsbedarf zeigt sich anhand der Bewertung von Informationssicherheit in diversen Bereichen der Unternehmen, dass die Notwendigkeit von Sicherheitsmaßnahmen von einem Großteil der Unternehmen erkannt wird. Über 80% der Unternehmen geben an, dass Informationssicherheit in ihrem Unternehmen einen eher hohen, bis sehr hohen Stellenwert hat. Weiter sind sich Unternehmen der Zunahme der Risiken bewusst. Die Zunahme wird ebenfalls als eher hoch bis sehr hoch bewertet.

Die Hauptursachen möglicher IT-Probleme sind für die befragten Unternehmen der Ausfall der Technik und eventuelle Fehler eigener Mitarbeiter. Große und mittlere KMUs sehen den Menschen als größte Problemquelle, während kleinere KMUs den Ausfall ihrer Technik problematischer bewerten. Unternehmen, die eigene Mitarbeiter als größte Problemquelle sehen, sollten umso mehr in die Sensibilisierungs- und Aufklärungsmaßnahmen investieren. Ohne entsprechende Maßnahmen wird sich das Verhalten der Mitarbeiter nicht ändern.

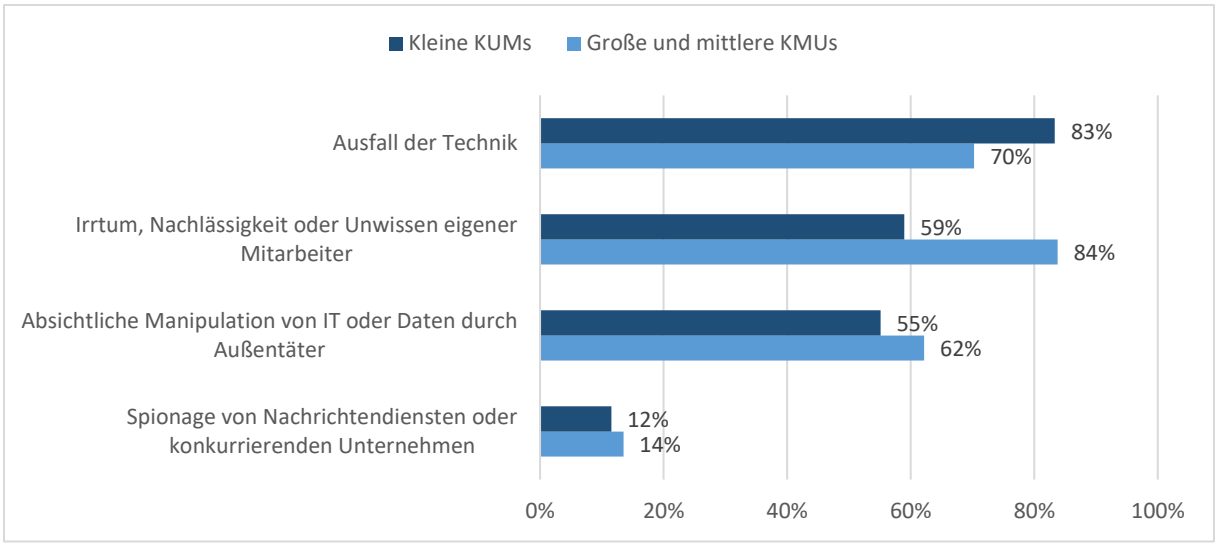

Abbildung 12: Hauptursachen möglicher IT-Probleme gruppiert nach Größe

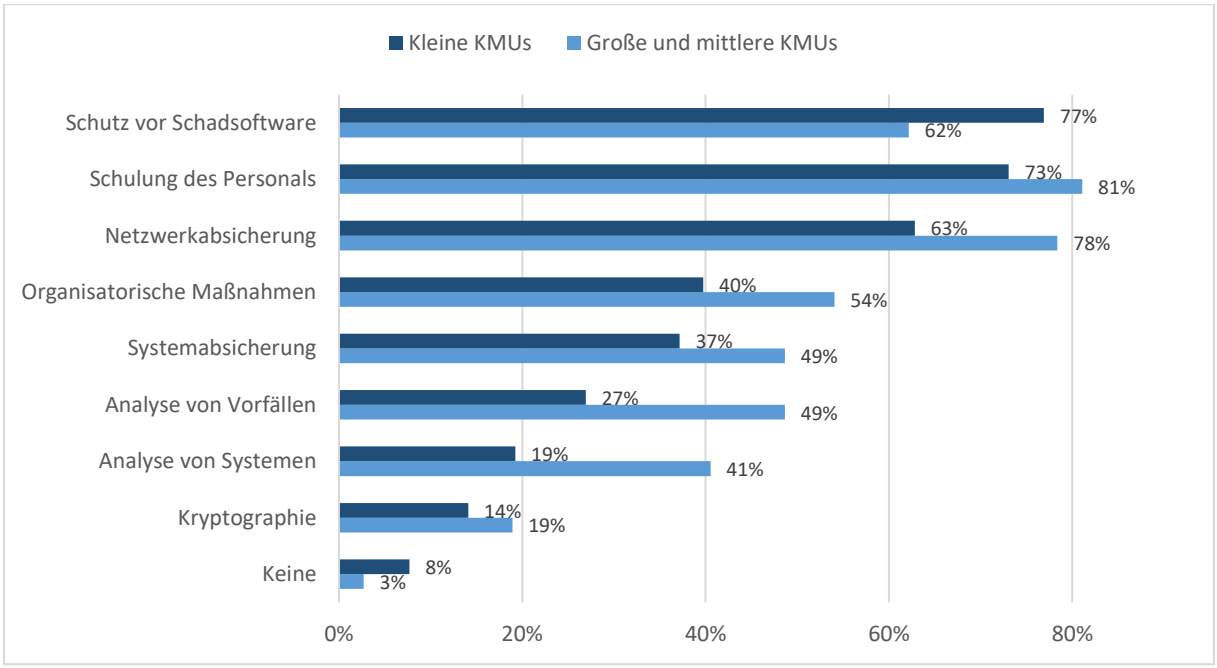

Abbildung 13: Als sinnvoll bewertete Maßnahmen zur Erhöhung des IT-Sicherheitsniveaus im eigenen Unternehmen gruppiert nach Größe

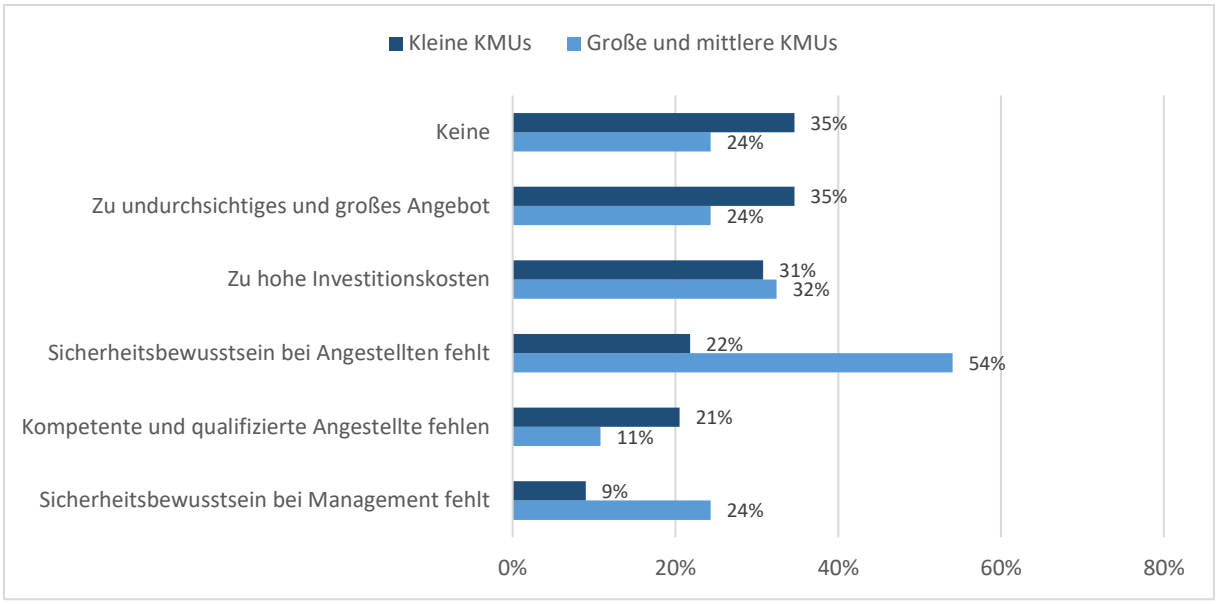

Abbildung 14: Hemmnisse zur Verbesserung des IT-Sicherheitsniveaus gruppiert nach Größe

3.2 Infrastruktur

Die Kategorie Infrastruktur umfasst Fragen, die sich mit physischen und digitalen Schutzmaßnahmen von Hard- und Softwarekomponenten befassen. Es werden unter anderem Schutzmaßnahmen für Serverräume, sowie die generelle Nutzung von WLANs und externen Datenträger betrachtet.

Für die Frage nach dem IT-Sicherheitsniveau ist es wichtig, die verschiedensten Zutrittsmöglichkeiten in Firmennetzwerke zu betrachten. Da Angreifer heutzutage über eine Vielzahl verschiedenster Angriffsmöglichkeiten verfügen, sollten Unternehmen jeweilige Zutrittsmöglichkeiten in ihr Netzwerk untersuchen und absichern. Sind diese nicht abgesichert, kann die Effektivität weiterführender Schutzmaßnahmen stark beeinträchtigt werden.

Die Unternehmen der Region setzen technische Standardmaßnahmen wie Firewalls und unternehmensweiten Schutz vor Schadsoftware größtenteils um. Dies stellt eine gute Ausgangsposition für erfolgreiche IT-Sicherheit dar. Der Einsatz solcher Schutzmaßnahmen ist eine Grundvoraussetzung für sichere Netzwerke, da sie gängige Angriffe und Schadsoftware identifizieren und somit Schäden vermeiden können.

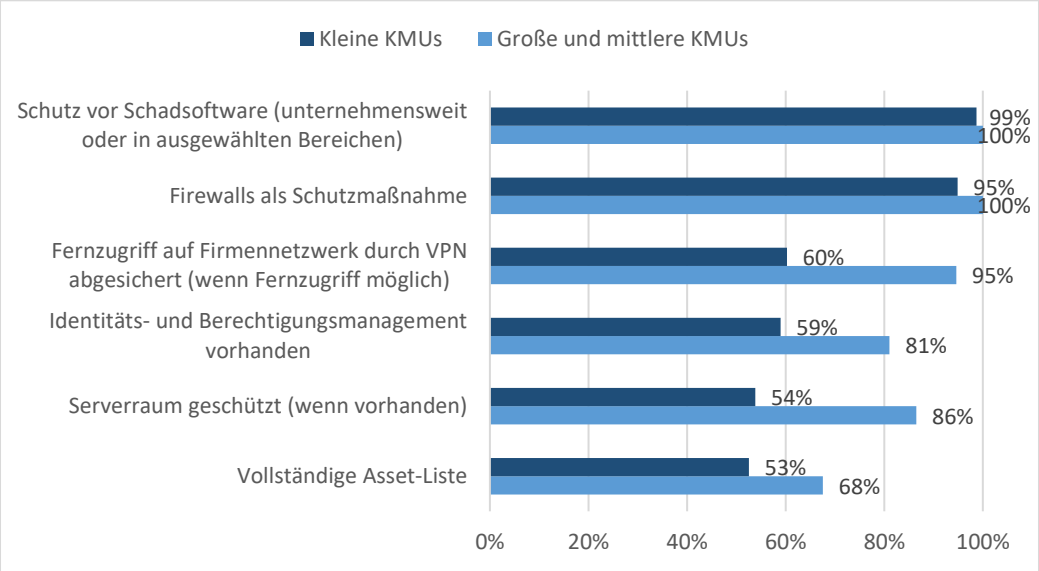

Abbildung 15: Kernaussagen über umgesetzte Maßnahmen aus dem Bereich Infrastruktur gruppiert nach Größe

Verbesserungsbedarf ist in der Absicherung von Serverräumen, auch hinsichtlich der verwendeten Schutzmaßnahmen vorhanden. Unternehmen sollten sich einen Überblick über die Vielzahl möglicher Schutzmaßnahmen für Serverräume verschaffen und prüfen, welche Schutzmaßnahmen gegen mögliche Probleme vorhanden sind und welche weiter ausgebaut werden sollten.

