Untersuchung zur Wirksamkeit der IT-Sicherheitsgesetze unter Betreibern Kritischer Infrastrukturen

erarbeitet für

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt
für Sicherheit in der
Informationstechnik

Ergebnisbericht

Durchführung:

INFO GmbH Markt- und Meinungsforschung

April 2023

INHALT

IMPRESSUM

INFO GmbH Markt- und Meinungsforschung

Ein Unternehmen der INFO Research Group.

Schönholzer Straße 1A, D-13187 Berlin

Tel. +49-30/49001-0 / Fax +49-30/49001-499

kontakt@infogmbh.de

https://www.infogmbh.de

Geschäftsführer: Dr. Holger Liljeberg

Prokuristinnen: Dipl.-Psych. Sindy Krambeer, Dipl.-Soz. Eileen Liljeberg

Berlin, 13. April 2023

1. ZUSAMMENFASSUNG

Die **Umsetzung technischer Sicherheitsmaßnahmen** ist bei den meisten Unternehmen weit vorangeschritten, insbesondere VPN und Zugangskontrollen, die nur in Einzelfällen noch nicht implementiert sind. Am geringsten ist der Umsetzungsstand bei der Client-Isolation, DDoS-Mitigation und der sicheren Software-Entwicklung. Großunternehmen liegen hier fast durchweg vor den kleinen und mittleren Unternehmen (KMU).

Bei der **Umsetzung organisatorischer Sicherheitsmaßnahmen** liegen die Unternehmen etwas weiter zurück. Weitgehend flächendeckend eingeführt sind jedoch die Aufrechterhaltung des aktuellen Informationsstandes und die Sensibilisierung/ Schulung der Mitarbeitenden. Die größten Defizite zeigen sich bei der Einführung von Security Operations und einer sicheren Dokumentenerstellung.

EnWG-/ TKG-Betreiber haben bei der Implementierung der technischen Maßnahmen einen leichten, bei der Einführung der organisatorischen Maßnahmen einen deutlichen Vorsprung gegenüber den anderen KRITIS-Unternehmen.

Hauptgrund für die Einführung von Sicherheitsmaßnahmen ist die aktuelle IT-Bedrohungslage, aber auch die IT-Sicherheitsgesetzgebung spielt dafür eine wichtige Rolle – bei KMU ist sie sogar fast ebenso so groß.

Das **IT-Sicherheits-Budget** wird von der Mehrheit als nicht angemessen beurteilt, auch wenn sechs von zehn Unternehmen es in den letzten zwei Jahre erhöhten: Den Anteil am gesamten IT-Budget - im Durchschnitt 14 Prozent - hält nur jedes dritte Unternehmen für ausreichend. KMU, die über einen etwas höheren prozentualen Anteil verfügen als Großunternehmen, äußern sich häufiger zufrieden.

Sieben von zehn Unternehmen, deutlich stärker jedoch Großunternehmen als KMU, nehmen gegenwärtig eine **erhöhte IT-Bedrohungslage** wahr. Als **Hauptursachen** werden der Ukraine-Krieg bzw. die geopolitische/ weltpolitische Lage sowie die zunehmenden und gezielten Angriffe auf KRITIS-Betreiber genannt. EnWG /TKG-Unternehmen beobachten häufiger eine erhöhte IT-Gefährdungslage als die Unternehmen anderer Sektoren.

Nicht alle, aber immerhin doch ein Großteil der besorgten Unternehmen erlebte in den vergangenen zwei Jahren eine stärkere Gefährdungslage speziell aufgrund häufigerer **Cyber-Angriffe auf das eigene IT-System**. Auch hier waren Großunternehmen stärker betroffen als KMU. Die mit Abstand häufigsten Cyber-Attacken erfolgten in Form von Phishing und Schadsoftware in Mailanhängen.

Zwei Drittel der von Cyber-Angriffen betroffenen Unternehmen erlitten einen **materiellen Schaden**, Großunternehmen beziffern ihn im Durchschnitt auf 157.000 Euro, KMU auf 71.000 Euro. Kosten

ergaben sich vor allem durch die Beauftragung von Dienstleistern, die Wiederherstellung der Systeme und den Betriebsausfall. Der wirtschaftliche Schaden fiel bei den meisten Unternehmen jedoch nur wenig ins Gewicht, existenzbedrohend war er in keinem Fall.

Der **aktuelle Stand der IT-Entwicklung und Digitalisierung** könnte höher sein: Zwar bezeichnet ihn kaum ein Unternehmen als schlecht, aber auch nur knapp unter der Hälfte der Befragten als sehr gut/ gut, darunter mehr KMU als Großunternehmen.

Der Aspekt der **Informationssicherheit** spielt im Zuge der Digitalisierung für so gut wie alle Unternehmen eine Rolle und wird mehrheitlich von Anfang an mitgedacht, spätestens aber im Laufe der Implementierung berücksichtigt. EnWG-/ TKG-Unternehmen denken diesen Aspekt etwas häufiger von Anfang an mit als die anderen KRITIS-Betreiber.

Ebenso erfolgt in fast allen Unternehmen eine regelmäßige **Dokumentation der IT-Sicherheitsvorfälle,** meist in einem internen System.

Das BSI ist der mit Abstand wichtigste Adressat für die **Kommunikation von Sicherheitsvorfällen**. Am häufigsten informiert werden daneben auch kooperierende Unternehmen, andere Behörden, Kunden, und Lieferanten.

Für Unternehmen mit einem geringeren Umsetzungsstand der gesetzlichen Maßnahmen (bis 70 %) spielen die Informationssicherheit, die Dokumentation von IT-Sicherheitsvorfällen und deren Kommunikation nach außen eine etwas geringere Rolle.

Die **Beseitigung von Sicherheitslücken** verläuft in unterschiedlichem Tempo. Dabei agieren KMU etwas häufiger sofort, Großunternehmen häufiger entlang einer Priorisierung im Rahmen einer Risikobewertung. Auch Nicht-EnWG-/ TKG-Unternehmen führen am häufigsten zunächst eine Risikobewertung durch, während bei EnWG-/ TKG-Betreibern die umgehende Beseitigung und die Priorisierung/ Risikobewertung etwa gleichauf liegen.

Die meisten KRITIS-Betreiber, die nicht (ausschließlich) unter die gesetzlichen Regelungen Energiewirtschaftsgesetz (EnWG) oder Telekommunikationsgesetz (TKG) fallen, sind mit den beiden **IT-Sicherheitsgesetzen** - überwiegend sogar sehr gut – vertraut. Großunternehmen geben dabei deutlich häufiger als KMU an, sich mit der IT-Gesetzgebung sehr gut auszukennen.

Die drei häufigsten **Auswirkungen der Gesetze und ihrer Änderungen** auf die Unternehmen sind ein erhöhter Dokumentations-/ Prüfaufwand, der Einführung/ der Aufbau von Sicherheitssystemen und die (schnellere) Einführung neuer Maßnahmen. Letzteres wird überdurchschnittlich häufig von Unternehmen mit geringerem Umsetzungsstand genannt.

Acht von zehn Nicht-EnWG/ TKG-Betreibern haben **aufgrund der geänderten IT-Sicherheitsgesetzgebung neue Projekte** zur Erhöhung der IT-Sicherheit umgesetzt oder zeitlich vorgezogen.

Schulungen der Mitarbeitenden im Zusammenhang mit dem ersten IT-SiG und dem IT-SiG 2.0 führten sieben von zehn Unternehmen durch; meist erfolgten sie intern.

Fast alle Unternehmen überwachen die **Einhaltung der gesetzlichen Anforderungen** regelmäßig. Firmen mit geringer/ mittlerer Vertrautheit mit der IT-Gesetzgebung sowie Firmen mit einem geringen Umsetzungsstand kontrollieren deren Einhaltung vergleichsweise am häufigsten nur sporadisch.

Der **Umsetzungsstand der gesetzlichen Maßnahmen** ist in den Nicht-EnWG/ TKG-Unternehmen recht hoch. Bis auf eine Ausnahme (Maßnahmen zur Kontrolle von Lieferanten, Dienstleistern und Dritten) sind sie im Durchschnitt zu mindestens drei Vierteln realisiert. KMU sind dabei etwas weiter vorangeschritten als die Großunternehmen.

Nicht-EnWG/ TKG-Unternehmen mit geringerem Umsetzungsstand haben den größten Nachholbedarf bei den Maßnahmen zur Kontrolle von Dritten, Überprüfungsmaßnahmen im laufenden Betrieb und Maßnahmen zur Sicherstellung der Betriebskontinuität.

Als **Hauptgründe für die noch unvollständige Umsetzung der gesetzlichen Anforderungen** gelten vor allem Personalmangel und fehlende finanzielle Mittel. Vor allem KMU und Betriebe mit geringer/ mittlerer Vertrautheit mit der IT-Gesetzgebung beklagen zudem die Zeitknappheit/ zu kurzfristige Änderungen. Bei Unternehmen mit einem geringeren Umsetzungsstand spielt neben einem allgemeinen Ressourcenmangel auch fehlendes Knowhow eine vergleichsweise große Rolle.

Etwa die Hälfte der befragten Nicht-EnWG/ TKG-Unternehmen will die erforderlichen Maßnahmen bis spätestens Ende des nächsten Geschäftsjahres **vollständig umgesetzt** haben. KMU planen eine schnellere Umsetzung als Großunternehmen. Unternehmen mit geringerem Umsetzungsstand gehen mehrheitlich von einem längeren Zeitraum aus.

Die große Mehrheit der Nicht-EnWG/ TKG-Befragten hält eine **vollständige Umsetzung der gesetzlichen IT-Sicherheitsvorgaben bei KRITIS-Betreibern** für wichtig. Das trifft - wenn auch auf etwas geringerem Niveau – auch auf Unternehmen zu, die mit der Gesetzgebung nicht gut vertraut sind, ihr nur einen geringen/ keinen Einfluss zuschreiben oder deren Umsetzungsstand bisher gering ist.

Die Kosten für die Anpassung von IT-Systemen/ -Prozessen sind die mit Abstand **größte Herausforderung bei der Umsetzung der IT-Sicherheitsgesetze**, gefolgt von Kosten für externe Dienstleister und fehlendem Knowhow.

Nahezu alle Nicht-EnWG/ TKG-Betreiber stellen sicher, dass ihre IT-Sicherheitsmaßnahmen die gesetzlichen Anforderungen erfüllen, meist durch externe **Audits** und Zertifizierungen.

Die gesetzlichen Vorgaben haben bei den KRITIS-Unternehmen, die nicht (ausschließlich) unter das EnWG/ TKG fallen, eine hohe **Akzeptanz** und werden als **wirksam** erlebt: Neun von zehn Unternehmen halten sie für sinnvoll, über drei Viertel bestätigen ihren positiven Einfluss auf die IT-Sicherheit, knapp drei Viertel beobachten eine höhere Sensibilisierung von Mitarbeitenden und Geschäftsführung.

Die meisten **BSI-Publikationen** sind der Mehrheit aller KRITIS-Unternehmen (inkl. EnWG/ TKG-Betreiber) bekannt. Die größte **Bekanntheit** haben die Tageslageberichte, die Cyber-Sicherheitswarnungen und der Jahreslagebericht, am wenigsten bekannt sind die Management-Berichte, die auch allgemein am seltensten genutzt werden. Vorne in der **Nutzung** liegen die Tageslageberichte, die Cyber-Sicherheitswarnungen und die Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung. Großunternehmen rezipieren die BSI-Publikationen häufiger als KMU, die nur bei den Cyber-Sicherheitsmaßnahmen nahezu gleichauf liegen.

Die BSI-Veröffentlichungen stoßen allgemein auf **Zufriedenheit**. Fast alle haben schon einmal einen **praktischen Nutzen** aus ihnen abgeleitet. Zu den am häufigsten geäußerten **Wünschen** an das Informationsangebot des BSI gehören mehr zielgruppen-/ branchenspezifische Informationen und konkrete Lösungsansätze/ Umsetzungshinweise.

KRITIS-Unternehmen, die nicht unter das EnWG/ TKG fallen, nutzen die BSI-Orientierungshilfen und Informationen zur Nachweiserbringung deutlich häufiger als die EnWG/ TKG-Betreiber. Diese wiederum äußern häufiger einen Mehrbedarf an detaillierteren Informationen, etwa zu ihrer Branche.

Bei den Nicht-EnWG/ TKG-Unternehmen ist die **Bekanntheit der inhaltlichen Anforderungen an die Nachweise**, die dem BSI alle zwei Jahre vorgelegt werden müssen, wesentlich höher als die vom BSI-Gesetz formulierte **„Absicherung nach dem Stand der Technik“**, die der Mehrheit nur ansatzweise oder in Teilen bekannt ist. Großunternehmen sind zu beiden Themen besser informiert als KMU.

Die weitaus meisten Nicht-EnWG-/ TKG-Unternehmen, in deren Sektor es einen **branchenspezifischen Sicherheitsstandard (B3S)** gibt, wenden ihn an, über zwei Drittel sprechen ihm einen Mehrwert zu. Bei den Betrieben, die über keinen B3S verfügen, ist keine klare Mehrheit für den **Wunsch nach Einführung eines Sicherheitsstandards** zu erkennen.

Nicht-EnWG-/ TKG-Unternehmen, die schon einmal einen **Mängelbericht an das BSI** geschickt haben, haben damit überwiegend positive Erfahrungen im Sinne einer Erhöhung der IT-Sicherheit nach der Mängelbeseitigung gemacht.

Die **Wirksamkeit der IT-Sicherheitsgesetze** kann insgesamt als gut bewertet werden. Die Defizite in der Umsetzung der Anforderungen liegen weniger an fehlender Bekanntheit oder mangelndem Willen seitens der Unternehmen als an deren fehlenden finanziellen und personellen Ressourcen. Unternehmen mit geringem Umsetzungsstand haben häufig eine geringere Kenntnis der IT-Gesetze, die es zu

verbessern gilt.