In den Punkten Fernzugriffabsicherung, Identitäts- und Berechtigungsmanagement, sowie vollständigen Asset-Listen besteht in der Region Handlungsbedarf. Wenn Mitarbeiter von außerhalb auf das Firmennetzwerk zugreifen können, sollten diese Zugänge zusätzlich abgesichert werden, damit Kriminellen das Abfangen der Daten zusätzlich erschwert wird.

Ein Identitäts- und Berechtigungsmanagementsysteme sorgt präventiv dafür, dass Unbefugte keinen Zugriff auf Daten bekommen, für die sie nicht autorisiert sind. Asset-Listen hingegen werden zwar insgesamt oft von Unternehmen geführt, jedoch beinhalten diese häufig nicht alle im Unternehmen verwendeten Informations- und Kommunikationssysteme. Eine vollständige Übersicht über verwendete Hardware

ermöglicht es, bei Bekanntwerden neuer Sicherheitslücken effektiv und effizient zu überprüfen, ob diese Lücken das Unternehmen betreffen und wenn ja, die betroffenen Geräte schnellstmöglich zu identifizieren. Durch eine aktuelle, vollständige Übersicht haben Unternehmen außerdem stets einen Überblick über die Geräte, die im Umlauf sind. So können beispielsweise Verluste schneller festgestellt und Neuanschaffungen besser geplant werden.

Das Angebot von WLANs innerhalb der Unternehmen ist weit verbreitet. 87% bieten WLAN für ihre Angestellten, Kunden, oder Besucher an. Bei der Absicherung der WLANs besteht jedoch starker Handlungsbedarf. 35% der Unternehmen besitzen keine expliziten Regeln für die Nutzung, was dazu führen kann, dass Nutzer unabsichtlich oder vorsätzlich das Firmennetzwerk mit Schadsoftware infizieren könnten.

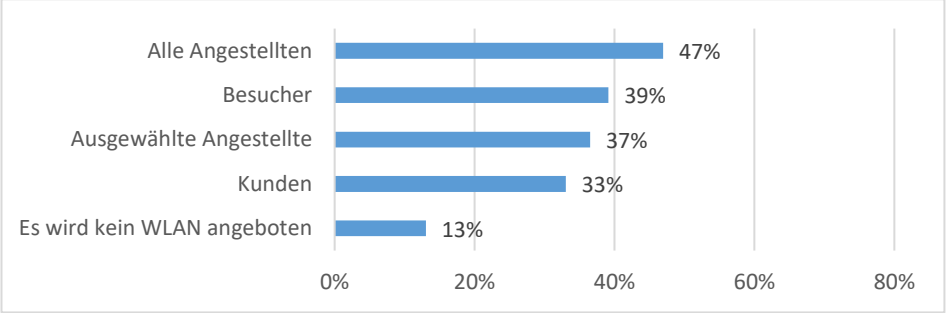

Abbildung 16: WLAN-Angebot befragter Unternehmen

Hinsichtlich der Regelung der WLAN-Nutzung ist anzumerken, dass der Handlungsbedarf bei kleinen KMUs stärker, als bei großen und mittleren KMUs ist.

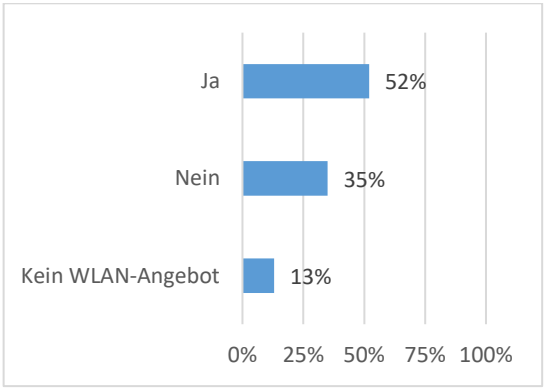

Abbildung 17: Regeln zur WLAN-Nutzung

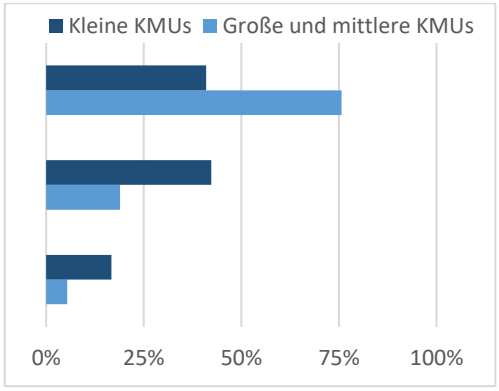

Abbildung 18: Regeln zur WLAN-Nutzung

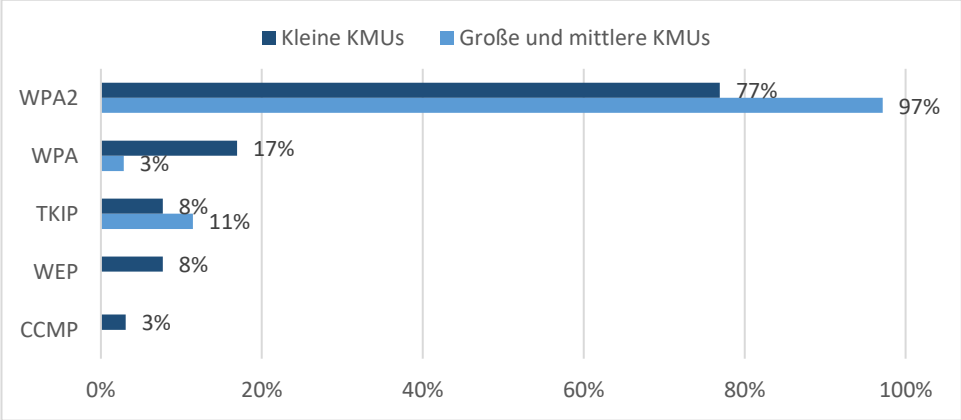

Abbildung 19: Eingesetzte WLAN-Verschlüsselungsmethoden (gruppiert nach Größe)

Die Nutzung externer Datenträger, wie USB-Sticks, externe Festplatten oder SD-Karten ist bei 70% der befragten Unternehmen möglich. In 44% der Unternehmen ist die Nutzung privater Datenträger entweder erlaubt, beziehungsweise wird diese technisch nicht verhindert. In 23% der Unternehmen werden die Datenträger vor der Nutzung untersucht. 29% der Unternehmen verbieten und unterbinden die Nutzung privater Datenträger komplett.

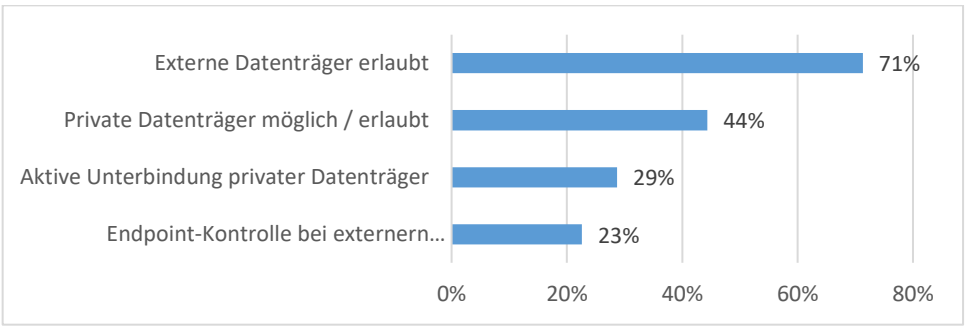

Abbildung 20: Umgang mit externen Datenträgern

Diese Ergebnisse zeigen, dass sich ein Großteil der Unternehmen, den Gefahren der Nutzung externer Datenträger entweder nicht bewusst ist, oder sie dem Nutzen unterordnen. Unternehmen sollten sich die Gefahren bewusst machen und prüfen, ob und in welchem Umfang sie externe Datenträger benötigen. Die Nutzung sollte ausschließlich in diesen Bereichen erlaubt, beziehungsweise möglich sein.

Die erwähnten Gefahren betreffen sowohl Daten, die mit Schadsoftware infiziert sind und so unerlaubt in das Firmennetzwerk gelangen, es unerlaubt verlassen und somit gestohlen werden, oder das grundsätzliche Risiko des Verlusts eines Datenträgers inklusive der darauf gespeicherten Daten.

3.3 Sicherheitskonzept

Durch die steigende Vernetzung und den hohen Stellenwert von IT-Systemen ist die Sicherheit dieser Systeme für den Unternehmenserfolg essenziell. Damit Unternehmen im Fall eines Angriffs vorbereitet sind, sollte IT-Sicherheit in den Sicherheitskonzepten verankert sein. Unternehmen können so dafür sorgen, dass Sie im Schadensfall nicht unvorbereitet sind, da Sie

das Vorgehen bereits geplant und Maßnahmen zur Reduzierung der Schadensschwere bestimmt haben. Eine solche Verankerung ist bislang erst bei 50% der befragten Unternehmen umgesetzt. Unternehmen, die sich bislang gegen die Verankerung entschieden, oder diesen Punkt nicht bedacht haben, sollten prüfen, ob ihre Existenz von der Funktionalität der IT-Systeme und den darauf gespeicherten Daten abhängig ist. Wenn eine Abhängigkeit besteht, sollten Schutzziele evaluiert und Sicherheitskonzepte angepasst werden.

Damit IT-Sicherheitsmaßnahmen zielgerichtet ausgesucht und etabliert werden können, sollten verbindliche IT-Sicherheitsziele festgelegt werden. Die Definition solcher Ziele ermöglicht außerdem, dass sich die verschiedenen Bereiche und Aktivitäten innerhalb des Unternehmens von Beginn an deren Einhaltung orientieren können. Auch in diesem Bereich besteht bei den Unternehmen der Region Handlungsbedarf. 43% der Unternehmen gaben an, verbindliche IT-Sicherheitsziele festgelegt zu haben. Im Umkehrschluss bedeutet dies, dass über die Hälfte der Befragten die Schutzmaßnahmen nicht nach einem festgelegten Plan, sondern unsystematisch umsetzen und einführen.

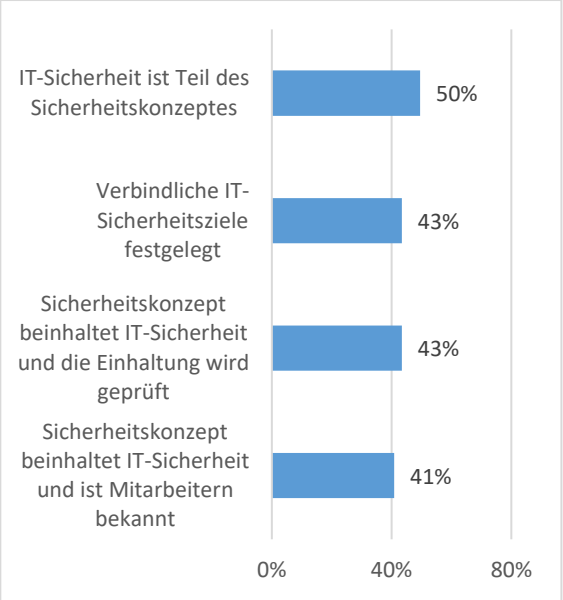

Abbildung 21: Sicherheitskonzepte und IT-Sicherheitsziele

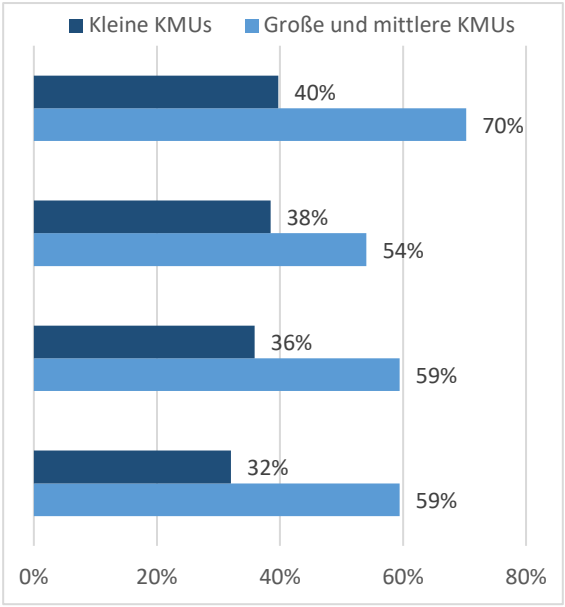

Abbildung 22: Sicherheitskonzepte und IT-Sicherheitsziele

Wenn IT-Sicherheit ein Teil des Sicherheitskonzeptes ist und entsprechende IT-Sicherheitsziele festgelegt wurden, hängt die Effektivität dieser Maßnahme davon ab, dass die Konzepte und Ziele den Mitarbeitern des Unternehmens bekannt sind, damit diese sich nach ihnen richten können. Die Bekanntmachung (41%) und anschließende Überprüfung der Einhaltung (43%) wird in einem vergleichbaren Maßstab von den Unternehmen umgesetzt. Dies ist ein Zeichen dafür, dass mit bestehen von Verbindlichen IT-Sicherheitszielen, die Mitarbeiter auf die Bedeutung und Notwendigkeit der IT-Sicherheit aufmerksam gemacht und für diese sensibilisiert werden.