2. UNTERSUCHUNGSDESIGN

Grundgesamtheit für die Erhebung waren alle beim BSI gelisteten Betreiber von Kritischen Infrastrukturen (KRITIS). Die Einladung zur Teilnahme erfolgte durch das BSI mit einem individualisierten Link. An der Befragung beteiligten sich insgesamt 379 KRITIS-Unternehmen.

Die Befragung wurde im Zeitraum vom 21. Februar 2023 bis 12. März 2023 durchgeführt und in Form von Online-Interviews (CAWI = Computer assisted Web Interviewing) realisiert.

Um repräsentative Gesamtergebnisse zu erzielen, wurde der vollständige Datensatz nach dem Merkmal Sektor (anhand der Verteilung der angeschriebenen Unternehmen) gewichtet.

Im Bericht dargestellt werden die Auswertungsgruppen Unternehmensgröße (KMU/ Großunternehmen), Vertrautheit mit dem IT-Sicherheitsgesetz 2.0, Umsetzung der Anforderungen im Unternehmen, Wirksamkeit der durch das erste IT-Sicherheitsgesetz und das IT-Sicherheitsgesetz 2.0 geforderten Maßnahmen und deren Umsetzung, die Wahrnehmung einer erhöhten Sicherheitslage sowie (Nicht-)EnWG/ TKG-Unternehmen.

3. STRUKTURDATEN

Der Anteil der Großunternehmen (> 250 Angestellte) an der Befragung beträgt 59 Prozent. Zwei Drittel dieser Unternehmen (67 %) beschäftigen über 1.000 Angestellte.

Die kleinen und mittleren Unternehmen (KMU), deren Anteil bei 40 Prozent liegt, haben zur Hälfte (51 %) 21 bis 100 Mitarbeitende. Bei 31 Prozent der KMU sind 101 bis 250 Personen beschäftigt, bei 19 Prozent weniger als 21 Mitarbeitende.

54 Prozent der Befragten - 61 Prozent der KMU und 44 Prozent der Großunternehmen - betreiben Anlagen, die unter das Energiewirtschafts- (EnWG) oder das Telekommunikationsgesetz (TKG) fallen.

Registrierung als KRITIS-Betreiber: Gut die Hälfte (54%) der Unternehmen ist seit bis zu fünf Jahren beim BSI als KRITIS-Betreiber gemeldet, 46 Prozent seit mehr als fünf Jahren.

Die Großunternehmen sind im Durchschnitt schon länger registriert als die KMU, ihr Mittelwert liegt bei sechs Jahren. Gut die Hälfte (53 %) ist schon seit mindestens sechs Jahren angemeldet, nur 9 Prozent erst seit den letzten zwei Jahren.

Bei KMU beträgt der Durchschnittswert der Registrierungsdauer vier Jahre. Nur 37 Prozent sind schon über sechs Jahre registriert, 27 Prozent erst seit bis zu zwei Jahren.

Zugehörigkeit zu Sektoren: Am stärksten sind Unternehmen aus den Sektoren Energie (35 %) und Gesundheit (25 %) vertreten. Das Finanz- und Versicherungswesen macht einen Anteil von 13 Prozent aus, der Sektor Wasser 10 Prozent, Transport und Verkehr 9 Prozent, Informationstechnik und Telekommunikation 7 Prozent und Ernährung 6 Prozent (Mehrfachnennungen waren möglich).

Dabei ist bei den KMU der Energie-Sektor mit einem Anteil von 54 Prozent am stärksten vertreten, gefolgt von Wasser (15 %) und Transport/Verkehr (10 %). Die Großunternehmen gehören am häufigsten den Sektoren Gesundheit (37 %), Energie (21 %) und Finanz- und Versicherungswesen (16 %) an.

22 Prozent der befragten Unternehmen betreiben ausschließlich Anlagen, die unter eine der folgenden Regelungen fallen: Energiewirtschaftsgesetz (EnWG) oder Telekommunikationsgesetz (TKG).

Bei der Umsetzung der gesetzlichen Maßnahmen ist der Sektor Finanz-/Versicherungswesen im Vergleich am weitesten vorangeschritten: Sein Anteil an den Unternehmen, die bereits über 90 Prozent der Vorgaben erfüllt haben, ist mit 25 Prozent ebenso hoch wie der Anteil der viel stärker vertretenen Energie-Unternehmen. Defizite weist hingegen der Gesundheits-Sektor auf: Sie machen einen Anteil von 45 Prozent der Unternehmen aus, die bisher nur bis 70 Prozent der Maßnahmen umgesetzt haben, aus.

Abbildung 1: Strukturdaten: Sektor

Standort: 89 Prozent der Unternehmen sind in den alten Bundesländern und den westlichen Bezirken Berlins angesiedelt, 25 Prozent in den neuen Bundesländern und den östlichen Bezirken Berlins (Mehrfachnennungen waren möglich).

Funktion der befragten Personen: Drei Viertel der Befragten (76 %) sind die Informationssicherheitsbeauftragten (ISM oder CISO) ihres Unternehmens, 18 Prozent leiten die IT-Abteilung (Mehrfachnennungen waren möglich).
Ihren Informationsstand zu den Themen IT-Sicherheit und IT-Struktur im Unternehmen schätzen 98 Prozent der Befragten als gut ein, 70 Prozent sogar als „sehr gut“.

Wirtschaftliche Lage: Gut die Hälfte der Befragten (53 %) bewertet die wirtschaftliche Lage ihres Unternehmens als sehr gut oder gut (Werte 1 und 2 auf einer 6er-Skala), nur 8 Prozent als schlecht/ sehr schlecht (Werte 5 und 6).

KMU stehen wirtschaftlich besser da: Hier stufen knapp zwei Drittel (65 %) ihre Lage als sehr gut/ gut ein, bei den Großunternehmen sind es nur 46 Prozent.

Auffällig ist, dass nur ein Drittel der Unternehmen (32 %), die weniger als 70 Prozent der gesetzlichen Maßnahmen umgesetzt haben, angeben, wirtschaftlich (sehr) gut da zu stehen. Dies deutet auf einen starken Zusammenhang zwischen wirtschaftlicher Leistungsfähigkeit und Umsetzung der gesetzlichen Maßnahmen zur IT-Sicherheit hin.

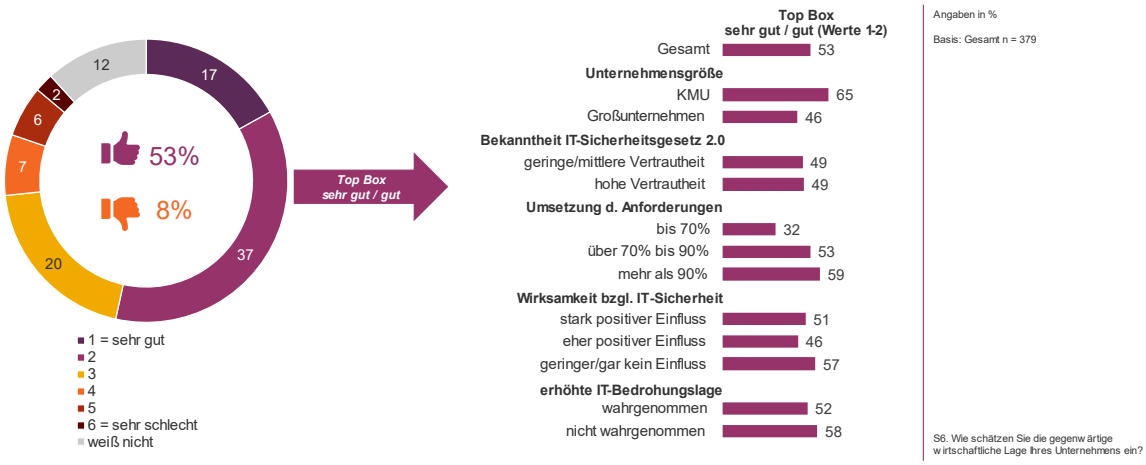

Abbildung 2: Wirtschaftliche Lage des Unternehmens

4. SPEZIFISCHE SICHERHEITSTHEMEN

Im Mittelpunkt dieses Kapitels stehen die Umsetzung technischer und organisatorischer Sicherheitsmaßnahmen, das Budget für Cyber-Sicherheit, die Wahrnehmung einer erhöhten IT-Bedrohungslage sowie konkrete Cyber-Angriffe und der dadurch erlittene Schaden für das eigene Unternehmen.

4.1 Umgesetzte technische Sicherheitsmaßnahmen

Die Umsetzung technischer Sicherheitsmaßnahmen ist in den meisten Unternehmen weit vorangeschritten.

Sechs Maßnahmen wurden von mindestens 90 Prozent umgesetzt – mehrheitlich schon vor 2015 - oder sind aktuell in der Planung: VPN (98 %), Zugangskontrollen (98 %), Notstromversorgung oder Netzersatzanlagen (94 %), Redundante Systeme zur Absicherung bei IT-Ausfällen (94 %), geeignete Aufstellung/ Schutz vor Umwelteinflüssen/ Zugriffsschutz und Einsatz von Diebstahlsicherungen (92 %) und Backup-Konzept inkl. Offline-Backups (90 %).

Weitere sechs Maßnahmen wurden von mindestens drei Viertel bis unter 90 Prozent der Unternehmen realisiert, ganz überwiegend bis 2020: Segmentierung und Absicherung von Netzen (87 %), Verschlüsselung (85 %), Identitätsmanagement und Zugriffskontrolle (85 %), Mehr-Faktor-Authentifizierung (80 %), End Point Protection Gesamtlösung (77 %) und automatisiertes Einspielen von Updates/ Patches (76 %).

Jeweils zwei Drittel der Unternehmen führten eine Härtung von Verzeichnisdiensten (68 %) bzw. eine Schnittstellenkontrolle/ Intrusion Detection/ Prevention (67 %) ein oder haben das vor: Beide Maßnahmen befinden sich am häufigsten noch in der Planungsphase (Schnittstellenkontrolle: 29 %, Härtung: 18 %).

Am niedrigsten ist der Umsetzungsstand bei der Client-Isolation (54 %), DDoS-Mitigation (50 %) und der sicheren Software-Entwicklung (47 %). Dass hier jeweils 15 bis 20 Prozent mit „weiß nicht“ antworteten, weist auf Informationsdefizite in diesem Bereich hin.

Fehlendes Wissen mag auch einer der Gründe dafür sein, dass bei diesen drei Maßnahmen die geringste Intention besteht, sie umzusetzen: 22 Prozent der Unternehmen planen aktuell keine sichere Software-Entwicklung, 21 Prozent keine DDoS-Mitigation und 14 Prozent keine Client-Isolation. Auch das automatische Einspielen von Updates/ Patches steht bei 13 Prozent der Unternehmen zurzeit nicht auf der Planungsliste.

Die am häufigsten vor 2015 umgesetzte technische Sicherheitsmaßnahmen sind die Notstromversorgung (77 % in diesem Zeitraum) und Zugangskontrollen (73 %), während die Zwei-Faktoren-Authentifizierung am häufigsten zwischen 2015 und 2020 (40 %) eingeführt wurde. Einen Schub nach Erscheinen des IT-Sicherheitsgesetzes 1.0 erhielten auch die Umsetzung einer Verschlüsselung (36 %), Patchmanagement (34 %), Identitätsmanagement (33 %), Härtung von Verzeichnisdiensten (33 %) und Schnittstellenkontrollen (32 %). Die Mehr-Faktoren-Authentifizierung ist auch die seit 2021 am stärksten implementierte Maßnahme (21 %), gefolgt von der Schnittstellenkontrolle (17 %).

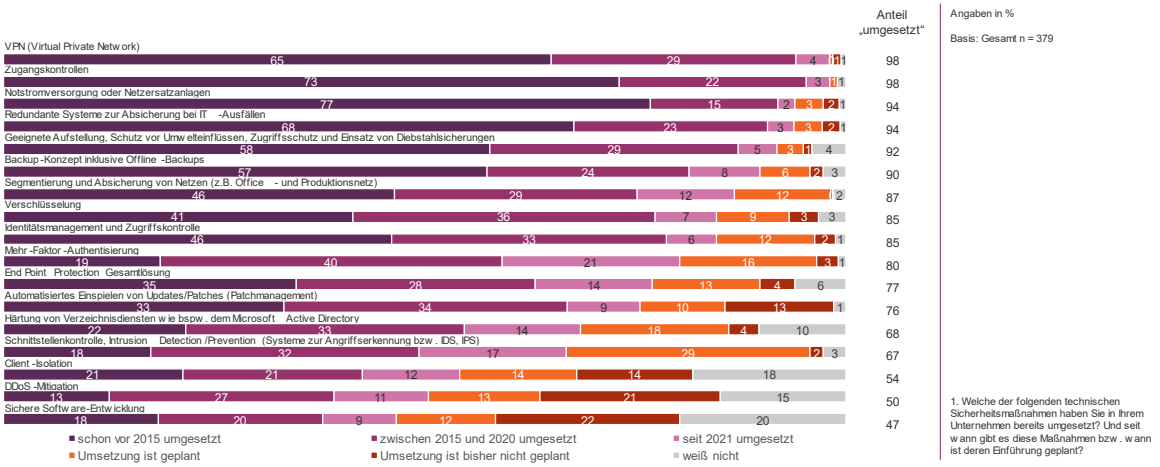

Abbildung 3: Umgesetzte technische Sicherheitsmaßnahmen

Großunternehmen sind überwiegend weiter vorangeschritten als KMU, vor allem bei der Umsetzung von fünf Maßnahmen: DDoS-Mitigation (58 % - KMU: 40%), Schnittstellenkontrolle (74 % - KMU: 58 %), sichere Software-Entwicklung (52 % - KMU: 39 %), EndPoint Protection Gesamtlösung (80 % - KMU: 73 %) und Härtung von Verzeichnisdiensten (72 % - KMU: 65 %).

Deutlich vor den Großunternehmen liegen KMU nur bei der Segmentierung/ Absicherung von Netzen (93 % - Großunternehmen: 82 %).

Unternehmen, die mit dem IT-Sicherheitsgesetz 2.0 sehr vertraut sind, haben fast durchweg mehr Maßnahmen umgesetzt als Unternehmen, die es weniger gut kennen. Die Differenzen liegen bei bis zu 18 Prozentpunkten (Härtung von Verzeichnisdiensten), einzig bei den Zugangskontrollen liegen die Werte gleichauf.

Die Unternehmen mit dem geringsten Umsetzungsgrad (bis 70 %) liegen beim Einsatz von VPN (99 %) gleichauf mit den weiter vorangeschrittenen Unternehmen, bei Zugangskontrollen (95 %) und

Notstromversorgung (89 %) nähern sie sich ihnen an. Die größten Defizite weisen sie bei folgenden fünf Maßnahmen auf: sichere Software-Entwicklung (28 %), Client-Isolation (31 %), DDoS-Mitigation (38 %), Schnittstellenkontrolle/ Intrusion Detection/ Prevention (48 %) und Härtung von Verzeichnisdiensten (46 %). Dass bisher so wenige gesetzliche Forderungen umgesetzt wurden, ist ein Hinweis darauf, die IT-Sicherheitsgesetze in diesen Bereichen weniger wirksam waren.

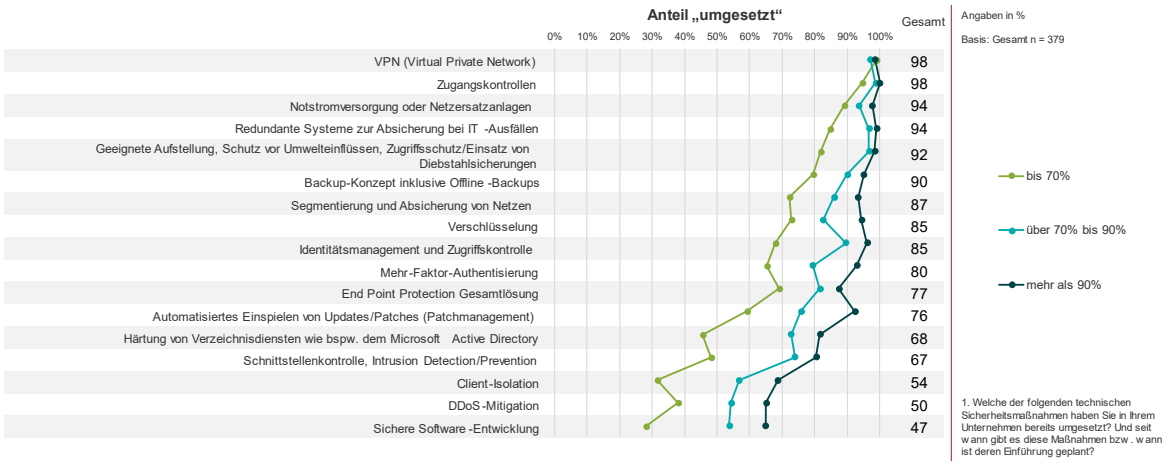

Abbildung 4: Umgesetzte technische Sicherheitsmaßnahmen (nach Umsetzungsstand)

4.2 Umgesetzte organisatorische Sicherheitsmaßnahmen

Zwei **organisatorische Sicherheitsmaßnahmen** sind in nahezu allen Unternehmen umgesetzt: Aufrechterhaltung des aktuellen Informationsstands durch Bezug von Warnungen/ CERT-Meldungen/ Lagebild (94 %) und Sensibilisierung/ Schulungen (91 %). 88 Prozent haben eine Rollentrennung eingeführt, 87 Prozent ein Information Security Management System (ISMS), 83 Prozent ein Assetmanagement und 73 Prozent ein Continuity- und Notfallmanagement.

Regelmäßige Notfallübungen werden in 64 Prozent der Unternehmen durchgeführt, Security Operations in 60 Prozent. Am seltensten umgesetzt ist die sichere Dokumentenerstellung (55 %).

Am häufigsten in der Planungsphase sind aktuell die Einführung regelmäßiger Notfallübungen (28 %), Continuity- und Notfallmanagement (25 %) und Security Operations (21 %).

Die vergleichsweise geringste Umsetzungsintention besteht bei der sicheren Dokumentenerstellung: Sie ist in 8 Prozent der Unternehmen derzeit nicht geplant. Diese Maßnahme scheint zudem eher unbekannt zu sein, worauf der hohe Anteil an „weiß nicht“-Antworten (27 %) hindeutet.

Das IT-SiG 1.0 scheint einen hohen Einfluss auf die Umsetzung organisatorischer Sicherheitsmaßnahmen gehabt zu haben: Anders als die technischen Maßnahmen wurden sie mehrheitlich erst zwischen 2015 bis 2020 realisiert, in besonderem Maße die Aufrechterhaltung des aktuellen Informationsstands (66 % in diesem Zeitraum) und ISMS (60 %). Nach Einführung des IT-SIG 2.0 kamen fast alle Maßnahmen mit einem Anteil von 13 bis 16 Prozent hinzu, die einzigen Ausnahmen sind das Assetmanagement (9 %) und die sichere Dokumentenerstellung (8 %).

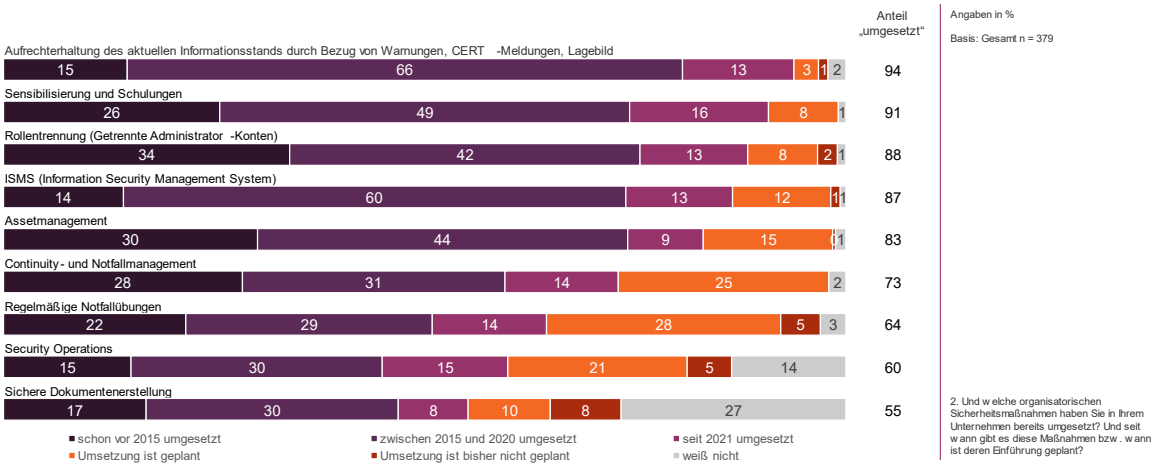

Abbildung 5: Umgesetzte organisatorische Sicherheitsmaßnahmen

KMU und Großunternehmen liegen bei der Umsetzung organisatorischer Sicherheitsmaßnahmen nahe beieinander – mit zwei Ausnahmen: Großunternehmen verfügen häufiger (92 %) als KMU (80 %) über ein ISMS, KMU führen hingegen häufiger (71 %) als Großunternehmen (60 %) regelmäßige Notfallübungen durch.

Auch hier ist der Umsetzungsstand bei den Unternehmen mit hoher Vertrautheit mit dem neuen IT-Sicherheitsgesetz durchweg höher als bei den Befragten mit geringer/ mittlerer Vertrautheit. Die Differenzen zwischen den beiden Teilgruppen liegen zwischen 6 Prozentpunkten (Assetmanagement) und 16 Prozentpunkten (Continuity- und Notfallmanagement und regelmäßige Notfallübungen).

Die Unternehmen mit dem geringsten Umsetzungsgrad (bis 70 %) liegen zum Teil beträchtlich hinter den schon weiter vorangeschrittenen Unternehmen. Besonders selten eingeführt (bzw. geplant) sind Security Operations (28 %), regelmäßige Notfallübungen (35 %) und Continuity- und Notfallmanagement (40 %). Am häufigsten umgesetzt haben sie die Aufrechterhaltung des aktuellen Informationsstands durch Bezug von Warnungen/ CERT-Meldungen/ Lagebild (87 %) und die Rollentrennung (75 %). Auch hier ist von einer geringeren Wirksamkeit der IT-Sicherheitsgesetze in diesen Bereichen auszugehen.

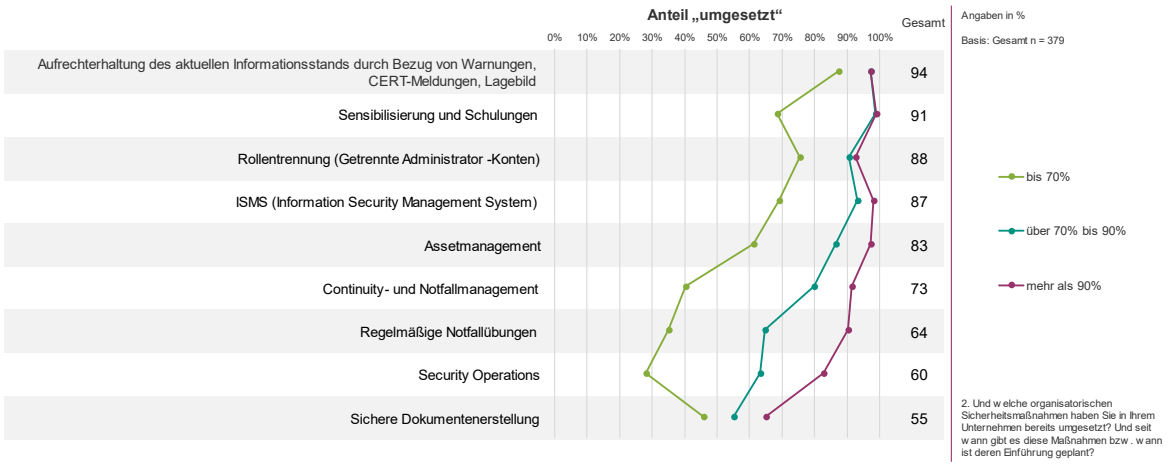

Abbildung 6: Umgesetzte organisatorische Sicherheitsmaßnahmen (nach Umsetzungsstand)

Für die Hälfte der Unternehmen (51 %) war bzw. ist die aktuelle IT-Bedrohungslage der **Hauptgrund für die Umsetzung von Sicherheitsmaßnahmen**, 39 Prozent nennen die aktuelle IT-Sicherheitsgesetzgebung als wichtigsten Grund. Für 2 Prozent waren die Auswirkungen der Corona-Pandemie auf die IT-Sicherheitsanforderungen ausschlaggebend, 9 Prozent führen andere Gründe an.

Für Großunternehmen ist die akute Bedrohungssituation (53 %) deutlich häufiger der Hauptgrund als die gesetzlichen Vorgaben (36 %). Bei KMU ist die Verteilung ausgewogener: 47 Prozent nennen die IT-Bedrohungslage, 44 Prozent die IT-Sicherheitsgesetzgebung.

Am häufigsten geben Unternehmen, die bereits über 90 Prozent der Maßnahmen umgesetzt haben, die akute IT-Gefährdungslage als Hauptgrund an (70 %). Die größten Treiber für die Umsetzung sind demnach die eigenen wirtschaftlichen Interessen, die IT-Sicherheitsgesetze wirken eher flankierend und als Orientierung.

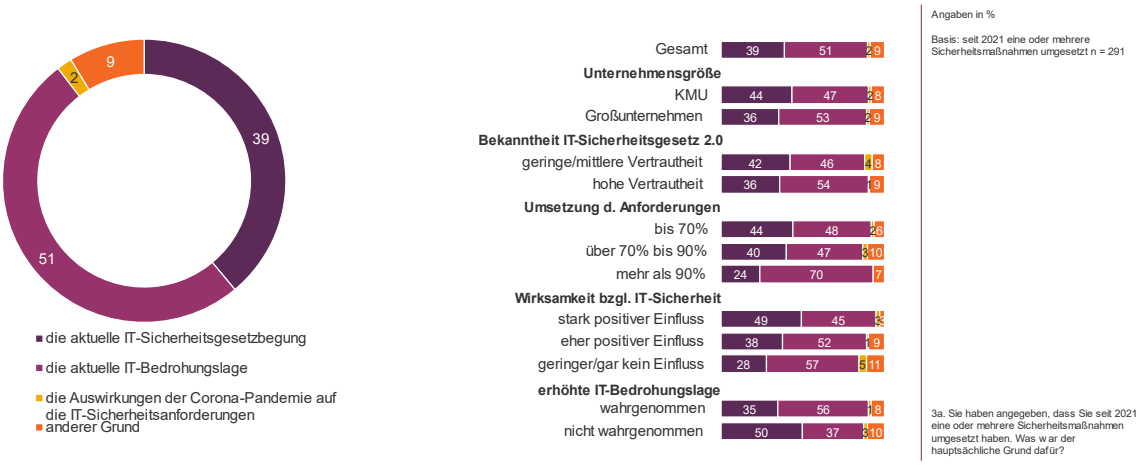

Abbildung 7: Gründe für umgesetzte Sicherheitsmaßnahmen

4.3 IT-Sicherheitsbudget

Im Durchschnitt liegt der prozentuale Anteil für Cyber-Sicherheit im IT-Budget bei 14 Prozent, bei KMU etwas höher (16 %) als bei Großunternehmen (12 %). Die Mehrheit der Unternehmen (58 %) hat dafür nur einen Anteil von unter 10 Prozent eingestellt. Ein gutes Viertel (28 %) wendet 11 bis 20 Prozent des IT-Budgets für Sicherheitsmaßnahmen auf, nur bei 14 Prozent liegt der Anteil höher.

Zwischen dem Budget und der Vertrautheit mit dem IT-SiG 2.0 besteht kein Zusammenhang.