3.4 IT-Sicherheitsbeauftragter/IT-Verantwortlicher

Um die Umsetzung und Einführung von IT-Sicherheitsmaßnahmen koordiniert und kontrolliert umzusetzen, bietet es sich für Unternehmen an, einen IT-Sicherheitsbeauftragten zu benennen. 33% der befragten Unternehmen haben eine solche Benennung bereits vorgenommen. Ist eine explizite Benennung keine Option für ein Unternehmen, sollte grundsätzlich ein IT-Verantwortlicher und Ansprechpartner für IT-Sicherheitsfragen und -Vorfällen vorhanden sein, der von Mitarbeitern kontaktiert und befragt werden kann. Ein solcher Ansprechpartner ist in 83% der Unternehmen vorhanden. Unternehmen, die keinen Ansprechpartner für Mitarbeiter besitzen haben akuten Nachholbedarf.

Durch das Ausbleiben einer festgelegten Kontaktstelle müssen Mitarbeiter im Zweifelsfall selbst entscheiden, ob einer verdächtigen Quelle vertraut wird, oder nicht. Dies kann dazu führen, dass unwissentlich falsch entschieden wird und ein Angreifer – beispielsweise durch eine Phishing-Mail – erfolgreich das Firmennetzwerk infiziert.

Nachdem feste Verantwortlichkeiten für IT-Sicherheit festgelegt sind, können die entsprechenden Mitarbeiter gezielt geschult, Kompetenzen ausgebaut und die Qualifikation – beispielsweise durch Zertifizierungen – gefördert werden. Unternehmen können so ihr internes Fachwissen zum Thema IT-Sicherheit fortlaufend ausbauen. Entsprechende Qualifikation und Zertifizierungsmaßnahmen werden von 57% der Unternehmen durchgeführt.

In der nachfolgenden Abbildung wird von IT-Verantwortlichen gesprochen. Hiermit ist sofern benannt entweder der IT-Sicherheitsbeauftragte oder der jeweilige IT-Verantwortliche (z.B. IT-Leiter, externer Beauftragter etc.) gemeint.

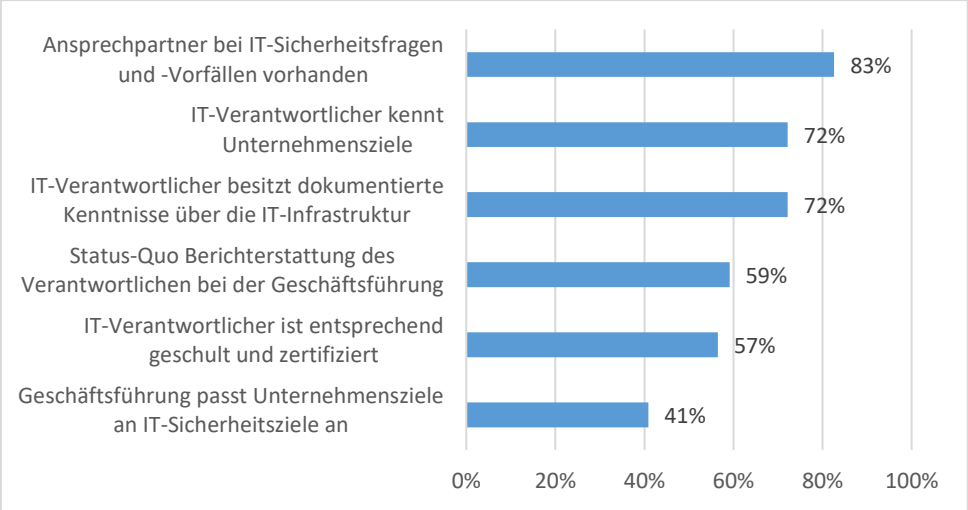

Abbildung 23: Diverse Sicherheitsaspekte bezüglich des IT-Verantwortlichen oder IT-Sicherheitsbeauftragten

3.5 Verschlüsselung

Die Verschlüsselung von Daten ist eine der ältesten und bewährtesten Sicherheitsmaßnahmen, um die Offenlegung von Daten zu verhindern und deren Vertraulichkeit zu gewährleisten. Befragte Unternehmen bewerten die Relevanz der Vertraulichkeit ihrer Daten in 83% der Fälle mit „sehr hoch“ (50%) oder „eher hoch“ (33%). Trotz der hohen Bewertung durch die Unternehmen werden entsprechende Maßnahmen erst von 58% der Unternehmen umgesetzt. Diese 58% lassen sich in zwei verschiedene Herangehensweisen unterteilen: Die Verschlüsselung aller Daten (von 14% der Unternehmen durchgeführt) und die Verschlüsselung ausgewählter Daten (von 44% der Unternehmen durchgeführt).

Neben der generellen Verschlüsselung von Daten gibt es weitere, spezifischere Sicherheitsmaßnahmen aus dem Bereich der Verschlüsselung. Die Verwendung digitaler Signaturen, die Verschlüsselung von E-Mails mit kritischen Informationen und die Nutzung eines geeigneten Schlüsselmanagements werden jeweils von 43% der Unternehmen umgesetzt. Die Einarbeitung in die Verwendung der jeweiligen Verschlüsselungsmaßnahmen wird lediglich von 23% aktiv umgesetzt.

Für Unternehmen die Verschlüsselung einsetzen und ihre Mitarbeiter nicht entsprechend auf in Nutzung einarbeiten besteht akuter Handlungsbedarf. Ohne eine entsprechende Einarbeitung kann es zu Fehlern im Vorgehen kommen, die die Effektivität der Verschlüsselung negativ beeinflussen und die Sicherheit gefährden können. Wenn bislang keine Verschlüsselung eingesetzt wird, sollten Unternehmen die Einführung entsprechender Maßnahmen prüfen.

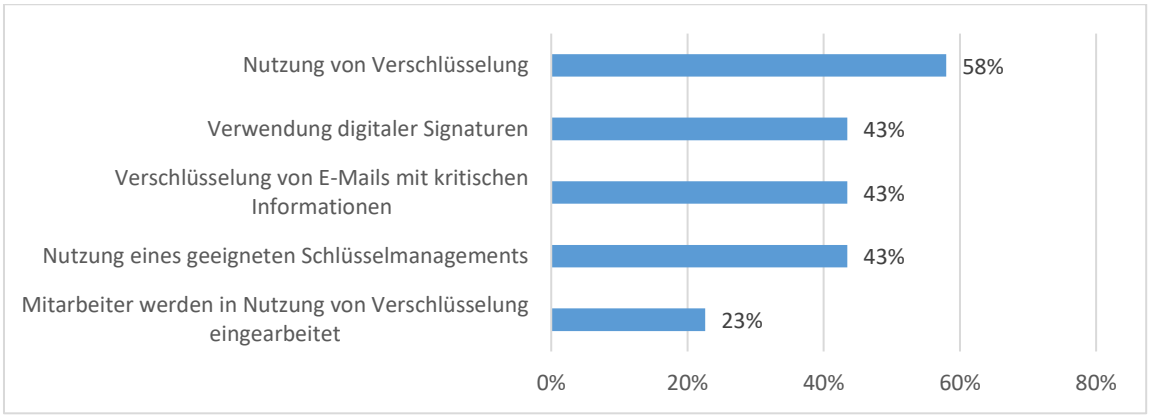

Abbildung 24: Einsatz von Verschlüsselung

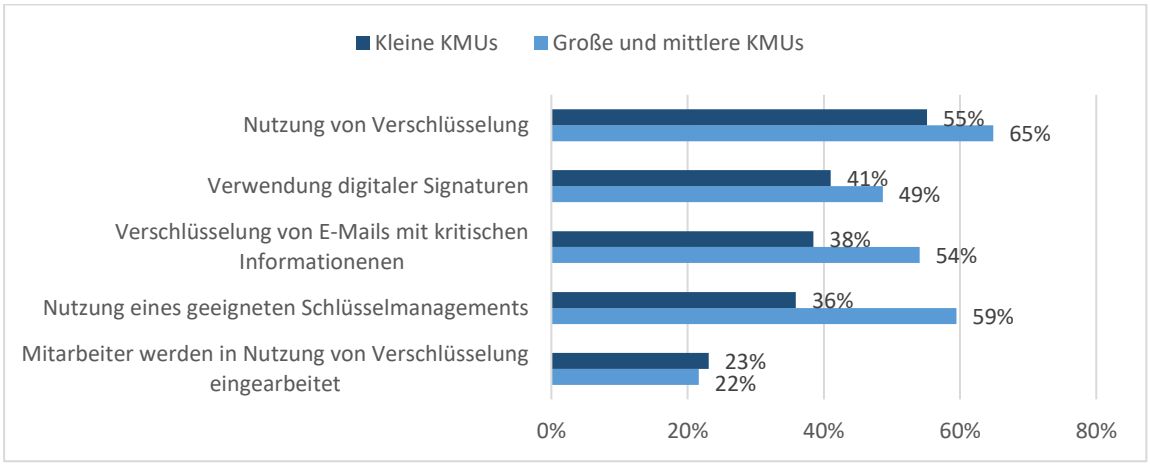

Abbildung 25: Abbildung 24 gruppiert nach Größe

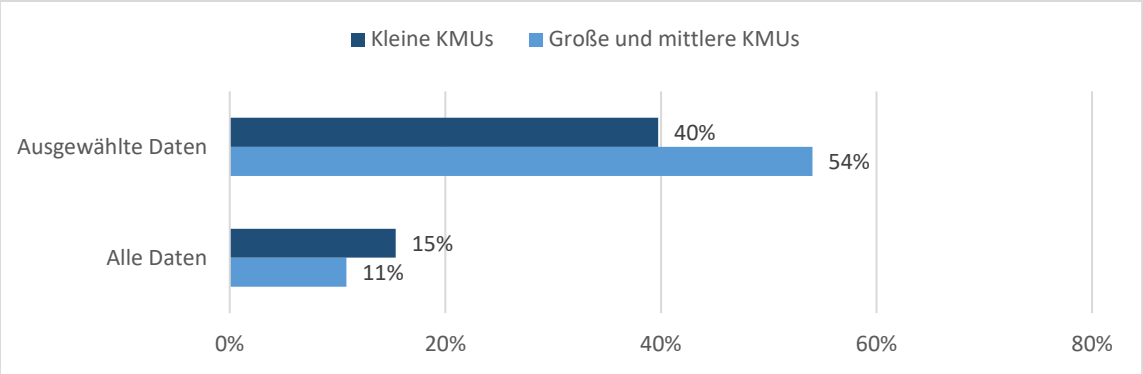

Abbildung 26: Eingrenzung verschlüsselter Datenmengen (gruppiert nach Größe)

Auch wenn die unternehmensweite Nutzung von Verschlüsselung grundsätzlich sinnig ist, müssen die aufgeführten Maßnahmen nicht zwingend unternehmensweit und für alle Daten umgesetzt werden. Ausgewählte, besonders kritische Dokumente und Datenträger durch Verschlüsselung zu schützen kann bereits dazu beitragen, das Sicherheitsniveau maßgeblich zu erhöhen. Um dies zu ermöglichen könnten Daten kategorisiert und für die jeweiligen Kategorien danach ein entsprechender Schutzbedarf und Schutzmaßnahmen definiert werden. Für solche Kategorisierungen gibt es diverse frei zugängliche Ansätze, wie die Schutzbedarfsfeststellung des BSI-Standards 200-2.

Ein Beispiel: Die zentrale Datensicherung enthält alle wichtigen und für das Unternehmen relevanten Daten. Sie ist somit kritisch für den Unternehmenserfolg, da eine Offenlegung der Daten das Unternehmen schädigen und die Konkurrenz stärken könnte. Zudem kann das Ansehen bei Geschäftspartnern und der Öffentlichkeit stark beeinträchtigt werden. Aufgrund der potenziellen Gefahren wird ein sehr hoher Schutzbedarf festgelegt. Die Datensicherungen werden aufgrund ihres Schutzniveaus zusätzlich verschlüsselt. Um den Arbeitsaufwand zu verringern wird die Verschlüsselung automatisch nach der Durchführung der Datensicherung durchgeführt. Durch die automatische Verschlüsselung wird dafür gesorgt, dass nur Befugte die Unternehmensdaten wiederherstellen und entschlüsseln können. Die getroffene Schutzmaßnahme verhindert, dass ein Angreifer durch den Diebstahl der Datensicherung an die gesicherten Firmendaten gelangen kann.