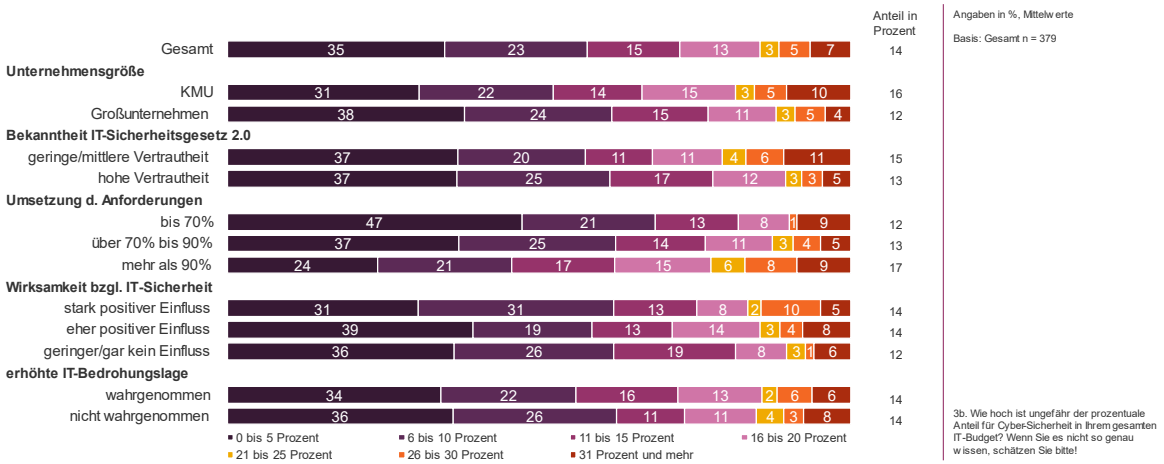

Abbildung 8: Anteil für Cyber-Sicherheit am gesamten IT-Budget

Die meisten Unternehmen halten das zur Verfügung stehende IT-Sicherheitsbudget nicht für angemessen. Nur gut ein Drittel hält es für „eher“ (30 %) oder „völlig“ (5 %) ausreichend. Dem stehen 30 Prozent gegenüber, die ihr Budget als „eher“ (22 %) oder „viel“ zu knapp (8 %) einschätzen. 35 Prozent ordnen sich mit der Antwort „teils/ teils“ dazwischen ein.

Vor allem bei Großunternehmen ist die Zufriedenheit gering: Nur 28 Prozent halten ihr Budget für „völlig/ eher“ ausreichend, bei KMU sind es 45 Prozent.

Vier von zehn Unternehmen (39 %) haben ihr IT-Sicherheitsbudget in den letzten zwei Jahren wegen der Cyber-Sicherheitslage erhöht (Großunternehmen: 41 %, KMU: 38 %), weitere 21 Prozent stockten es aus anderen Gründen auf. Bei 17 Prozent blieb das Budget gleich, weitere 5 Prozent haben eine spätere Erhöhung eingeplant. 3 Prozent der Unternehmen mussten ihr Budget in diesem Zeitraum kürzen.

4.4 IT-Bedrohungslage und Cyber-Angriffe

71 Prozent der Befragten nehmen gegenwärtig eine erhöhte IT-Bedrohungslage wahr. Großunternehmen zeigen sich hier alarmierter (76 %) als KMU (63 %).

Besonders besorgt äußern sich Unternehmen, die mehr als 90 Prozent der gesetzlichen Maßnahmen umgesetzt haben (77 %), und Unternehmen, die den IT-Sicherheitsgesetzen einen stark positiven Einfluss zuschreiben (80 %). Dies zeigt erneut einen Wirkzusammenhang: Die Einschätzung einer hohen Gefährdungslage führt zu hohen Investitionen und vermutlich auch zu einer stärkeren Beschäftigung mit den IT-Sicherheitsgesetzen.

Zu den Ursachen für die gewachsene Cyber-Bedrohung gehört für rund ein Drittel der besorgten Unternehmen (31 %) der Ukraine-Krieg bzw. die geopolitische/ weltpolitische Lage. Jedes vierte (26 %) - KMU häufiger als Großunternehmen – rechnet mit zunehmenden und gezielten Angriffen auf die Kritische Infrastruktur. Weitere konkrete Befürchtungen sind Ransomware/ Schadsoftware (20 %), Spam/ Phishing-Mails (20 %) und Hacking/ Softwareschwachstellen/ Zero-Day-Exploits (10 %). 10 Prozent nennen Informationen über IT-Bedrohungen und BSI-Meldungen als Ursache für ihre gestiegene Sorge (Mehrfachnennungen waren möglich).

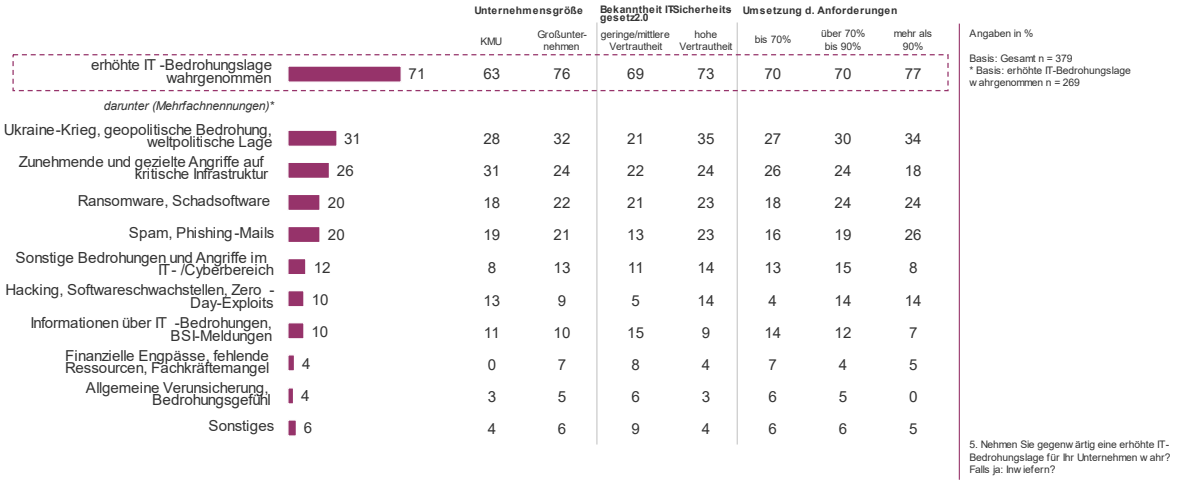

Abbildung 9: Wahrnehmung einer erhöhten IT-Bedrohungslage (Gründe)

Eine erhöhte IT-Gefährdungslage durch häufigere Cyber-Angriffe auf das eigene Unternehmen stellten in den vergangenen zwei Jahren 45 Prozent der Befragten fest, Großunternehmen (52 %) deutlich häufiger als KMU (35 %).

40 Prozent mussten in diesem Zeitraum aktiv auf Cyber-Attacken reagieren. Auch hier sind Großunternehmen (47 %) stärker betroffen als KMU (31 %).

Bei den erlebten Angriffen handelte es sich mit Abstand am häufigsten um Phishing (79 %) und Schadsoftware in E-Mail-Anhängen (72 %). Rund die Hälfte der Unternehmen hatte mit CEO-Fraud zu tun (53 %), 40 Prozent mit DDoS-Attacken, 35 Prozent mit Ransomware, 31 Prozent mit Supply-Chain-Angriffen und 26 Prozent mit dem Ausnutzen von Zero-Day-Schwachstellen. Seltenere Nennungen sind Daten-Exfiltration (13 %), APT-Angriffe (13 %) und Innentäter (12 %).

Großunternehmen waren insgesamt mehr und häufiger von Angriffen betroffen als KMU. Die kleineren und mittleren Unternehmen waren allerdings häufiger Phishing-Angriffen ausgesetzt (84 % - Großunternehmen: 77 %), CEO-Fraud und DDoS-Attacken erlebten sie etwa genauso oft.

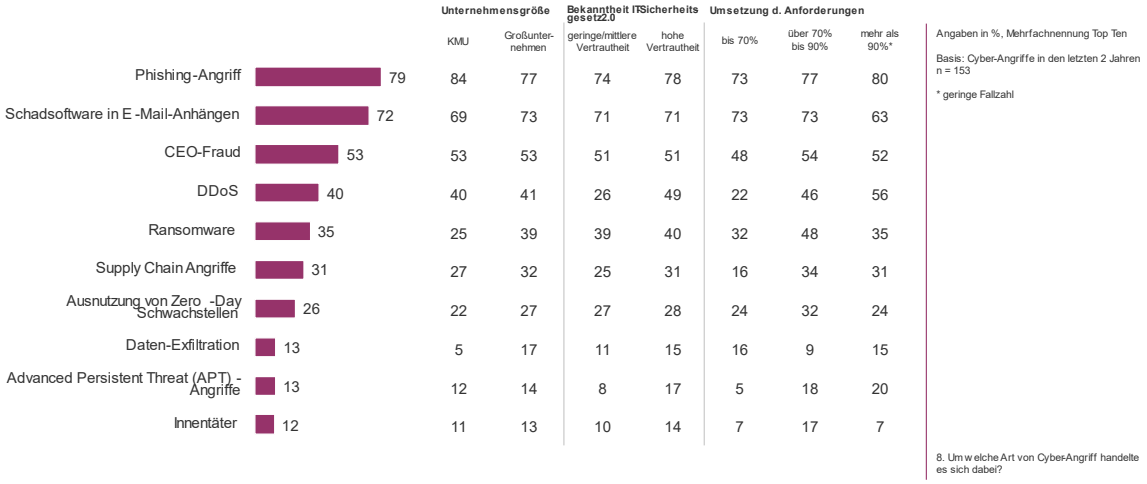

Abbildung 10: Formen der Cyber-Angriffe

4.5 Wirtschaftlicher Schaden durch Cyber-Angriffe

Rund zwei Drittel der von Cyber-Angriffen betroffenen Unternehmen wurden dadurch finanziell geschädigt.

36 Prozent mussten Kosten für Dienstleister aufwenden, 31 Prozent hatten Ausgaben für die interne Wiederherstellung, 21 Prozent für den Betriebsausfall, 3 Prozent für finanzielle Ansprüche Dritter. Lösegeldzahlungen entrichteten 1 Prozent, darunter kein Großunternehmen. 29 Prozent hatten weitere Ausgaben.

Großunternehmen nennen neben Kosten für Dienstleister (37 %) fast ebenso häufig Aufwendungen für die Wiederherstellung (36 %), die bei KMU deutlich seltener anfielen (21 %).

Auch bei den betroffenen Unternehmen, die weniger als 70 Prozent der gesetzlichen Maßnahmen umgesetzt haben, fielen überdurchschnittlich häufig Kosten für externe Dienstleister (47 %) und Wiederherstellung (40 %) an.

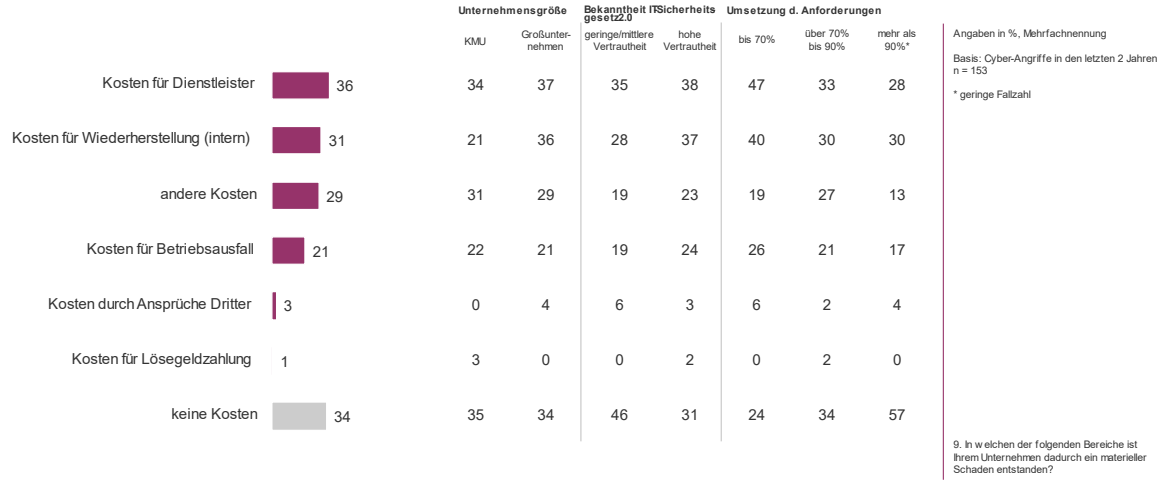

Abbildung 11: Unternehmensbereiche mit materiellem Schaden durch Cyber-Angriffe

34 Prozent der Betroffenen erlitten keinen materiellen Schaden, bei einem Viertel (26 %) betrug der Schaden unter 50.000 Euro, bei 30 Prozent lag er höher.

Im Durchschnitt liegt der finanzielle Gesamtschaden durch Cyber-Attacken in den letzten zwei Jahren bei 128.000 Euro. Bei Großunternehmen lagen die Kosten mit durchschnittlich 157.000 Euro wesentlich höher als bei KMU (71.000 Euro).

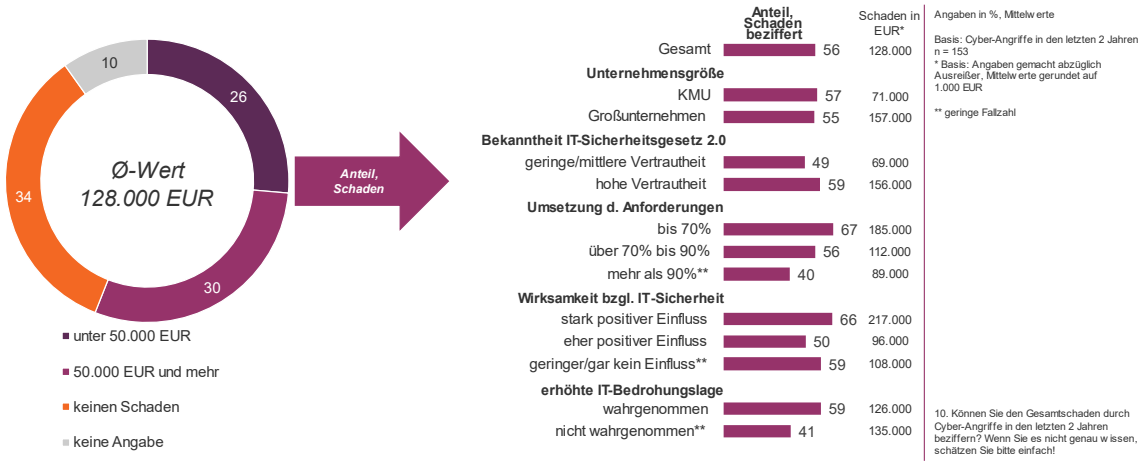

Abbildung 12: Gesamtschaden durch Cyber-Angriffe

Für die meisten von Cyber-Attacken betroffenen Unternehmen fiel der erlittene materielle Schaden allerdings nicht stark ins Gewicht. Für 48 Prozent war er „unbedeutend“, für 38 Prozent „weniger schwer“. Als „eher schwer“ ordnen ihn 10 Prozent ein, als „sehr schwer“ nur 3 Prozent. In eine existenzbedrohende Lage geriet dadurch kein Unternehmen.

5. DIGITALISIERUNG IM UNTERNEHMEN

Dieses Kapitel stellt den Stand der IT-Entwicklung der befragten Unternehmen dar und betrachtet die Bedeutung von Informationssicherheit sowie die Dokumentation und Kommunikation von IT-Sicherheitsvorfällen und die Behebung von Sicherheitslücken im IT-System.

5.1 Stand der IT-Entwicklung/ Digitalisierung im Unternehmen

Mit dem aktuellen Stand der IT-Entwicklung und Digitalisierung in ihrem Betrieb sind nur knapp unter der Hälfte der Unternehmen zufrieden: 41 Prozent bezeichnen ihn als gut (Wert 2 auf einer 6er-Skala), nur 6 Prozent als sehr gut (Wert 1). 40 Prozent ordnen sich im oberen Mittelfeld (Wert 3), 11 Prozent im unteren Mittelfeld (Wert 4) ein.

Als schlecht stufen nur 2 Prozent der Unternehmen ihren internen IT-Entwicklungsstand ein (Wert 5), die schlechteste Note 6 wurde nicht vergeben.

KMU bezeichnen ihren Entwicklungsstand häufiger (52 %) als die Großunternehmen (43 %) als sehr gut oder gut.

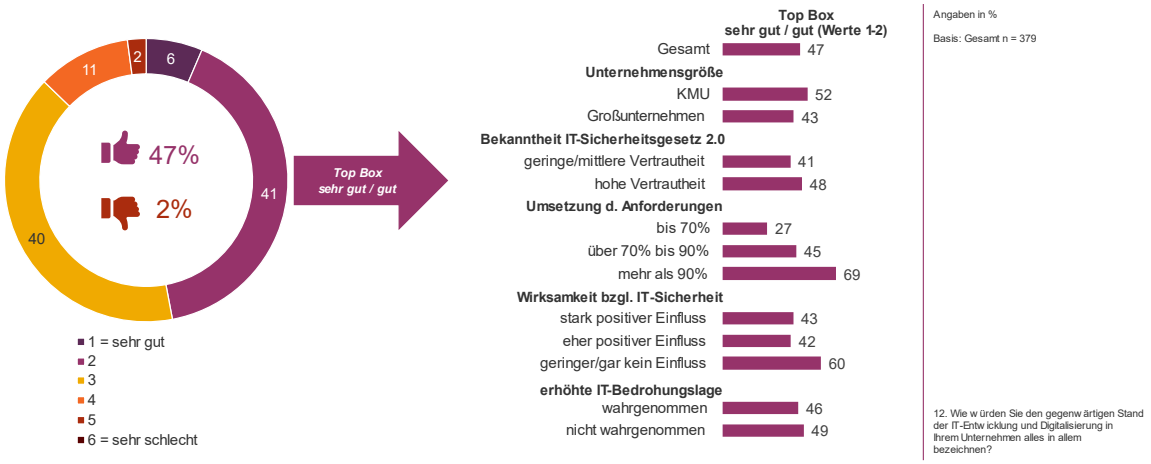

Abbildung 13: Stand der IT-Entwicklung/ Digitalisierung im Unternehmen

Für die (weitere) Digitalisierung von Geschäftsprozessen spielt die Informationssicherheit bei den meisten Unternehmen eine Rolle. 56 Prozent denken diesen Aspekt von vornherein mit, weitere 37 Prozent berücksichtigen ihn im Laufe der Implementierung. 4 Prozent geben an, sich erst nach der

Implementierung damit zu beschäftigen, 3 Prozent weisen ihr eine untergeordnete Rolle zu.

Insbesondere Unternehmen, die die gesetzlichen Maßnahmen zu mehr als 90 Prozent umgesetzt haben, denken Informationssicherheit von Anfang an mit (78 %), während das nur 26 Prozent der Unternehmen mit einem Umsetzungsstand von bis zu 70 Prozent tun. In dieser Zielgruppe ist der Anteil derjenigen am höchsten, die diesen Aspekt erst nachträglich berücksichtigen (10 %) oder für die er eine untergeordnete Rolle spielt (8 %).

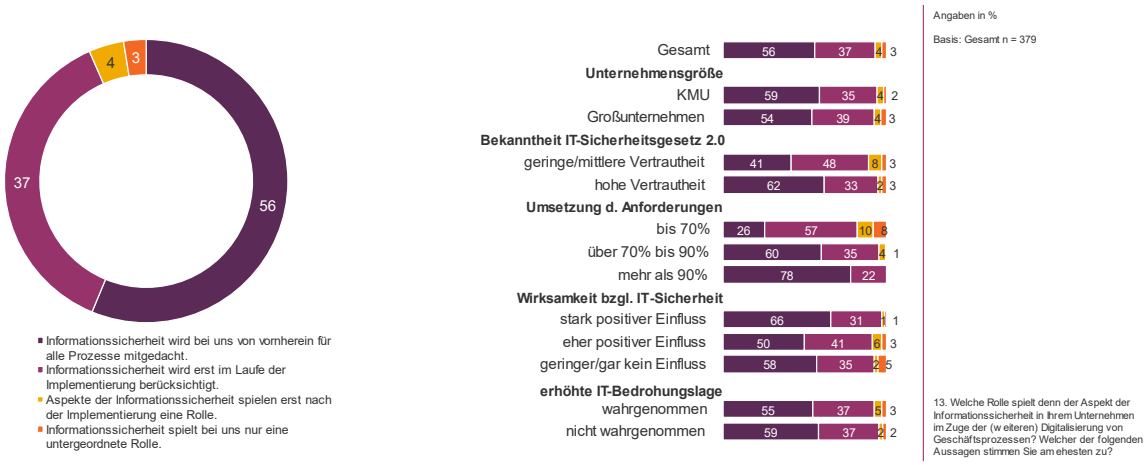

Abbildung 14: Informationssicherheit im Kontext der Digitalisierung

5.2 Dokumentation und Kommunikation von Sicherheitsvorfällen

Fast alle befragten Unternehmen halten Sicherheitsvorfälle in einem internen Dokumentationssystem fest (95 %). 9 Prozent nutzen ein externes Dokumentationssystem, 8 Prozent dokumentieren Vorfälle nur sporadisch (Mehrfachnennungen waren möglich).

Unternehmen, die bis 70 Prozent der Sicherheitsmaßnahmen umgesetzt haben, verfügen am häufigsten über eine nur sporadische Dokumentation (26 %).

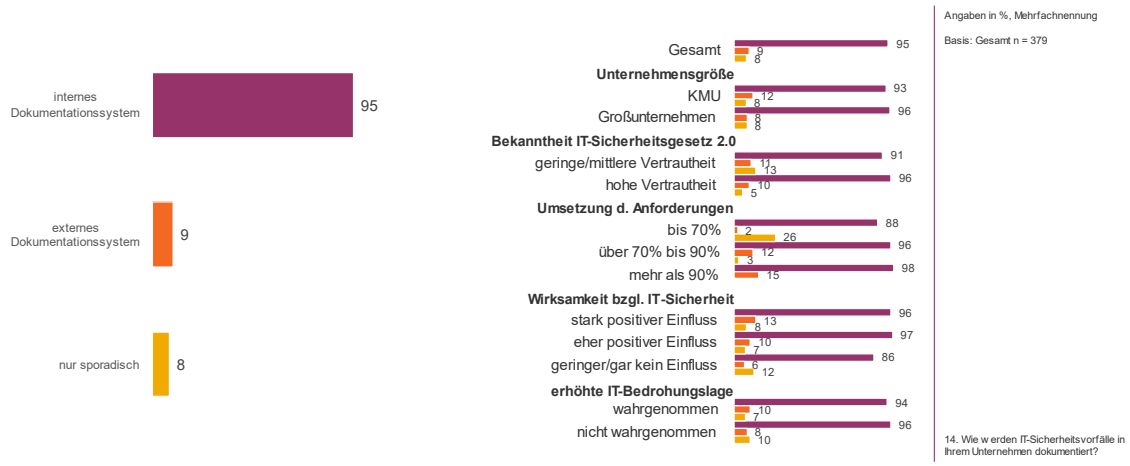

Abbildung 15: Dokumentation von IT-Sicherheitsvorfällen

Was die Kommunikation von Sicherheitsvorfällen angeht, steht das Bundesamt für Sicherheit in der Informationstechnik mit Abstand an erster Stelle: 87 Prozent der Unternehmen nennen es als Adressat. 52 Prozent informieren kooperierende Unternehmen, 44 Prozent andere Behörden. 38 Prozent geben Kunden, 37 Prozent Lieferanten Bescheid.

9 Prozent geben die Informationen „auch intern“ bzw. „nur intern“ (7 %) weiter. 8 Prozent adressieren situationsspezifisch die Betroffenen, 5 Prozent das Management/ Vorstand/ Führungskräfte (Mehrfachnennungen waren möglich).

Eine hohe Vertrautheit mit den IT-Sicherheitsgesetzen zieht häufigere Meldungen an das BSI und andere Behörden nach sich, schlägt sich aber nicht in der weiteren Kommunikation nieder.

Unternehmen mit einem geringeren Umsetzungsstand der gesetzlichen Maßnahmen (< 71 %) sind bei der Kommunikation von Sicherheitsvorfällen an Externe weniger aktiv als die anderen Unternehmen. Insbesondere das BSI informieren nur unterdurchschnittliche 76 Prozent.

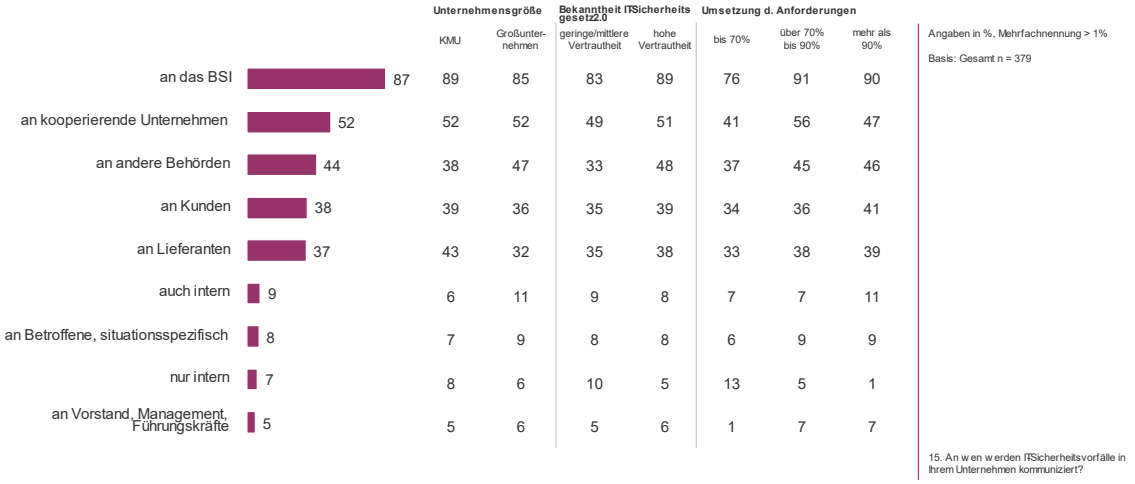

Abbildung 16: Kommunikation von IT-Sicherheitsvorfällen (nach Teilgruppen)

Auch Unternehmen, die keine erhöhte Bedrohungslage wahrnehmen, kommunizieren Sicherheitsvorfälle seltener nach außen. Einzige Ausnahme ist die Weitergabe an das BSI (89 Prozent).

Die Beseitigung von Sicherheitslücken in den IT-Systemen erfolgt in jedem vierten Unternehmen (26 %) sofort nach deren Entdeckung, ein gutes weiteres Viertel (27 %) beseitigt sie innerhalb einer festgelegten Frist. 43 Prozent werden erst nach einer Priorisierung im Rahmen einer Risikobewertung aktiv, jeweils 2 Prozent erledigen es „so schnell wie möglich und machbar“ bzw. „situationsspezifisch, abhängig von der Kritikalität“.

KMU agieren bei Sicherheitslücken schneller als Großunternehmen: 33 Prozent beseitigen sie sofort (Großunternehmen: 22 %). Großunternehmen setzen hingegen häufiger zunächst eine Risikobewertung ein (46 %, KMU: 37 %).