3.6 Mobilgeräte

Die Nutzung mobiler Endgeräte im Arbeitsalltag nimmt stetig zu. Smartphones und Tablets sind für viele Unternehmen, z.B. im mobilen Arbeiten, nicht mehr wegzudenken. Die wachsende Anzahl von verschiedenen Modellvarianten erschwert zusätzlich einen Überblick über spezifische, sicherheitsrelevante Eigenschaften beizubehalten. Nicht nur die Verwaltung, sondern auch der Umgang mit Mobilgeräten sollte im Unternehmen klar definiert und in schriftlicher Form fixiert sein. In der Befragung gaben 46% der Unternehmen an, bisher keine Sicherheitsrichtlinien für den Umgang mit mobilen Endgeräten definiert zu haben. Nur gut ein Drittel gaben an ihre Mitarbeiter dazu anzuhalten Mobiltelefone zu schützen. Um Datenverlust durch mobile Endgeräte überhaupt erkennen zu können, muss die Unternehmung von Verlust oder Diebstahl der Geräte erfahren. Dreiviertel der KMUs verpflichtet ihre Mitarbeiter, den Verlust von Mobiltelefonen, unverzüglich zu melden. Um die Möglichkeit des Missbrauchs von sensiblen Daten auf Mobilgeräten und den damit verbundenen Reputationsschaden bestmöglich zu

begrenzen, sollte es möglich sein, die darauf befindlichen Daten aus der Ferne zu sperren oder zu löschen. Die Einrichtung einer solchen Fernsperrung bzw. -löschung haben 43% der Unternehmen vorgenommen.

Viele Anwendung aus dem privaten Umfeld wie z.B. Messenger-Dienste, greifen auf die Kontakte des Mobiltelefons zu. Sind auf dem Mobiltelefon Kontaktdaten von Privatkunden enthalten, kann das Auslesen dieser Kontakte schnell im Sinne der DSGVO relevant werden. Dies ist einer der Gründe weshalb Unternehmen zwischen privater und geschäftlicher Nutzung der mobilen Endgeräte unterscheiden sollten. Gut ein Drittel der befragten KMUs vollzieht eine solche Trennung.

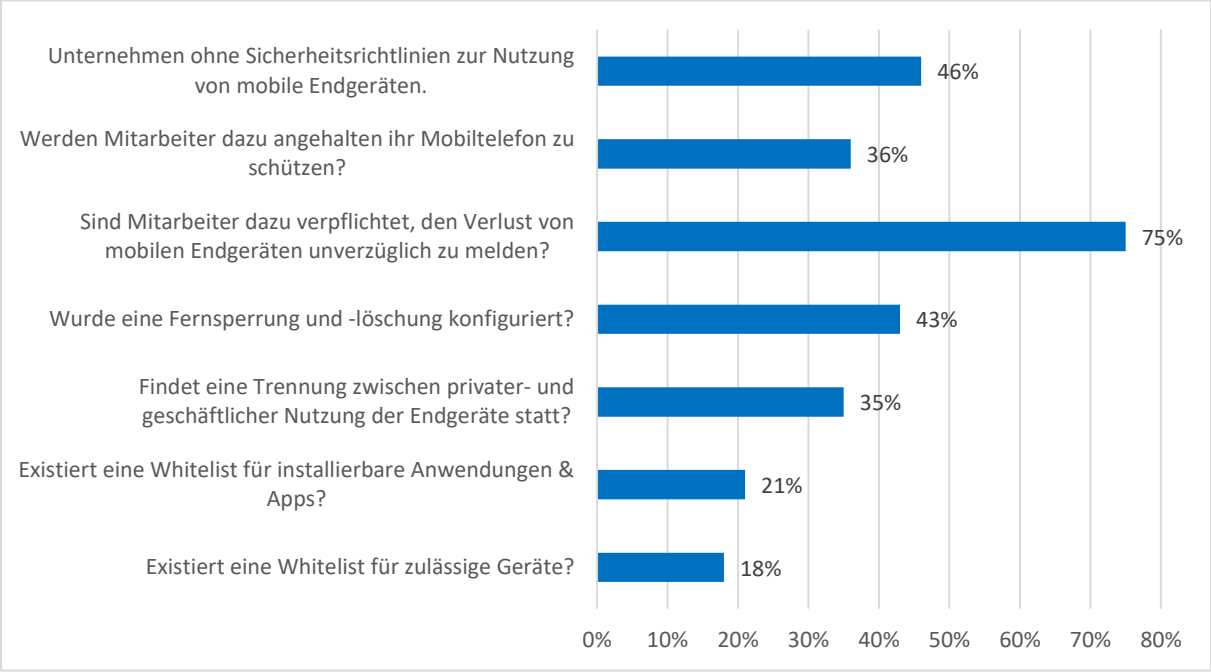

Abbildung 27: Umgang mit Mobilgeräten

Eine Whitelist für installierbare Anwendung, also eine Auflistung der vom Arbeitgeber erlaubten Anwendungen gibt dem Mitarbeiter klare Vorgaben, welche Anwendungen unkritisch sind und welche nicht. Nur gut jedes vierte KMU gibt an eine solche Liste zu führen. Auch für die im Unternehmen eingesetzten Mobilgeräte sollte eine solche Liste bestehen, um Geräte die bekanntermaßen unsicher sind, erst gar nicht zuzulassen. 18% der befragten Unternehmen gaben an eine Liste für erlaubte Endgeräte zu führen.

3.7 Mitarbeitersensibilisierung

Um Informationssicherheit im eigenen Unternehmen erfolgreich umzusetzen, müssen Mitarbeiter sensibilisiert werden, um unternehmensweit relevante Gefahren für die Informationssicherheit erkennen und abwenden zu können.

Mitarbeiter setzen die Sicherheitsziele Ihrer Institution dann am besten um, wenn sie deren Notwendigkeit verstanden haben. Durch initiale und wiederkehrende Schulungen zu den Informationssicherheitszielen und Maßnahmen zu deren Einhaltung, kann im Unternehmen eine Kultur der Informationssicherheit geschaffen werden.

In der Befragung gaben 86% der größeren und 59% der kleineren KMUs an, ihre Mitarbeiter zum Thema IT-Sicherheit zu sensibilisieren.

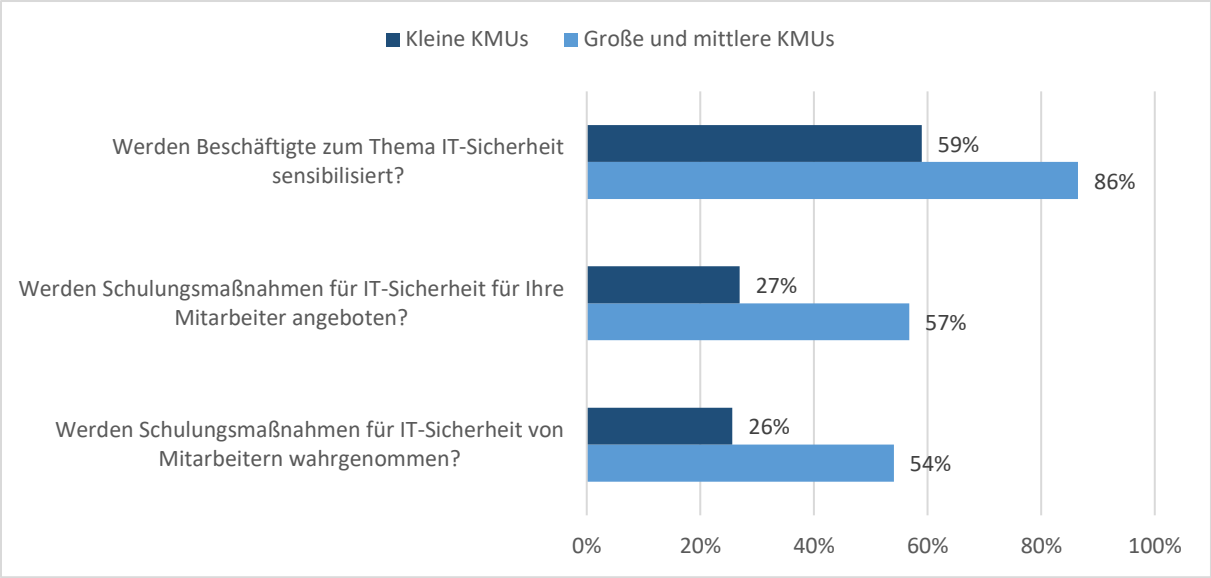

Abbildung 28: Mitarbeitersensibilisierung gruppiert nach Größe

Gerade kleinere Unternehmen haben hier Nachholbedarf. Die Vielfalt angebotener Maßnahmen ist ebenfalls ausbaufähig. Ein kleinerer Teil der Unternehmen setzt beispielsweise auf Sensibilisierung durch Schulungen (37%). Anders als bei Hinweisen oder Tipps zu IT-Sicherheitsvorfällen, lässt sich bei Maßnahmen wie Schulungen und Seminaren, überprüfen welche Mitarbeiter teilgenommen haben. Aus der Befragung geht hervor, dass Mitarbeiter bei vorhandenen Schulungsangebot, dieses auch in den meisten Fällen wahrnehmen.

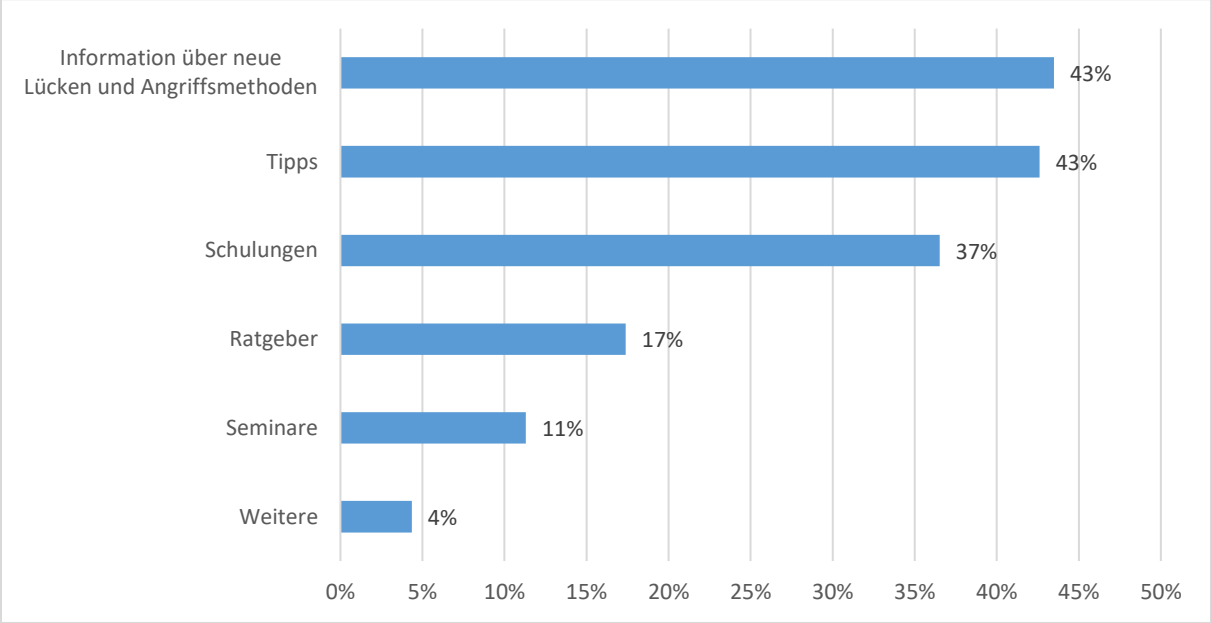

Abbildung 29: Sensibilisierungsangebot

3.8 Datensicherung

Für die meisten Unternehmen ist die Verfügbarkeit ihrer Daten existenziell. Je nach Branche kann der Verlust von Unternehmensdaten zu einem hohen finanziellen Schaden und bis hin zur Geschäftsaufgabe führen. Die Bedrohungen für Unternehmensdaten sind vielfältig. Zu den häufigsten Ursachen für den Verlust von Daten zählen menschliche Fehler, Schadsoftware, Fehler in Soft- bzw. Hardware, oder dem Zusammenspiel von Komponenten und physische Schäden an Datenträgern.

Damit im Ernstfall der Schaden eines Datenverlusts möglichst begrenzt werden kann, empfiehlt unteranderem das BSI, die Unternehmensdaten durch regelmäßige Backups zu sichern. Mit 95% gaben fast alle Unternehmen an, eine solche Datensicherung durchzuführen.

Die zeitlichen Abstände der Datensicherung richten sich dabei nach der Bedeutung der Aktualität der gespeicherten Daten. Das genaue Vorgehen und die eingesetzten Werkzeuge für die Datensicherung werden in der Backup Strategie dokumentiert. Die schriftliche Fixierung der Backup Strategie gewährleistet auch bei wechselnden Verantwortungen eine korrekte und nachhaltig richtige Durchführung der Datensicherung. Erst 53% der befragten Unternehmen haben ihre Backup Strategie dokumentiert.

Der Verantwortliche für die Datensicherung überwacht und vollzieht diese konform der Backup Strategie. 86% der Unternehmen haben einen solchen Verantwortlichen ernannt.

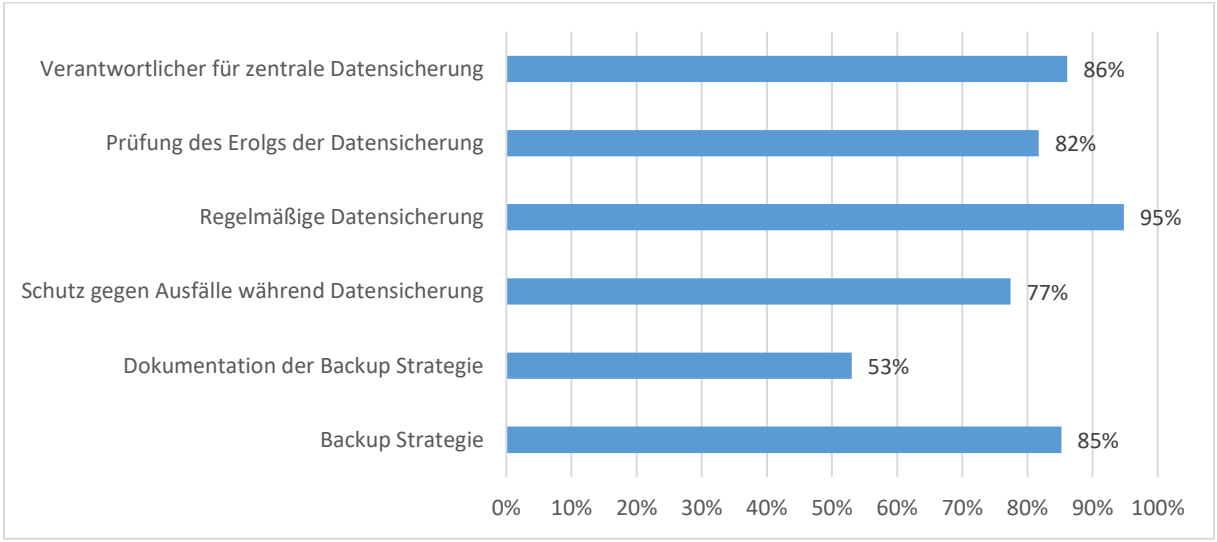

Abbildung 30: Datensicherung - Überblick über umgesetzte Maßnahmen

3.9 Notfallbehandlung

Ähnlich dem Verhalten während eines Brandfalls, sollte auch das Verhalten bei IT-Sicherheitsvorfällen gedanklich vorweggenommen werden. Die Festlegung expliziter Handlungsanweisungen erleichtert das zielgerichtete Handeln in Notfallsituationen. Um wiederkehrende Gefahren erkennen zu können, sollten sicherheitsrelevante Vorfälle protokolliert werden. Knapp die Hälfte der kleinen- und Dreiviertel der größeren KMUs protokollieren IT-Sicherheitsvorfälle. Notfälle können beispielweise Defekte in Soft- oder Hardware sein, die den Unternehmensbetrieb in kritischer Weise beeinträchtigen. Die entsprechenden Handlungsanweisungen werden Bestandteil des unternehmensindividuellen Notfallkonzepts. Die Befragung zeigt auf, dass rund 40% der Unternehmen ein solches Konzept haben. Nur wenn den Mitarbeitern das Notfallkonzept bekannt ist, können Sie im Ernstfall schnell und richtig reagieren.

Simulationen eines solchen Ernstfall, erproben das Notfallkonzept und stellen sicher, dass die Mitarbeiter in der Lage sind die Anweisungen umzusetzen. Eine Analyse dazu wie lange das Unternehmen ohne EDV-Systeme funktionsfähig ist, ermöglicht die Einordnung des Schutzbedarfs einzelner Komponenten.

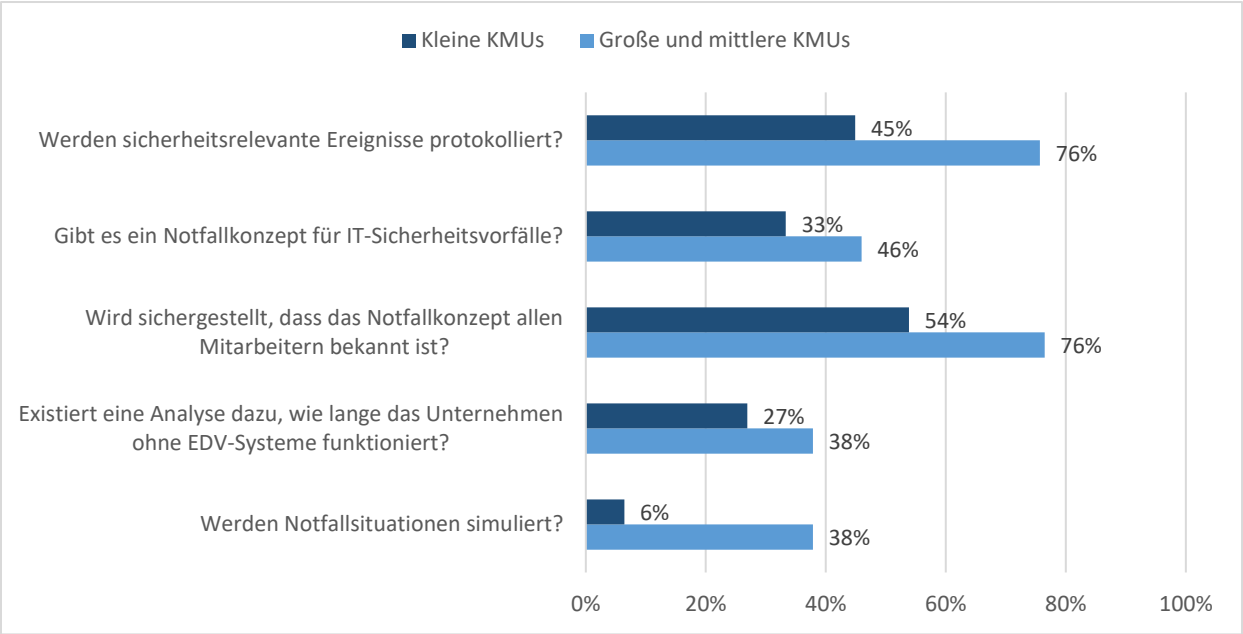

Abbildung 31: Notfallbehandlung gruppiert nach Größe

Aus der Befragung wird deutlich, dass besonders konzeptionelle Sicherheitsmaßnahmen häufiger von größeren als von kleineren KMUs umgesetzt werden.

3.10 Datenschutz

Die Datenschutz-Grundverordnung (DSGVO) ist eine auf europäischer Ebene beschlossene Verordnung mit dem Zweck, die Rechte der EU-Bürger hinsichtlich des Datenschutzes zu stärken und zu vereinheitlichen. Im Fokus steht der Schutz personenbezogener Daten von natürlichen Personen. Die DSGVO wurde 2016 beschlossen und ist am 25. Mai 2018 in Kraft getreten. Die aufgestellten Grundsätze stellen dabei so etwas wie die „Grundregeln“ zur Verarbeitung von personenbezogenen Daten dar und helfen Insbesondere bei der Auslegung von Regelungen der DSGVO. Fast alle befragten Unternehmen kennen diese Grundsätze. Alle größeren und 91% der kleineren KMUs sind sich der Spezifizierung von personenbezogenen Daten bewusst.

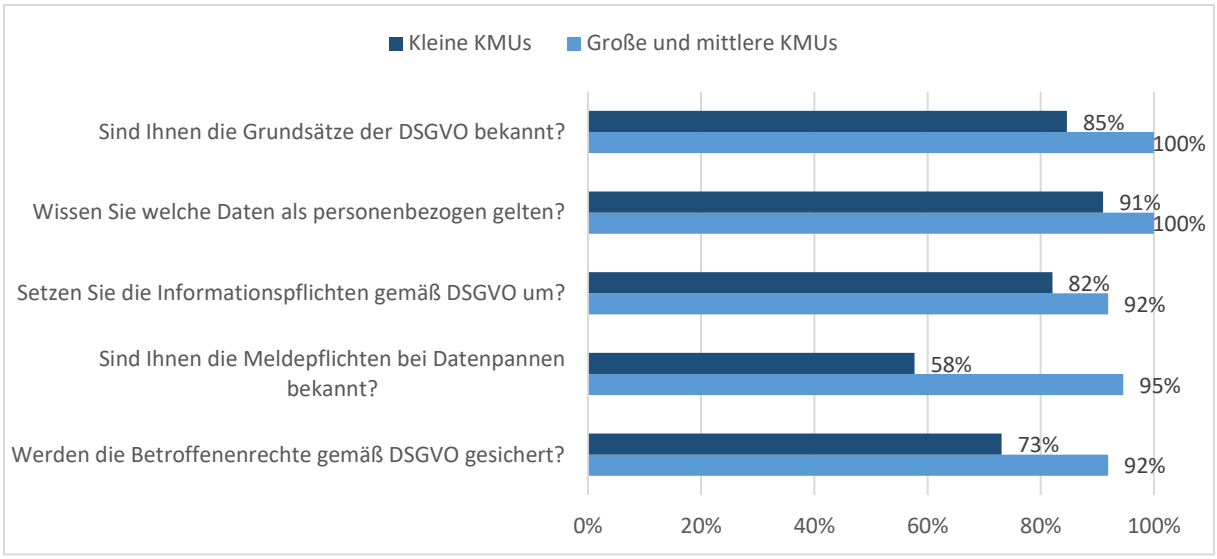

Abbildung 32: DSGVO - Übersicht gruppiert nach Größe

Im Falle einer Verletzung des Schutzes der personenbezogenen Daten sind die Unternehmen rechtlich verpflichtet, unverzüglich eine Meldung an die zuständige Aufsichtsbehörde abzugeben. Nur gut die Hälfte der kleineren Unternehmen sind sich dieser gesetzlichen Anforderung bewusst.

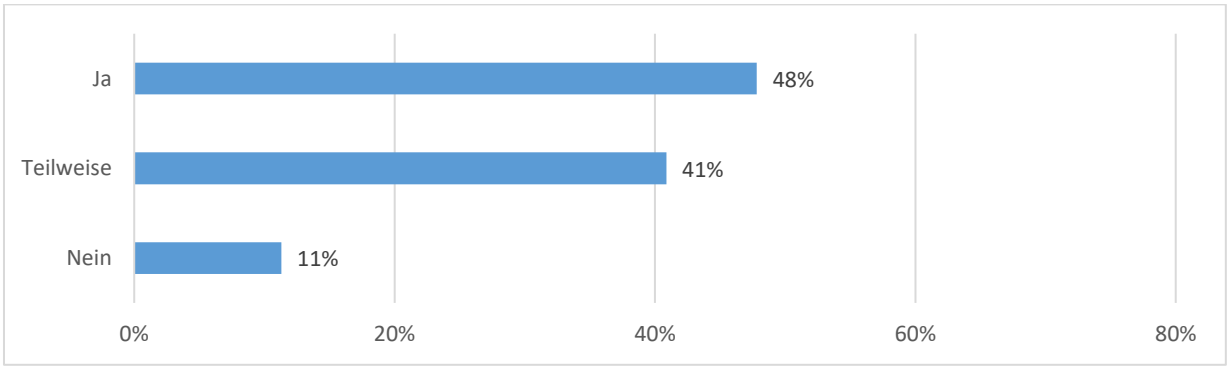

Abbildung 33: Selbsteinschätzung der DSGVO-Konformität

Rund jedes zweite Unternehmen gibt an, DSGVO-Konform aufgestellt zu sein. 11% sind sich sicher die Anforderungen der DSGVO nicht umzusetzen.