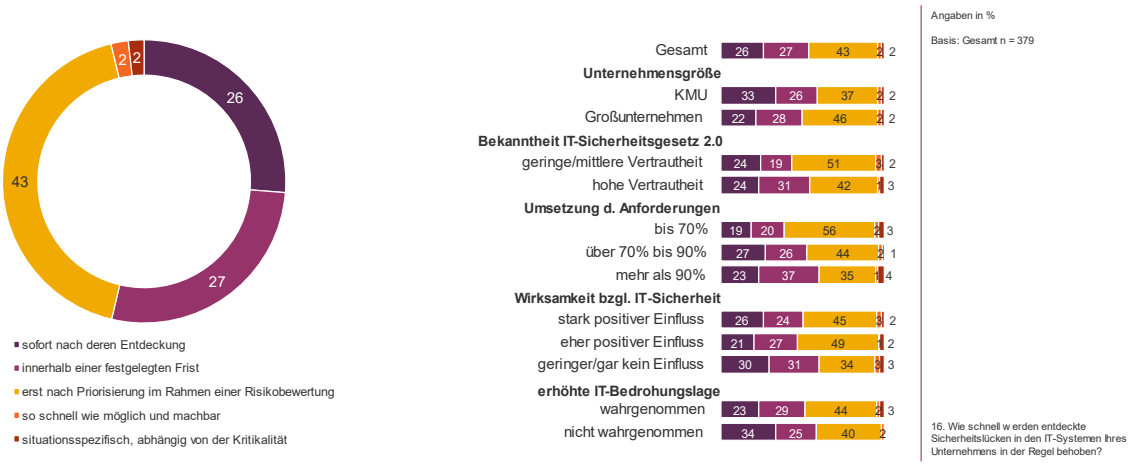

Abbildung 17: Behebung von Sicherheitslücken im IT-System

6. IT-SICHERHEITSGESETZE

Das folgende Kapitel behandelt die Vertrautheit der Unternehmen mit den KRITIS-relevanten gesetzlichen Anforderungen in der BSI-Gesetzgebung, den Auswirkungen dieser Gesetze und seiner Änderungen auf das Unternehmen, den Stand ihrer Umsetzung und die Einführung interner Kontrollmechanismen.

Befragt wurden hier nur Betreiber kritischer Infrastrukturen, die nicht ausschließlich unter das Energiewirtschaftsgesetz (EnWG) oder das Telekommunikationsgesetz (TKG) fallen.

6.1 Vertrautheit mit den IT-Sicherheitsgesetzen (IT-SiG)

82 Prozent der Unternehmen fühlen sich mit den KRITIS-relevanten Aspekten im **BSI-Gesetz nach Änderungen durch das erste IT-Sicherheitsgesetz (2015)** weitgehend bis sehr vertraut (Werte 6-10 auf einer Skala von 0-10). Die Bestwerte 8 bis 10 vergeben zwei Drittel für sich (66 %). Nur 12 Prozent geben an, wenig oder gar nicht damit vertraut zu sein (Werte 0-4).

Großunternehmen kennen sich etwas häufiger gut mit dem Gesetz aus (84 %: Werte 6-10) als KMU (77 %), 71 Prozent fühlen sich damit sogar sehr vertraut (KMU: 55 %).

Die geringste Bekanntheit hat das BSI-Gesetz bei Unternehmen mit niedrigem Umsetzungsstand (< 71 %): Mit seinem Inhalt fühlen sich nur 67 Prozent vertraut, 22 Prozent ordnen sich am unteren Ende der Skala ein (Werte 0-4). Auch unter den Firmen, die keine erhöhte Bedrohungslage wahrnehmen, ist der Anteil derjenigen, die das Gesetz nicht gut kennen, vergleichsweise hoch.

Anders sieht es bei Unternehmen aus, die die Anforderungen bereits zu über 90 Prozent umgesetzt haben: 92 Prozent sind mit dem Gesetz vertraut (sehr gut: 79 %). Auch bei Unternehmen, die den IT-SiG einen stark positiven Einfluss zuschreiben, liegt dieser Anteil mit 92 Prozent überdurchschnittlich hoch (sehr gut: 77 %).

Eine etwas höhere Bekanntheit hat das **IT-Sicherheitsgesetz 2.0 (2021):** Mit ihm fühlen sich 88 Prozent der Befragten vertraut (sehr vertraut: 65 %). Und auch hier stufen sich die Großunternehmen besser ein (90 %) als die KMU (84 %), insbesondere was die starke Vertrautheit angeht (71 % - KMU: 51 %).

Auch hier ist das Gesetz bei Unternehmen mit geringerem Umsetzungsstand (< 71 %) am wenigsten bekannt, wenn auch auf höherem Niveau (74 %), während sich 98 Prozent der Unternehmen mit hohem Umsetzungsstand (> 90%) damit vertraut fühlen, 79 Prozent sogar sehr.

Auch Unternehmen, die keine erhöhte Bedrohungslage wahrnehmen, sind etwas seltener gut informiert (84 %).

Hier lässt sich ein Zusammenhang erkennen: Das Gefühl der Bedrohung führt eher zur Beschäftigung mit den Gesetzen, deren Bekanntheit wiederum fördert eine stärkere Umsetzung der Vorgaben. Ob sich das Vertrauen in die Wirksamkeit der Maßnahmen positiv auf ihre Umsetzung auswirkt oder umgekehrt deren Umsetzung das Vertrauen erhöht, lässt sich hier nicht herauslesen.

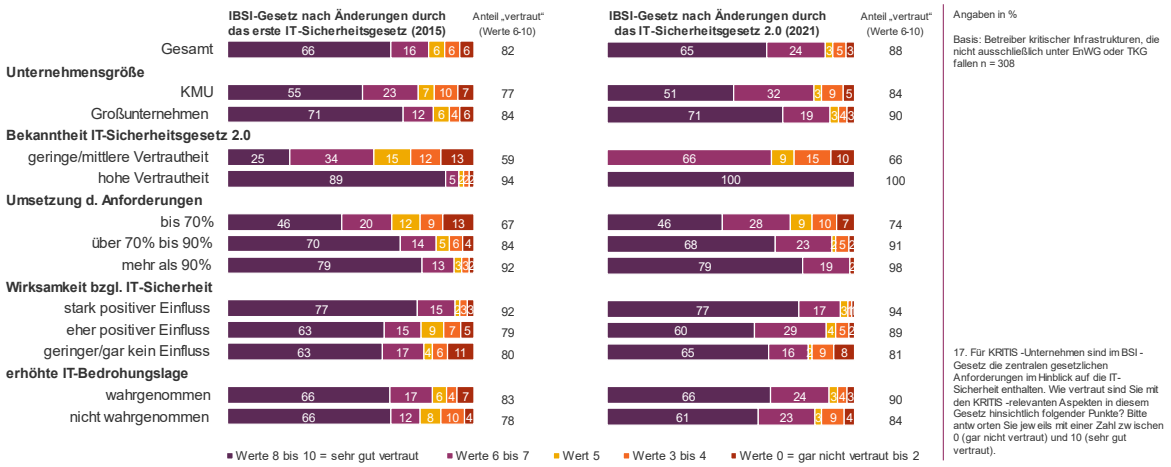

Abbildung 18: Vertrautheit mit KRITIS-relevanten Aspekten in BSI-Gesetzen

6.2 Auswirkungen der geänderten Sicherheitsgesetze

In der offen gestellten Frage nach den Auswirkungen der Gesetze und Gesetzesänderungen stehen der erhöhte Dokumentations-/ Prüfaufwand (26 %) und die Einführung/ der Aufbau von Sicherheitssystemen (23 %) an erster Stelle. Ersteres nennen Großunternehmen häufiger (30 %), zweiteres KMU (27 %).

Weitere Auswirkungen sind die (schnellere) Einführung neuer Maßnahmen (15 %), die Überprüfung/ Optimierung von Prozessen (12 %), die Einstellung neuer Mitarbeitenden, ein erhöhtes Sicherheitsbewusstsein sowie erhöhte Kosten (jeweils 11 %).

Genannt werden auch die Anmeldung als KRITIS-Unternehmen beim BSI und ein erhöhter Sicherheitsstandard (jeweils 9 %), mehr Investitionen in IT-Systeme, die Einführung von Systemen zur Angriffserkennung, eine organisatorische Umstrukturierung (jeweils 8 %) und die Einführung und Anpassung von Audits (7 %).

Eine hohe Vertrautheit mit den IT-SiG zieht offenbar mehr Auswirkungen nach sich: Diese Unternehmen berichten häufiger von einem erhöhten Dokumentationsaufwand, Einführung/ Aufbau von Sicherheitssystemen, Überprüfung/ Optimierung von Prozessen und – wohl damit verbundenen – höheren Kosten.

Unternehmen mit geringem Umsetzungsstand (bis 70 %) nennen überdurchschnittlich häufig die (schnellere) Einführung neuer Maßnahmen (22 %), bei Unternehmen mit hohem Umsetzungsstand (> 90 %) fielen häufiger erhöhte Kosten (19 %) und die Überprüfung/ Optimierung von Prozessen (18 %) an.

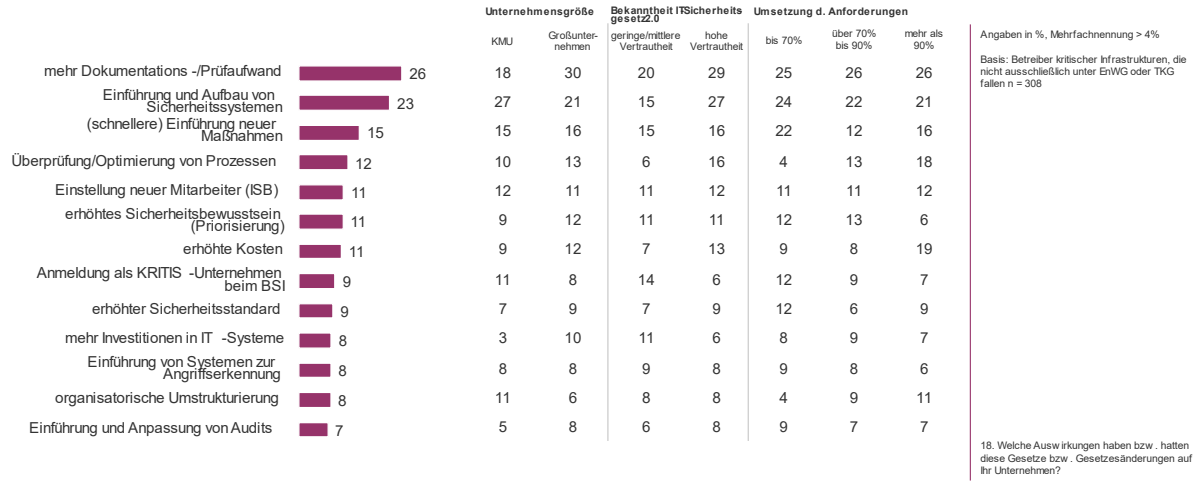

Abbildung 19: Auswirkungen der BSI-Gesetze auf Unternehmen

Unternehmen, die den Gesetzen nur einen geringen/ keinen Einfluss auf ihre IT-Sicherheit zuschreiben, nennen mit weitem Abstand am häufigsten den erhöhten Dokumentations-/ Prüfaufwand (39 %). Für Unternehmen, die den Einfluss als stark positiv bewerten, stehen Einführung und Aufbau von Sicherheitssystemen an erster Stelle (32 %).

62 Prozent der befragten Unternehmen setzten aufgrund der geänderten IT-Sicherheitsgesetzgebung neue Projekte zur Erhöhung der IT-Sicherheit durch, weitere 20 Prozent zogen geplante Projekte zeitlich vor. Nur 15 Prozent verneinen diese Frage; am stärksten vertreten sind hier Unternehmen, die den gesetzlichen Maßnahmen nur einen geringen/ keinen Einfluss zuschreiben (27 %).

Kein Zusammenhang zeigt sich zwischen der Reaktion auf die neuen Gesetze und der Vertrautheit mit dem IT-SiG oder dem Umsetzungsgrad der gesetzlichen Anforderungen.

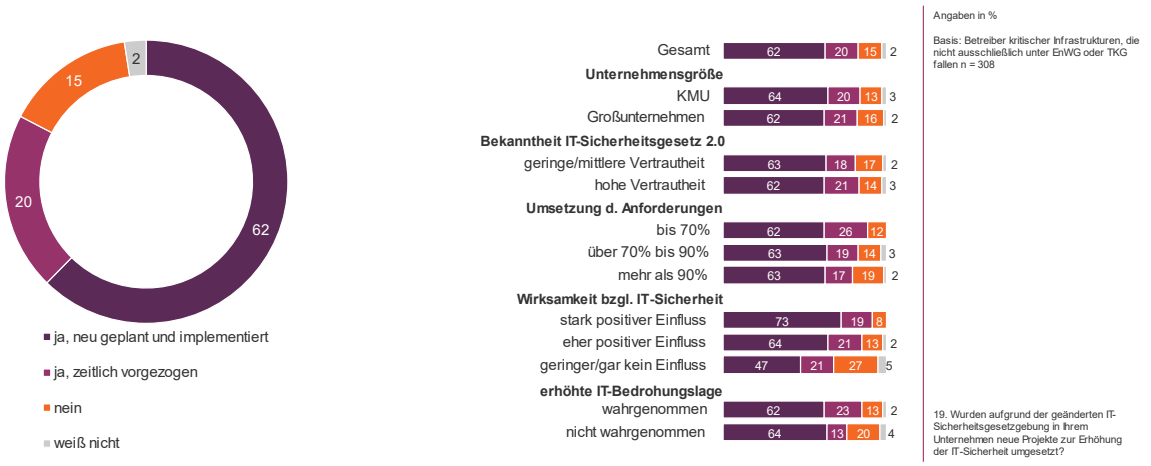

Abbildung 20: Reaktion auf geänderte IT-Sicherheitsgesetzgebung

Die Mehrheit der befragten Unternehmen führte im Zusammenhang mit dem ersten IT-SiG und dem IT-SiG 2.0 Schulungen durch. Sechs von zehn Unternehmen (60%) schulten ihre Mitarbeitenden firmenintern, rund ein Drittel (35 %) entschied sich für einen externen Anbieter (Mehrfachnennungen waren möglich). In 30 Prozent der Unternehmen fanden keine gesonderten Informationsveranstaltungen statt.

Auf Schulungen setzten vor allem Unternehmen mit hohem Umsetzungsstand der Maßnahmen (> 90 %) bzw. einer stark positiven Einstellung gegenüber der Wirksamkeit der IT-Gesetze: Nur 18 bzw. 15 Prozent verzichteten darauf.

Die Einhaltung der Anforderungen der IT-Sicherheitsgesetze wird in 83 Prozent der Unternehmen mit Hilfe eines internen Überwachungssystems kontrolliert. 48 Prozent nutzen ein externes Überwachungssystem (Mehrfachnennungen waren möglich).

11 Prozent überprüfen die Einhaltung nur sporadisch. Am häufigsten vertreten sind hier Firmen mit geringer/ mittlerer Vertrautheit mit der Gesetzgebung (24 %) und Unternehmen, die bis 70 Prozent der Maßnahmen umgesetzt haben (29 %).

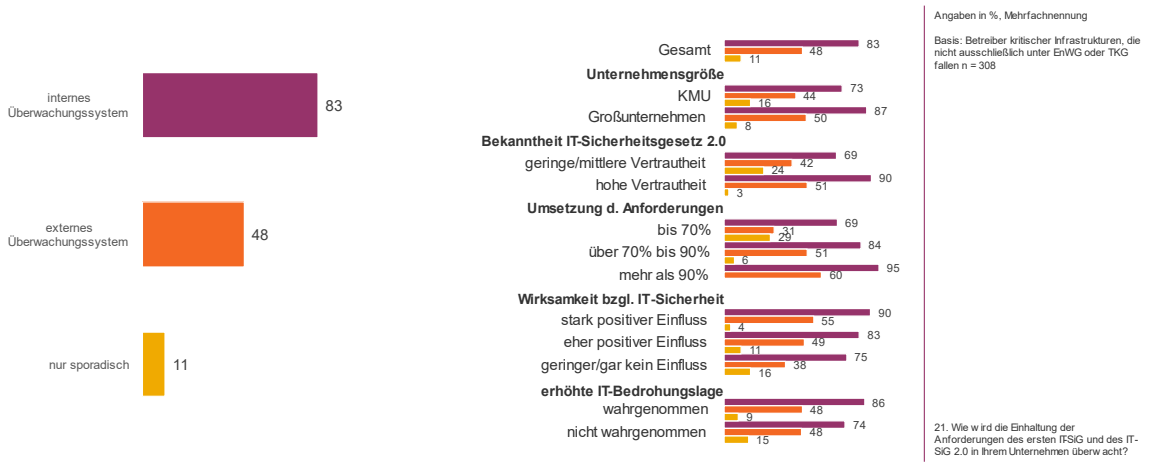

Abbildung 21: Interne Kontrollmechanismen der IT-Sicherheitsgesetze

6.3 Umsetzung der Sicherheitsgesetze

In den meisten Unternehmen ist der geschätzte Umsetzungsstand der gesetzlichen Maßnahmen recht hoch. Am häufigsten gilt das für die Anforderungen an das Meldewesen, die im Durchschnitt zu 88 % umgesetzt sind, Maßnahmen zur Sicherung der baulichen und physischen Sicherheit (84 %), Anforderungen an das Information Security Management System (84 %) und Maßnahmen zur Sicherung der Technischen Informationssicherheit (82 %).

Im Durchschnitt zu jeweils 79 Prozent realisiert sind Maßnahmen für die personelle und organisatorische Sicherheit und zur Erkennung und Bearbeitung von Sicherheitsvorfällen, zu 78 Prozent die Anforderungen an externe Informationsversorgung und Unterstützung, zu 77 Prozent die Anforderungen an Risikoanalyse/ Risikomanagement und zu 75 Prozent an das Asset-Management. Ebenfalls zu 75 Prozent stehen die Überprüfungsmaßnahmen im laufenden Betrieb, zu 73 Prozent die Maßnahmen zur Sicherstellung der Betriebskontinuität.

Den größten Nachholbedarf gibt es bei den Anforderungen zur Kontrolle von Lieferanten, Dienstleistern und Dritten: Hier liegt der Umsetzungsstand bei 65 Prozent.

KMU sind bei der Umsetzung etwas weiter vorangeschritten als die Großunternehmen, insbesondere was die Anforderungen an Risikoanalyse/ -management (Stand: 81%, Großunternehmen: 75 %), Maßnahmen zur Sicherstellung der Betriebskontinuität (77 %, Großunternehmen: 72 %) und Maßnahmen zur Kontrolle von Lieferanten, Dienstleistern und Dritten (70 %, Großunternehmen: 63 %) angeht.

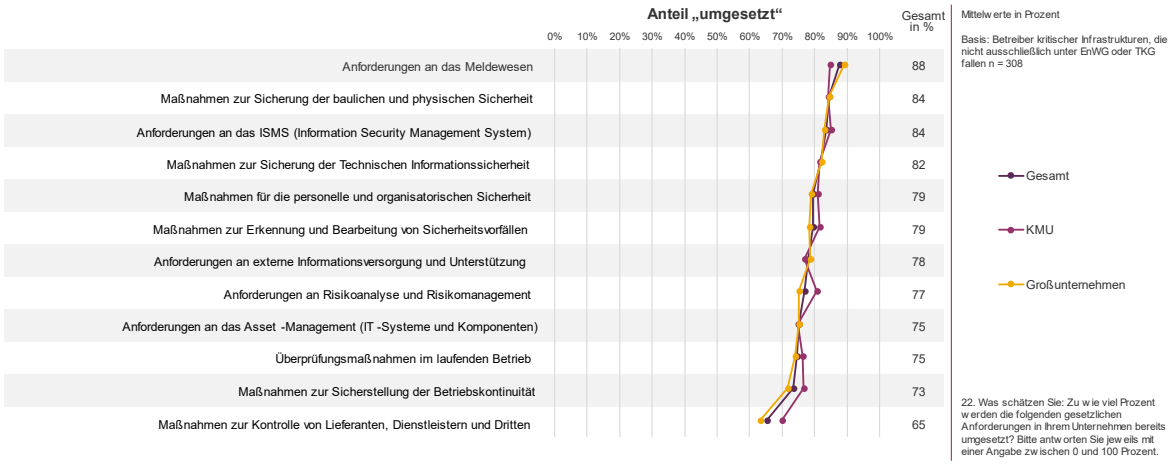

Abbildung 22: Umsetzung der IT-Sicherheitsgesetze (nach Unternehmensgröße)

Unternehmen, die mit dem IT-Sicherheitsgesetz 2.0 sehr vertraut sind, liegen in der Umsetzung sämtlicher Maßnahmen deutlich vor denjenigen mit mittlerer/ geringer Vertrautheit.

Unternehmen, die den Anforderungen bisher nur bis zu 70 Prozent genügen, haben in allen Bereichen erhebliche Defizite. Am größten sind sie bei den Maßnahmen zur Kontrolle von Dritten (34 %), Überprüfungsmaßnahmen im laufenden Betrieb und Maßnahmen zur Sicherstellung der Betriebskontinuität (jeweils 46 %).

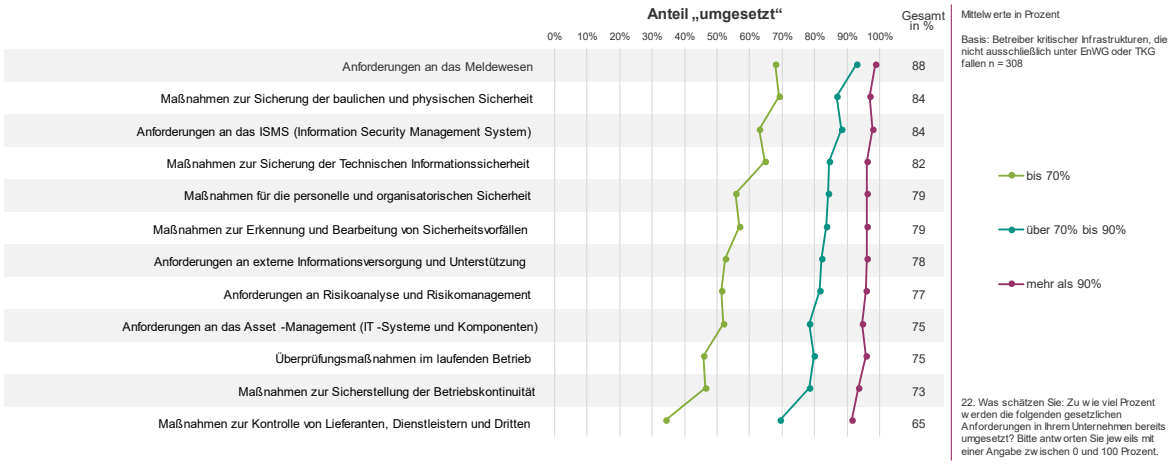

Abbildung 23: Umsetzung der IT-Sicherheitsgesetze (nach Umsetzungsstand)

Als Hauptgründe für die noch unvollständige Umsetzung der gesetzlichen Anforderungen nennen die Unternehmen vor allem Personalmangel (34 %) und fehlende finanzielle Mittel (23 %).

15 Prozent sehen die Ursache in Zeitmangel/ Kurzfristigkeit der Änderungen, 14 Prozent im allgemeinen Ressourcenmangel. Etwa jedes zehnte Unternehmen erlebt die Anforderungen als sehr hoch/ komplex (11 %) bzw. sich stetig verändernd (10 %). 9 Prozent antworten, dass die Umsetzung bei ihnen bereits erfolgt ist oder bald erfolgen wird. Jeweils 8 Prozent führen ihre Unternehmensstruktur/ organisatorische Probleme, fehlendes Bewusstsein/ Knowhow oder den allgemein hohen Aufwand an, 6 Prozent die ihrer Ansicht nach unklaren Vorgaben. In ebenfalls 6 Prozent der Unternehmen hat das Thema keine Priorität, 5 Prozent nennen die Abhängigkeit von Richtlinien/ Externen (offene Frage; Mehrfachnennungen waren möglich).

Vor allem für Großunternehmen sind Personalmangel (38 %) und fehlende finanzielle Mittel (30 %) die Hauptursachen, während nur 10 Prozent der KMU eine Budgetknappheit beklagen. Für sie ist neben fehlendem Personal (27 %) der Zeitmangel/ Kurzfristigkeit der Änderung (25 %) das größte Problem.

Unternehmen mit einem Umsetzungsstand von bis 70 Prozent geben besonders häufig an, dass es bei ihnen an Personal (42 %), Budget (38 %) und allgemeinen Ressourcen (22 %) fehlt. Überdurchschnittlich viele (18 %) begründen die Defizite auch mit fehlendem Bewusstsein/ Knowhow.

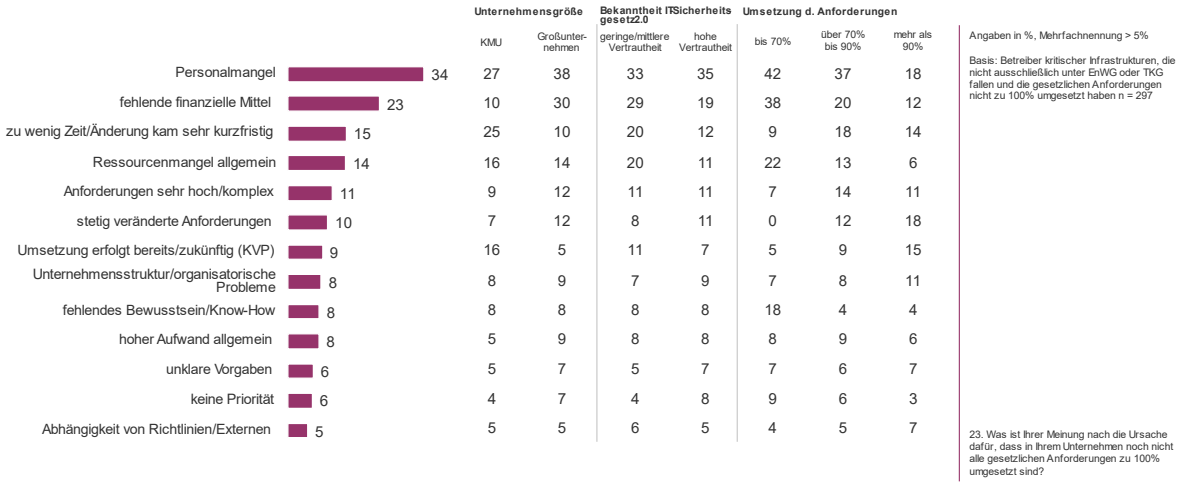

Abbildung 24: Vermutete Gründe für unvollständige Umsetzung der IT-SiG

Nur 19 Prozent der Unternehmen wollen die erforderlichen Maßnahmen bis zum Ende des laufenden Geschäftsjahres vollständig umgesetzt haben. Ein weiteres Drittel (32 %) plant, dieses Ziel innerhalb des nächsten Geschäftsjahres zu erreichen, 45 Prozent gehen von einem späteren Zeitpunkt aus. Aktuell gar

keinen Zeitplan haben 4 Prozent der Unternehmen.

KMU legen ein schnelleres Tempo vor: Zwei Drittel (64 %) gehen davon aus, die Maßnahmen in diesem (29 %) oder spätestens innerhalb des nächsten Geschäftsjahres (35 %) zu implementieren, während es bei den Großunternehmen nur 46 Prozent sind, im laufenden Geschäftsjahr sind es nur 15 Prozent.

Besonders langsam agieren die Unternehmen mit einem geringen Umsetzungsgrad (< 71 %): Nur jedes dritte Unternehmen (33 %) geht davon aus, alle Ziele spätestens bis Ende des nächsten Geschäftsjahres vollständig erreicht zu haben.