4 Handlungsempfehlungen

In diesem Kapitel werden entsprechende Handlungsempfehlungen für Unternehmen getroffen und weiterführendes Informationsmaterial verlinkt. Die Empfehlungen sind an Sicherheitsmaßnahmen aus anerkannten Leitfäden, offiziellen Standards, bewährten Vorgehensweisen und Richtlinien angelehnt. Sie sollen Unternehmen, die ihr IT-Sicherheitsniveau verbessern möchten, als Orientierungshilfe dienen und mögliche Sicherheitsmaßnahmen aufzeigen. Aufgrund der Heterogenität der befragten Unternehmen sind nicht alle Maßnahmen für alle Befragungsteilnehmer gleichermaßen relevant und zutreffend, weswegen die Relevanz der Einzelmaßnahmen von den Unternehmen geprüft werden sollte, bevor sie umgesetzt werden. Eine Checkliste für erste Schritte zu einer guten IT-Sicherheit befindet sich im Anhang.

4.1 Allgemein

Grundsätzlich sollten sich neben den Mitarbeitern und denen für IT-Sicherheit verantwortlichen Mitarbeiter, auch die Verantwortlichen eines Unternehmens mit dem Thema IT-Sicherheit beschäftigen und aktuelle Meldungen über Schwachstellen, Bedrohungen oder ähnlichem, beschäftigen. Die notwendigen Informationen sind sowohl kostenpflichtig als auch kostenlos erhältlich und zugänglich. Nachfolgend werden einige, generell als vertrauenswürdig geltende Informationsquellen in keiner spezifischen Reihenfolge aufgeführt.

Generelle Informationen, Checklisten und aktuelle Publikationen werden auf den Internetseiten des BSI (Bundesamt für Sicherheit in der Informationstechnik) zur Verfügung gestellt. Mit dem Bürger-CERT des BSI gibt es eine weitere Anlaufstelle an der Unternehmen und Privatpersonen über aktuelle Themen mit IT-Sicherheitsbezug informiert werden.

Auf der Webseite www.mittelstand-digital.de ist eine Vielzahl an Informationen zu verschiedenen IT-Sicherheitsthemen vorhanden. Unter dem Suchwort „IT Sicherheit“ können entsprechende Informationen gefunden werden. Eine Sammlung an Checklisten, Tipps, Risiken, Empfehlungen, Verhaltensregeln und generelle Informationen zum Thema IT-Sicherheit finden Sie auf der Internetseite des „BSI für Bürger“ oder dem „Bürger-CERT“ des BSI.

Neben den aktuellen Sicherheitshinweisen des Bürger-CERT, gibt es diverse Internetplattformen, die kostenlos aktuelle Nachrichten aus dem Bereich der IT- und Informationssicherheit veröffentlichen. Nachfolgend werden einige dieser Plattformen in keiner bestimmten Reihenfolge aufgezeigt:

- https://www.heise.de/security/
- https://www.security-insider.de
- https://www.itsicherheit-online.com/news/

Unternehmen sollten Informationen über ihre Systeme und den Datenfluss innerhalb des Netzwerkes sammeln und kontrollieren. Eine solche Überwachung und regelmäßige Kontrolle ermöglicht Angriffe rechtzeitig zu bemerken und die Schadensschwere einzudämmen. Jedes Unternehmen das den Ausfall der Technik als einen der Hauptursachen möglicher IT-Probleme sieht, sollte entsprechende Kontrollmaßnahmen etablieren. Ein Beispiel für eine solche Schutzmaßnahme ist der Einsatz von Intrusion-Detection-Systemen (auch „Angriffserkennungssystem“ oder kurz „IDS“ genannt). Diese Systeme prüfen den Netzwerkverkehr auf Unregelmäßigkeiten und Auffälligkeiten und geben entsprechende Meldungen aus, sobald potenziell verdächtiger Verkehr gefunden wird.

Weiterführende Informationen über die Grundlagen, rechtliche Aspekte und einen Leitfaden zur Einführung von Intrusion-Detection-Systemen stellt das BSI frei zur Verfügung (Weiterleitung zum BSI: BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen). Neben reinen IDS gibt es Intrusion-Prevention-Systeme (kurz „IPS“ genannt). Diese Systeme verfügen neben der Erkennung von Angriffen über Funktionen zur Blockierung und Vermeidung erkannter Angriffe. Beide Systeme haben entsprechende Vor- und Nachteile. Unternehmen sollten daher individuell prüfen, welches System ihre Anforderungen am besten erfüllt und entsprechende Sicherheitsmaßnahmen umsetzen.

4.2 Infrastruktur

Damit die verschiedenen IT-Systeme innerhalb eines Netzwerks zielgerichtet koordiniert und kontrolliert werden können, müssen Unternehmen Asset-Listen oder vergleichbare, zur Inventarisierung und Lokalisierung geeignete Listen führen. Über die IT-Systeme müssen mindestens drei Kerndaten gespeichert werden: ein eindeutiges Identifizierungsmerkmal (z.B. eine Inventarnummer), Informationen über den Einsatzort (z.B. das Büro, in dem das Gerät eingesetzt wird) und der Einsatzzweck (z.B. Laptop IT-Mitarbeiter „Max Mustermann“). Neben diesen Kerndaten ist es ratsam, von vornherein weitere Details der Systeme zu speichern. Eine Speicherung der eingesetzten Soft- und Hardware, Herstellernamen, Seriennummern, oder Informationen über Serviceverträge, erhöhen die Effektivität einer solchen Liste, da so schnell neue Schwachstellen in Systemen auf ihre Relevanz geprüft und betroffene Geräte umgehend identifiziert und geupdated werden können.

Benutzer und Geräte, die auf Daten des Unternehmens zugreifen, müssen zweifelsfrei identifiziert und authentifiziert werden. Ohne entsprechende Kontrollen kann nicht gewährleistet werden, dass nur berechtigte Entitäten auf die Daten und Ressourcen zugreifen können. Um Zugriffe unberechtigter Dritter auf nichtöffentliche Bereiche Ihrer IT-Systeme zu verhindern, können diverse grundlegende Maßnahmen ergriffen werden:

- Legen Sie eine Regelung fest, ab wann Mitarbeiter Ihren PC-Arbeitsplatz sperren müssen
- Richten Sie eine automatische Sperrung bei Inaktivität ein
- Legen Sie eine Passwort-Richtlinie fest
- Der Zugang zu allen nichtöffentlichen Bereichen der IT-Systeme muss durch geeignete Anmeldeverfahren abgesichert werden
- Verteilen Sie Zugangs-, Zutritts- und Zugriffsberechtigungen nur entsprechend der zu erledigenden Aufgabe und Funktion innerhalb des Unternehmens
- Verwalten Sie Zugänge und Zugriffsrechte in einem strukturierten System
- Legen Sie Verantwortlichkeiten zur Vergabe von Nutzungsrechten fest, damit Ihre Übersicht stets gepflegt und somit aktuell gehalten wird.

Neben den genannten Maßnahmen muss die Einrichtung und Vergabe von Benutzern und Benutzergruppen geregelt sein. Die Rechtevergabe darf nur durch administrative Rollen (wie beispielsweise dem System-Administrator) möglich sein. Einmal vergebene Benutzer sollten dokumentiert und festgehalten werden, damit zu einem späteren Zeitpunkt ersichtlich ist, wann welcher Benutzer welche Rechte hatte. Damit die Dokumentation die Ursachensuche unterstützen kann, sollte sie möglichst bei jeder Änderung an den Benutzern automatisch aktualisiert werden. Wenn eine automatische Aktualisierung nicht möglich ist, muss die Dokumentation in regelmäßigen Abständen auf ihre Aktualität geprüft werden. Sobald ein Mitarbeiter das Unternehmen verlässt, muss dies umgehend dem Administrator mitgeteilt werden, damit dieser die Rechte des Benutzers entfernen kann. Wird dies nicht gemacht, könnten die Benutzerberechtigungen dazu missbraucht werden, um dem Unternehmen zu schaden.

Neben einem aktiven Identitäts- und Berechtigungsmanagement erhöht die Nutzung von VPNs („Virtual Private Networks“) das Sicherheitsniveau in Unternehmen. VPNs sorgen primär dafür, dass schützenswerte Daten über nicht-vertrauenswürdige Netzwerke, wie beispielsweise dem Internet, zu übertragen. Sie sind somit essenziell, wenn der Zugriff von Mitarbeitern außerhalb des Firmennetzwerks auf Daten aus dem Firmennetzwerk möglich sein soll. Wenn ein VPN eingesetzt wird oder werden soll, müssen die folgenden Aspekte berücksichtigt werden:

- Der Einsatz von VPNs muss planmäßig angegangen und darf nicht überstürzt umgesetzt werden.
- Wenn ein VPN-Dienstleister genutzt wird, müssen Service Level Agreements ausgehandelt und deren Einhaltung in regelmäßigen Abständen geprüft werden.
- VPN-Clients, -Server und -Verbindungen müssen sicher konfiguriert und implementiert werden. Eine Orientierung hierfür können Leitfäden zur sicheren Implementierung von VPNs bieten.
- VPN-Zugänge sollten nur bei Bedarf und nicht grundsätzlich verteilt werden. Nicht mehr benötigte Zugänge müssen umgehend gelöscht werden.

Weiterführende Informationen zum Thema VPN werden unter anderem durch das BSI zur Verfügung gestellt (Weiterleitung zum BSI: Virtual Private Network (ISi VPN)).

4.3 Sicherheitskonzept

Die Befragung hat ergeben, dass IT-Sicherheit nur bei der Hälfte der Unternehmen im Sicherheitskonzept verankert ist und weniger als die Hälfte verbindliche IT-Sicherheitsziele festgelegt hat. Damit ein angemessenes IT-Sicherheitsniveau zielgerichtet erreicht werden kann, müssen unter anderem die Herangehensweise geplant, so wie feste Verantwortlichkeiten und Vorgehensweisen in einem Sicherheitskonzept festgehalten werden.

Für Unternehmen lassen sich entsprechende Handlungsempfehlungen ableiten:

- Die Gesamtverantwortung der IT-Sicherheit muss durch die Geschäftsführung, beziehungsweise Leitungsebene übernommen werden.
- Legen Sie IT-Sicherheitsziele fest. Fehlinvestitionen können so vermieden und Fortschritte geprüft werden.
- Verankern Sie IT-Sicherheit in dem Sicherheitskonzept des Unternehmens.
- Definieren Sie Rollen und verteilen entsprechende Verantwortlichkeiten (sofern hinsichtlich der Unternehmensgröße und entstandenen Aufgaben sinnvoll).
- Legen Sie für vorhandene Geschäftsprozesse entsprechende Sicherheitsmaßnahmen fest.
- Legen Sie für neue Geschäftsprozesse von Beginn an Sicherheitsmaßnahmen fest.
- Integrieren Sie Ihre Mitarbeiter in den Prozess. Mitarbeiter sind für den täglichen Betrieb des Unternehmens verantwortlich und sollten daher in Maßnahmen, die ihre Arbeit betreffen eingebunden werden. Sie kennen die Abläufe und sehen Verbesserungspotentiale und Änderungen an den Prozessen aus einer anderen Perspektive.
- Weisen Sie auf Konsequenzen bei Nicht-Beachtung hin und schulen Ihre Mitarbeiter, damit das Sicherheitskonzept bekannt ist und gelebt werden kann.

Informationen über die Umsetzung von IT-Sicherheit in einem Sicherheitskonzept stellt das BSI in einer Lerneinheit zur Verfügung und beschreibt Anforderungen in dem Baustein *„ISMS.1 Sicherheitsmanagement“*. Der TÜV-Nord listet in diesem Beitrag elementare Informationen und zentrale Dokumente in Sicherheitskonzepten kleiner und mittlerer Unternehmen auf.

4.4 IT-Sicherheitsbeauftragter/IT-Verantwortlicher

Ein Drittel der Unternehmen gab bei der Befragung an, einen IT-Sicherheitsbeauftragten benannt zu haben. Die Vergabe der Verantwortung für Planung und Kontrolle von IT-Sicherheitsmaßnahmen bringt diverse Vorteile mit sich, weswegen Unternehmen ohne IT-Sicherheitsbeauftragten eine Benennung prüfen und umsetzen sollten. Eine Benennung muss nicht zwingend eine eigene Stelle besetzen, sondern kann bedarfsorientiert ausgelegt und an die Unternehmenssituation angepasst werden. Durch entsprechende Schulungs-, Zertifizierungs-, oder vergleichbare Maßnahmen werden Mitarbeiter auf neue Aufgabenbereiche vorbereitet und erlangen die notwendige Kompetenz, um das IT-Sicherheitsniveau des Unternehmens zu erhöhen. Grundsätzlich lassen sich die folgenden Handlungsempfehlungen ableiten:

- Schaffen Sie eine zentrale Anlaufstelle für Fragen mit IT-Sicherheitsbezug, an die sich Ihre Mitarbeiter wenden können.
- Lagern Sie die Verantwortung für Planung und Kontrolle von IT-Sicherheitsmaßnahmen an die Rolle des IT-Sicherheitsbeauftragten aus und benennen einen internen oder externen IT-Sicherheitsbeauftragten.
- Verteilen Sie die Verantwortung für IT und deren Sicherheit an einen Mitarbeiter der IT – beispielsweise den IT-Verantwortlichen – wenn Sie keinen IT-Sicherheitsbeauftragten benennen können.
- Sorgen Sie dafür, dass der IT-Sicherheitsbeauftragte die Unternehmensziele kennt.
- Investieren Sie in die Kompetenz und Qualifikation Ihres IT-Sicherheitsbeauftragten (sofern es ein interner IT-Sicherheitsbeauftragter ist).
- Etablieren Sie regelmäßige Status Quo-Berichterstattungen zwischen dem IT-Sicherheitsbeauftragten und der Geschäftsführung.

4.5 Verschlüsselung

Die Verschlüsselung von Daten ist eine effektive Möglichkeit, um die Vertraulichkeit von Informationen zu gewährleisten. Verschlüsselte Daten können zwar weiterhin von Angreifern gestohlen, jedoch aufgrund der Verschlüsselung nicht gelesen und weiterverwendet werden. Ein entscheidender Vorteil kryptografischer Schutzmaßnahmen ist der vergleichsweise geringe Aufwand (nach einer einmaligen Einrichtung und Erklärung des Krypto Systems) den Anwender benötigen, um ihre Daten zusätzlich zu sichern. Gerade kritische Daten, wie personenbezogene Daten, Geschäftsgeheimnisse, Zahlungsdaten oder aktuelle Kennzahlen und Planungen müssen vor dem Austausch verschlüsselt werden, da eine Offenlegung verheerende Folgen für das Unternehmen haben könnte. Unternehmen, die ihre Daten nicht durch Verschlüsselung schützen, sollten die folgenden Maßnahmen prüfen und umsetzen

- Prüfen Sie, ob die Verschlüsselung von Daten und Kommunikationswegen mit vertretbarem Aufwand möglich ist.
- Legen Sie fest, welche Daten und Kommunikationswege kritische und schützenswerte Informationen enthalten.
- Wählen Sie geeignete kryptografische Verfahren aus.
- Führen Sie ein geeignetes Schlüsselmanagement ein.
- Etablieren Sie die Verschlüsselung von Daten und Kommunikationswegen.

Neben der Verschlüsselung ausgetauschter Informationen ist es empfehlenswert, Datensicherungen durch Verschlüsselung zu schützen. Diese Maßnahme verhindert, dass Unbefugte die Datenträger stehlen und die Datensicherungen auf ihren Systemen nutzen können.

Das Bundesministerium für Wirtschaft und Energie (kurz: BMWi) stellt kleinen und mittleren Unternehmen mit seinem *„Kompass IT-Verschlüsselung“* ein Werkzeug zur Verfügung, das aktuelle Verschlüsselungsmaßnahmen gebündelt erklärt und somit als Orientierungs- und Entscheidungshilfe dient. Informationen über potentielle Gefahren bei der Etablierung und generelle Anforderungen an ein Kryptokonzept erläutert das BSI in seinem IT-Grundschutz Kompendium in dem Baustein *„CON.1 Kryptokonzept“*.

4.6 Mobilgeräte

Jedes Unternehmen welches Mobilgeräte einsetzt, sollte sich auch mit der sicheren Handhabung dieser beschäftigen. Nur durch schriftlich fixierte Vorgaben zur Nutzung z.B. in Form von Richtlinien, lassen sich die mit dem Einsatz von Mobilgeräten verbunden Risiken richtig einschätzen und bestmöglich begrenzen. Insbesondere für Unternehmen mit einer größeren Anzahl von Mobilgeräten, ist der Einsatz eines Mobile Device Management zu empfehlen. Mit einer solchen Software lassen sich die Endgeräte zentral verwalten und Sicherheitsregeln durchsetzen. Im Ernstfall können hierdurch Notfallaktion wie eine Fernlöschung durchgeführt werden. Weitreichende Informationen zum Richtigen Umgang mit Smartphones bzw. Tablets werden über das BSI im Grundschutz Baustein *„SYS.3.2.1 Allgemeine Smartphones und Tablets“* zur Verfügung gestellt. Informationen zum richtigen Einsatz eines Mobile Device Management befinden sich im Baustein *„SYS.3.2.2 Mobile Device Management (MDM)“*.

4.7 Mitarbeitersensibilisierung

In der Befragung gaben gut die Hälfte der größeren und nur rund jedes vierte der kleineren KMUs an, ihre Mitarbeiter mittels Schulungen für IT-Sicherheit zu sensibilisieren. Dies erscheint angesichts der elementaren Bedeutung von informierten und geschulten Mitarbeitern, viel zu gering. Die Unternehmen sollten also prüfen, ob sie ein geeignetes Schulungskonzept für ihre Mittarbeiter anbieten. Zur Überprüfung oder Konzeption eines zielgruppengerechten Schulungskonzepts, bietet das BSI im IT-Grundschutz Kompendium *„ORP.3 Sensibilisierung und Schulung“* eine Hilfestellung. Wenn z.B. aufgrund der Unternehmensgröße die Erstellung eines eigenen Schulungskonzept nicht gewünscht oder wirtschaftlich sinnvoll ist, können externe Dienstleister zur Durchführung von Schulungen und zur Erstellung von Schulungskonzepten beauftragt werden.

4.8 Datensicherung

Die Ergebnisse der Befragung zeigen auf, dass die Unternehmen bereits ein hohes Sicherheitsniveau in Bezug auf die Datensicherung erreicht haben (95% gaben an eine regelmäßige Datensicherung durchzuführen). Mit 53% gaben jedoch nur gut die Hälfte der befragten Unternehmen an, ihre Backup Strategie schriftlich dokumentiert zu haben. Dies kann insbesondere dann kritisch werden, wenn z.B. der Verantwortliche für die Datensicherung kurzfristig ausfällt oder das Unternehmen verlässt. Unternehmen sollten also kurzfristig prüfen ob ein Datensicherungskonzept besteht und ob sie dieses auch in angemessener Weise dokumentiert haben.

Hilfestellung bei der Entwicklung und Dokumentation eines geeigneten Datensicherungskonzept bietet das BSI im IT-Grundschutz mit dem Baustein *„CON.3 Datensicherungskonzept“*.

4.9 Notfallbehandlung

Die Grundlage für einen effektiven Umgang mit IT-Sicherheitsvorfällen stellt das Notfallkonzept dar. Die kleineren KMUs gaben zu 33% und die größeren KMUs zu 46% an, ein Notfallkonzept erstellt zu haben (Abb. 31). In Anbetracht der Selbsteinschätzung zum Schutzbedarf der im Unternehmen gespeicherten Daten (über 80% der KMUs sagten „eher hoch“ bzw. „sehr hoch“), erscheint die Erstellung eines Notfallkonzept, bei noch zu wenigen Unternehmen in der Region umgesetzt zu sein.

Der Aufwand für die Erstellung eines unternehmensindividuellen Notfallkonzept, ist immer im angemessenen Verhältnis zum Schutzbedarf der jeweiligen Unternehmung zu betrachten.

Hilfestellung bei der Entwicklung und Dokumentation eines geeigneten Notfallkonzept bietet das BSI im IT-Grundschutz mit dem Baustein *„DER.4 Notfallmanagement“*.

4.10 Datenschutz

Der Block Datenschutz behandelte maßgeblich die Fragen zur Umsetzung der DSGVO. Die Unternehmen in der Region gaben in der Befragung an, grundsätzlich über die Anforderung in Teilbereichen der DSGVO informiert zu sein.

Lediglich zu den Meldepflichten bei Datenpannen scheint bei den kleineren KMUs noch Unsicherheit zu bestehen. Die IHK Mittlerer Niederrhein stellt Informationen zu den Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen auf Ihrer *Webseite* zur Verfügung.

Trotz der hohen Selbsteinschätzung zu dem Wissen in den Teilbereichen der DSGVO, bezeichneten sich nur lediglich 48% der Unternehmen als gänzlich DSGVO konform. Dies zeigt das immer noch Verunsicherung zur Umsetzung der DSGVO besteht.

Die IHK Mittlerer Niederrhein bietet auf Ihrer Webseite einen vom Bayrischen Landesamt für Datenschutz (BayLDA) erstellen *Fragebogen* zur Umsetzung der DSGVO an. Unternehmen, die für sich noch Handlungsbedarf sehen, können mithilfe des Fragebogen Unsicherheiten zur Umsetzung der DSGVO abbauen.

5 Fazit

Die Ergebnisse der Befragung zeigen, dass sich Unternehmen der Region Mittlerer Niederrhein der Notwendigkeit von IT-Sicherheitsmaßnahmen bewusst sind. Ebenso bewusst sind sich die Unternehmen der steigenden Bedrohung und Zunahme der Risiken durch IT-Sicherheitsvorfälle, weswegen die Informationssicherheit vielfach einen hohen bis sehr hohen Stellenwert besitzt.

Unternehmen in der Region sind in einigen Bereichen, wie beispielsweise Datensicherung, Datenschutz und Infrastruktur, bereits gut aufgestellt und haben viele Maßnahmen umgesetzt. Die umgesetzten Sicherheitsmaßnahmen schützen häufig die Verfügbarkeit und Funktionalität von IT-Systemen und Daten. Unternehmen sollten sich nicht nur auf die reine Verfügbarkeit ihrer Systeme konzentrieren, sondern Aspekte wie Integrität, Vertraulichkeit und Authentizität nicht vernachlässigen. Die anderen Bereiche und Aspekte bieten ungenutzte Verbesserungspotentiale und tragen zu einer Verbesserung des IT-Sicherheitsniveaus bei.

Die genauere Betrachtung der bereits etablierten IT-Sicherheitsmaßnahmen zeigt eine nicht unerhebliche Diskrepanz zwischen unterschiedlich großen Unternehmen auf. Auch wenn diese Diskrepanz keine regionale Besonderheit, sondern auch überregional zu beobachten ist, verdeutlicht sie die Probleme, die gerade kleine Unternehmen bei der Einführung und Etablierung entsprechender Schutzmaßnahmen haben.

Die Erhebung zeigt, dass die größten Hemmnisse bezüglich der Verbesserung des IT-Sicherheitsniveaus

- Ein zu großes und undurchsichtiges Angebot,
- Zu hohe Investitionskosten
- Und ein mangelndes Sicherheitsbewusstsein bei Mitarbeitern

sind.

Zusätzlich zu der bisherigen Sensibilisierung für IT- und Informationssicherheit sollten Unternehmen über aktuelle Vorgehensweisen und Standards, wie beispielsweise den BSI-Grundschutz, die ISO27000er Reihe oder Vergleichbare, informiert werden. So können Unternehmen die Risiken, der Nutzen und konkreten Kosten nähergebracht, von Diesen in ein Verhältnis gestellt und die Etablierung entsprechender Schutzmaßnahmen wirtschaftlich betrachtet werden.

Die Unternehmen selbst sollten dazu bereit sein, in ihre Mitarbeiter zu investieren und sie zu entsprechenden Themen der IT- und Informationssicherheit zu sensibilisieren. Insbesondere große und mittlere KMUs gaben an, dass die Mitarbeiter die Hauptursache möglicher IT-Probleme sind und deren Schulung die sinnvollste Maßnahme zur Verbesserung des IT-Sicherheitsniveaus ist. Maßnahmen für eine solche Sensibilisierung können zum Beispiel Informationsveranstaltungen und Schulungsangebote externer Anbieter, so wie frei zugängliche Informationen durch Quellen wie das BSI sein.

Abschließend kann gesagt werden, dass es einen nicht verwunderlichen Unterschied zwischen dem IT-Sicherheitsniveau kleiner und mittlerer Unternehmen gibt. Gerade kleine Unternehmen haben oft nicht das nötige Fachwissen und Geld, um sich intensiv mit dem Thema IT- und Informationssicherheit zu beschäftigen. Dennoch sollten sich Unternehmen über aktuelle Themen und Neuigkeiten aus dem Bereich der IT-Sicherheit informieren, um sich entsprechend schützen zu können. Wenn Mitarbeiter mit sensiblen Firmendaten arbeiten, sollten sie entsprechend für die Sicherheit dieser Daten sensibilisiert werden. Unternehmen sollten das Thema IT-Sicherheit zielgerichtet angehen, um so relevante und essenzielle Sicherheitsmaß-

nahmen bestimmen zu können. Wenn der Einsatz von IT-Sicherheitsmaßnahmen konzeptionell angegangen, geplant und kontrolliert wird und Mitarbeiter entsprechend geschult und sensibilisiert werden, können Unternehmen ihr IT-Sicherheitsniveau auch ohne enorme Kosten verbessern und IT-Sicherheitsvorfällen vorbeugen. Da Unternehmen ihre Angestellten als eine der Hauptursachen möglicher IT-Probleme sehen, sollte der Fokus auf deren Sensibilisierung gelegt werden, um so eine nachhaltige IT-Sicherheitskultur etablieren zu können.

Quellenverzeichnis

Quellen der Handlungsempfehlungen (Kapitel 4)

In dieser Übersicht finden Sie die in Kapitel 4 verlinkten und erwähnten Quellen in einer komprimierten, übersichtlichen Form. Da die nachfolgenden Übersichten größtenteils Link-Sammlungen sind, wird auf einen wissenschaftlichen Zitierstil verzichtet, um die Übersichtlichkeit und Zugänglichkeit zu wahren. Die Verfügbarkeit und Funktionalität aller Links wurden zuletzt am 08.07.2019 geprüft.

Industrie- und Handelskammer Mittlerer Niederrhein

Fragebogen zur Umsetzung der DSGVO
https://www.ihk-krefeld.de/de/media/pdf/recht/gvo/nr.-7-fragebogen-zur-umsetzung-der-ds-gvo.pdf
Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen
https://www.ihk-krefeld.de/de/media/pdf/recht/gvo/nr.-11-melde-und-benachrichtigungspflichten-bei-datenschutzverletzungen.pdf

ISO/IEC 27000er Familie

Bundesamt für Sicherheit in der Informationstechnik

BSI-Standards
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html
IT-Grundschutz Downloadbereich
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzDownloads/itgrundschutzDownloads_node.html
IT-Grundschutz Kompendium
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2019.html
Leitfaden zur Einführung von IDS
https://www.bsi.bund.de/DE/Publikationen/Studien/IDS02/index_htm.html
Virtual Private Network (ISi-VPN)
https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-VPN/vpn_node.html
Lerneinheit: Sicherheitskonzepte
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/OnlinekursITGrundschutz2018/Lektion_2_Sicherheitsmanagement/Lektion_2_08/Lektion_2_08_node.html

TÜV Nord

IT-Sicherheit in kleinen und mittelständischen Unternehmen
https://www.tuev-nord.de/de/unternehmen/bildung/wissen-kompakt/it-sicherheit/it-sicherheit-in-kmu/

VdS 10000: Informationssicherheitsmanagementsysteme für kleine und mittlere Unternehmen (KMU)

VdS 10000 (PDF)
https://vds.de/fileadmin/vds_publikationen/cyber/V10000_low.pdf
VdS – Cyber Security
https://vds.de/de/cyber/

Weiterführende Literatur

Neben den in Kapitel 4 erwähnten Informationsquellen sind in der nachfolgenden Übersicht Quellen aufgeführt, bei denen es zu verschiedenen Bereichen der IT-Sicherheit weiterführende Informationen gibt.

Übersicht über branchenspezifische Sicherheitsstandards (B3S)
https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/Was_tun/Stand_der_Technik/B3S/B3S.html

Bundesamt für Sicherheit in der Informationstechnik
Leitfaden zur Basis-Absicherung nach IT-Grundschutz (Übersicht)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.html
Leitfaden zur Basis-Absicherung nach IT-Grundschutz (PDF)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.pdf?__blob=publicationFile&v=3
Standards zur Internet-Sicherheit (ISi-Reihe)
https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-Reihe_node.html

Bundesministerium für Wirtschaft und Energie
Kompass IT-Verschlüsselung
https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/kompass-it-verschluesselung.html
Kompass IT-Verschlüsselung (PDF)
https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/kompass-it-verschluesselung.pdf?__blob=publicationFile&v=18

Industrie- und Handelskammer Mittlerer Niederrhein
Leitfäden und Broschüren
https://www.ihk-krefeld.de/de/digitalisierung-internet/datenschutz-und-it-sicherheit/leitfaeden-whitepaper-und-broschueren.html

Anhang

Methodik

Konstruktion des Fragebogens

Der Fragebogen wurde in zwölf Kategorien unterteilt. Die ersten drei Kategorien beschäftigen sich mit Strukturdaten zur Einordnung der Unternehmen und deren individueller Einstellung und Bewertung der Bedeutung von IT-Sicherheit. Die verbleibenden neun Kategorien sind: Infrastruktur, Sicherheitskonzept, IT-Sicherheitsbeauftragter, Verschlüsselung, Mobilgeräte, Mitarbeitersensibilisierung, Datensicherung, Notfallbehandlung und Datenschutz. Durch die gewählte Kategorisierung wird eine breit gefächerte Betrachtung verschiedener Sicherheitsaspekte und -Maßnahmen ermöglicht. Die Reihenfolge der Kategorien hat keinen fachlichen Hintergrund. Inklusiver zwei abschließender Feedback-Fragen besteht der Fragebogen aus 88 Fragen. Bei den Fragen werden Single-Choice, Multiple-Choice, Freitext und Skalenniveaus als Antwortmöglichkeiten eingesetzt.

Durchschnittliche Befragungsdauer

Die Durchführung von Pretests durch Mitarbeiter von Clavis, der IHK und fachfremde Probanden (Familie und Freunde der Testersteller) ergab eine durchschnittliche Bearbeitungsdauer von 22 Minuten.

Befragungszeitraum

Die Befragung wurde vom 15.02.2019 bis zum 15.05.2019 durchgeführt.

Auswertung und Dokumentation

Die Ergebnisse der Befragung wurden vom 15.05.2019 bis zum 13.06.2019 ausgewertet und verschriftlicht.

Handlungsempfehlungen

Die Handlungsempfehlungen in Kapitel 4 wurden auf Grundlage der Auswertungsergebnisse in Kapitel 3 getroffen. Sie orientieren sich an etablierten Handlungsempfehlungen und IT-Sicherheitsmaßnahmen aus anerkannten Leitfäden, offiziellen Standards, bewährten Vorgehensweisen und Richtlinien. Die Maßnahmen richten sich an Unternehmen diverser Branchen, Mitarbeiterzahlen und Jahresumsatz, weswegen sie vor ihrer Umsetzung von den Unternehmen auf Relevanz untersucht werden sollten.

Grundgesamtheit

Die Grundgesamtheit bildeten kleine und mittelständische Unternehmen, die Mitglieder der IHK Mittlerer Niederrhein sind.

Die Befragung wurde als Betriebsbefragung ausgelegt. Unternehmen mit mehreren Standorten in der Region wurden nicht mehrfach befragt. Zielpersonen in den Unternehmen waren die Geschäftsführer oder IT-Verantwortlichen.

Kontaktdaten

Die Kontaktdaten der Unternehmen waren aus dem Bestand der IHK. Unternehmen wurden entweder direkt durch die IHK kontaktiert (zufällige Auswahl der kontaktierten Unternehmen), oder über Newsletter auf die Online-Befragung aufmerksam gemacht.

Stichprobengröße

Neben der Online-Befragung wurden 3.600 zufällig ausgewählte KMUs postalisch durch die IHK kontaktiert und um Teilnahme an der Befragung gebeten. Durch die Maßnahmen der Online-Bewerbung und postalischen Bewerbung lagen im Ergebnis 133 abgeschlossene Interviews vor, von denen n=115 verwertbare Interviews waren. Die Größen der teilgenommenen Unternehmen verteilen sich auf:

- 1 – 10 Mitarbeiter
  n = 33 Interviews
- 11 – 49 Mitarbeiter
  n = 45 Interviews
- 50 – 99 Mitarbeiter
  n = 13 Interviews
- 100 – 499 Mitarbeiter
  n = 24 Interviews

Befragungsmethodik

Die Befragung wurde in Form einer Online-Befragung mit dem Befragungstool „SoSci Survey“ durchgeführt. Unternehmen wurden per Newsletter auf die Online-Befragung aufmerksam gemacht und zur Teilnahme angeregt. Zusätzlich zu der Bewerbung durch Newsletter wurde ein Beitrag im IHK-Magazin (Ausgabe März 2019) veröffentlicht. Des Weiteren wurden 3.600 zufällig ausgewählte KMUs postalisch durch die IHK kontaktiert und um Teilnahme an der Befragung gebeten. Diesen Unternehmen wurde eine Print-Version der Befragung mitgesendet. Diese Print-Version konnten die Unternehmen dann an Clavis senden, wo die Interviews dann in das Online-Tool überführt wurden. Die Überführung der Print-Versionen wurde von zwei Angestellten von Clavis durchgeführt.

Validierung und Schutz der erhobenen Daten

Die erhobenen Daten werden komplett anonymisiert gespeichert. Erfolgreich abgeschlossene Interviews werden auf Vollständigkeit, Plausibilität und Konsistenz geprüft. Diese Prüfung geschieht in zwei Schritten. In einem ersten Schritt wird die Vollständigkeit automatisch durch das Befragungstool geprüft. In einem zweiten Schritt prüfen Angestellte von Clavis die Daten händisch auf Vollständigkeit, Plausibilität und Konsistenz. Der zweite Schritt wird blockweise und nicht nach jedem abgeschlossenen Interview durchgeführt.

Die Daten werden so gespeichert, dass der endgültige Verlust der Daten ausgeschlossen und eine Manipulation verhindert wird. Es werden regelmäßige Backups der Daten erstellt, die getrennt voneinander und in unterschiedlichen Städten aufbewahrt werden.

Abbildungsverzeichnis

Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik
DSGVO	Datenschutz-Grundverordnung
EDV	elektronische Datenverarbeitung
Etc	et cetera
IHK	Industrie- und Handelskammer
IKT	Informations- und Kommunikationstechnik
ISO	International Organization for Standardization
IT	Informationstechnik
KMU	Kleine und mittlere Unternehmen
PC	Personal Computer
SD	Storage Device
USB	Universal Serial Bus
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
z.B.	zum Beispiel

Checkliste: Erste Schritte zu einer guten IT-Sicherheit

Um die IT-Sicherheit Ihres Unternehmens zu erhöhen, bedarf es nicht zwingend zu Beginn große Investitionen. In der nachfolgenden Checkliste sind einzelne erste Schritte aufgeführt, die ein solides Fundament schaffen sollen, auf dem künftige Maßnahmen aufbauen.

- [ ] Prüfen Sie, welche Bedrohungen (technischer Art) für Ihr Unternehmen von Relevanz sind. Wer die Bedrohung kennt, kann sich dagegen schützen.

- [ ] Analysieren Sie, welchen Schaden diese Bedrohungen anrichten könnten. So können Sie sich bereits im Vorfeld Gedanken zu jeglichen „Was-wär-wenn-Szenarien“ machen und überlegen, wie dann gehandelt werden soll.

- [ ] Schreiben Sie allgemeine Nutzungsrichtlinien mit Ge- und Verboten für die Nutzung der Firmengeräte. Gerade hinsichtlich der Nutzung im Internet (keine illegalen Seiten besuchen etc.).

- [ ] Suchen Sie nach leicht verständlichen/zugänglichen Informationsquellen über aktuelle Sicherheitslücken, Angriffstechniken o.d.G. (z.B. durch Newsletter von Behörden oder Informationsveranstaltungen, der Security-Rubrik der heise.de-News, eines CERTs, oder dem „Bürger-CERT“ des BSI), um sich so – sofern nötig – rechtzeitig schützen zu können.

- [ ] Erstellen Sie eine Übersicht über die von Ihnen verwendete IT (Stichwort: Netzwerkplan, Asset-Liste).

- [ ] Erstellen Sie ein Identitäts- und Berechtigungsmanagement, bzw. sprechen Sie mit Ihrem Dienstleister darüber.

- [ ] Suchen und installieren Sie eine für Sie geeignete Schutzsoftware.

- [ ] Sichern Sie Ihren Server/Serverraum zusätzlich ab.

- [ ] Prüfen Sie, ob Sie Daten speichern, die eine besondere Sicherheit (z.B. durch Verschlüsselung) benötigen.

- [ ] Führen Sie regelmäßige Backups durch und legen Verantwortungen in einer Backup-Strategie fest.