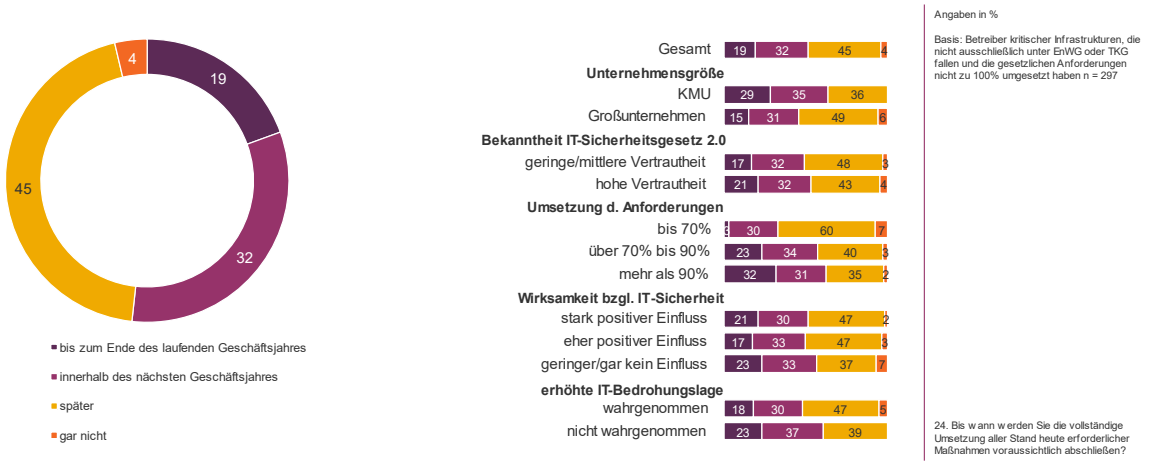

Abbildung 25: Erwartete vollständige Umsetzung der IT-SiG

Verantwortlich für die Umsetzung der IT-Sicherheitsmaßnahmen in den Unternehmen war/ ist überwiegend die IT-Abteilung (79 %), bei 60 Prozent (auch) die Geschäftsführung. 30 Prozent beauftragten einen externen Dienstleister, 27 Prozent stellten eine gesonderte Projektmanagement-gruppe zusammen. In 9 Prozent der Unternehmen war der/ die Informationssicherheitsbeauftragte zuständig, in 8 Prozent eine andere Abteilung (Mehrfachnennungen waren möglich).

Mit 83 Prozent Zustimmung hält die überwiegende Mehrheit der Unternehmen die vollständige Umsetzung aller gesetzlichen IT-Sicherheitsvorgaben bei KRITIS-Betreibern für „sehr wichtig“ (53 %) oder sogar „extrem wichtig“ (30 %). „Eher unwichtig“ ist sie nur für 2 Prozent der Befragten, völlig „unwichtig“ für niemanden.

Das vergleichsweise geringste Bewusstsein für die Vorgaben der IT-Sicherheitsgesetze äußern erwartungsgemäß Unternehmen, die diesen nur einen geringen/ keinen Einfluss zuschreiben (extrem/

sehr wichtig: 76 %), Firmen, die die Gesetze nicht ausreichend gut kennen (77 %) oder deren Anforderungen bisher nur bis

zu 70 Prozent umgesetzt haben (78 %). Aber auch in diesen Unternehmen wird die Bedeutung der vollständigen Umsetzung der gesetzlichen Vorgaben mehrheitlich anerkannt.

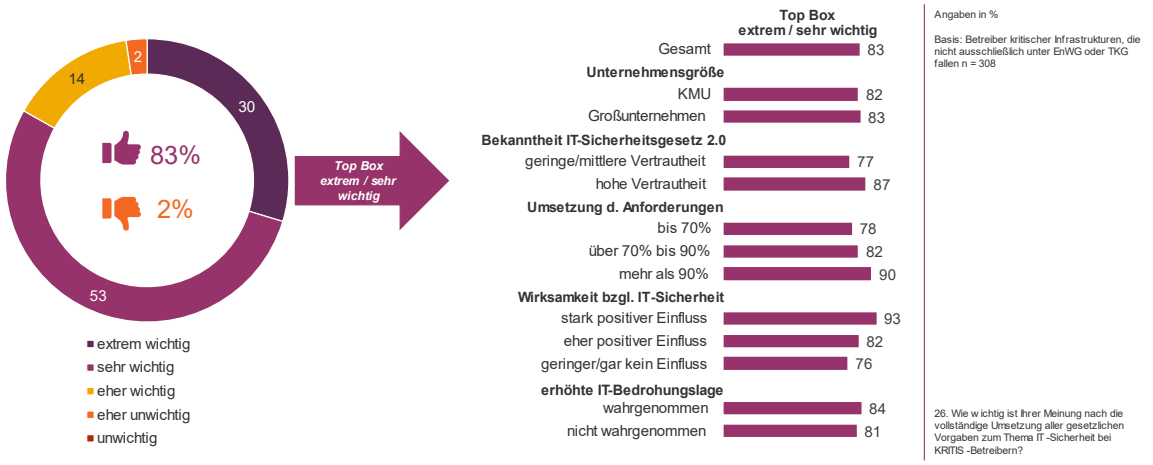

Abbildung 26: Notwendigkeit der vollständigen Umsetzung aller Vorgaben der IT-SiG

Die mit Abstand größte Herausforderung bei der Umsetzung der IT-Sicherheitsgesetze sind für die Unternehmen die Kosten für die Anpassung von IT-Systemen und -Prozessen (76 %), gefolgt von Kosten für externe Dienstleister (49 %) und fehlendem Knowhow (43 %).

Weitere häufig genannte Hürden sind die Kosten für Schulungen (31 %), Fehlverhalten von Mitarbeitenden (25 %) und Ressourcen-/ Personal-/ Fachkräftemangel (20 %).

Für einige Unternehmen stellen auch die Komplexität der Umsetzung (5 %), Zeitmangel (5 %), fehlende Priorisierung/ mangelndes Problembewusstsein bei der Unternehmensführung (4 %) und gesetzliche Vorgaben (3 %) ein Problem dar (Mehrfachnennungen waren möglich).

Großunternehmen beklagen deutlich häufiger als KMU die hohen Kosten (Anpassung von IT-Systemen: 80 %; externe Dienstleister: 52 %, Schulungen: 35 %), während für die kleineren/ mittleren Unternehmen nach den Kosten für die Anpassung von IT-Systemen und -Prozessen (69 %) das fehlende Knowhow (49 %) die zweitgrößte Herausforderung ist.

Unternehmen mit geringerem Umsetzungsstand (< 71 %) nennen überdurchschnittlich häufig mangelndes Knowhow (58 %), hohe Schulungskosten (48 %) und Fehlverhalten von Mitarbeitenden (35 %).

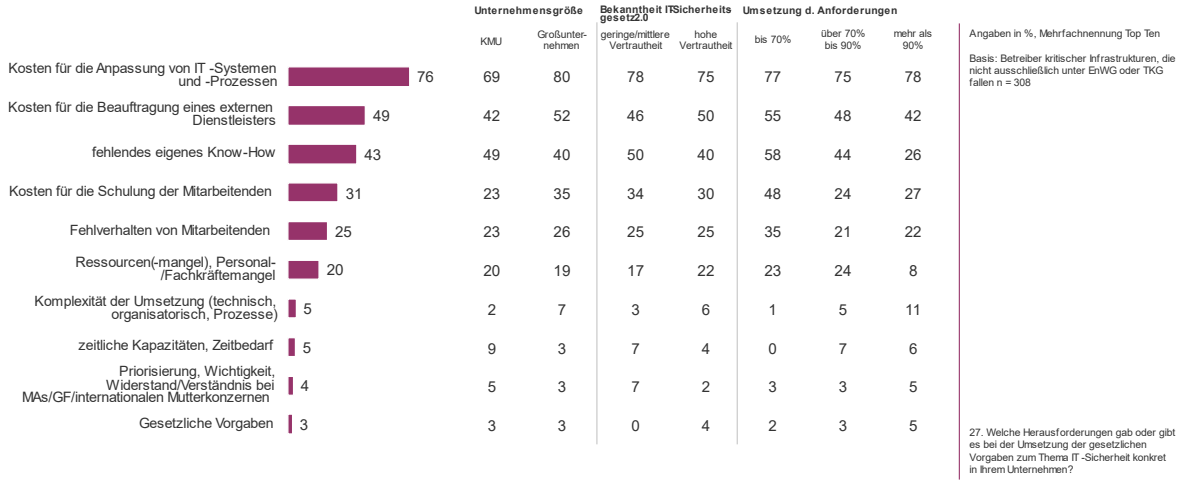

Abbildung 27: Herausforderungen bei der Umsetzung der IT-SiG

Drei Viertel der befragten Unternehmen (75 %) stellen durch externe Audits und Zertifizierung sicher, dass ihre IT-Sicherheitsmaßnahmen die gesetzlichen Anforderungen erfüllen. 23 Prozent kontrollieren das mittels regelmäßiger interner Audits. Nur 2 Prozent geben an, keine Kontrollen durchzuführen.

6.4 Nutzen und Wirksamkeit der geforderten Maßnahmen

Nahezu alle Unternehmen (90 %) halten die gesetzlichen Vorgaben für „sehr“ (33 %) oder „eher“ (56 %) sinnvoll. Nur 10 Prozent finden sie „weniger“ oder „gar nicht“ sinnvoll.

Insofern beobachten nach Umsetzung der Maßnahmen auch über drei Viertel (78 %) der Unternehmen - unabhängig von ihrer Größe - einen positiven Einfluss auf ihre IT-Sicherheit („eher“: 57 %; „stark“: 21 %). Nur 22 Prozent stellten einen „eher geringen“ (20 %) oder „gar keinen“ (2 %) Einfluss fest.

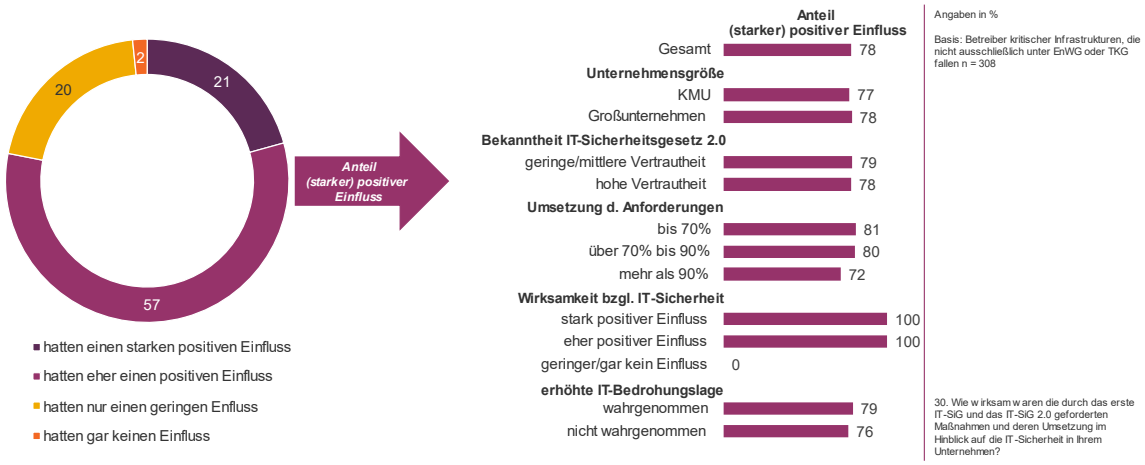

Abbildung 28: Wirksamkeit der Maßnahmen auf IT-Sicherheit

Auch die Sensibilisierung von Mitarbeitenden und Geschäftsführung wurden durch die Umsetzung der gesetzlichen Maßnahmen „eher“ (55 %) oder sogar „stark“ (17 %) positiv beeinflusst. Nur 24 Prozent schätzen den Einfluss als „eher gering“ ein, 4 Prozent sehen überhaupt keine Wirkung.

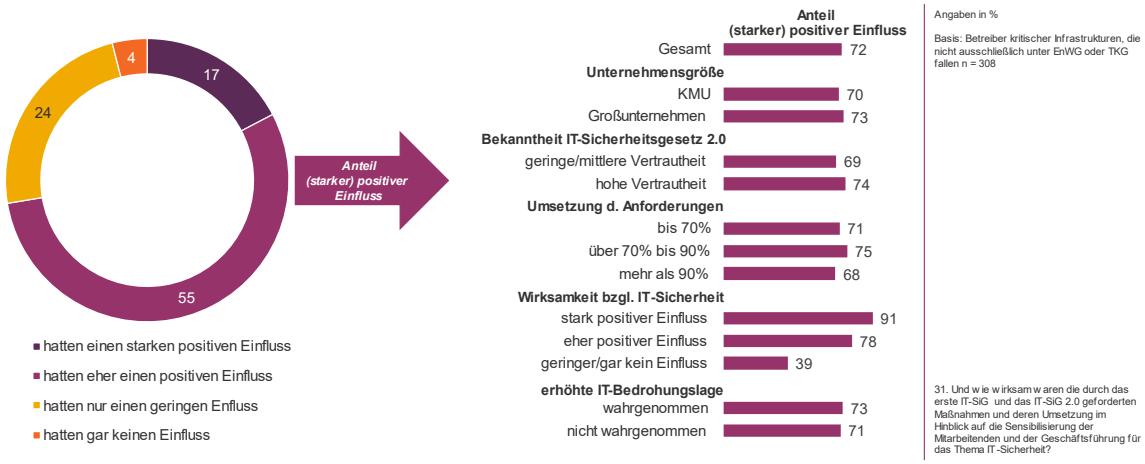

Abbildung 29: Sensibilisierung von Mitarbeitenden/ Geschäftsführung

7. BSI-PUBLIKATIONEN

Im folgenden Abschnitt stehen die Publikationen des BSI zur Diskussion: Wie bekannt sind sie, wie zufrieden sind die Unternehmen damit, und welche weiteren Wünsche haben sie an das Informationsangebot der Behörde?

7.1 Bekanntheit und Nutzung der BSI-Publikationen

Die bekanntesten und am häufigsten genutzten Publikationen des BSI sind die Tageslageberichte: 94 Prozent der befragten Unternehmen kennen sie, 87 Prozent nutzen sie. An zweiter Stelle stehen die Cyber-Sicherheitswarnungen, die 87 Prozent kennen und 81 Prozent nutzen.

83 Prozent kennen den Jahreslagebericht des BSI (Nutzung: 55 %), 79 Prozent die Orientierungshilfe B3S (Nutzung: 57 %). Die Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung ist 78 Prozent der Befragten bekannt, bei der Nutzung steht sie auf Platz 3 (66 %).

Die Orientierungshilfe Nachweise ist bei 73 Prozent der Unternehmen bekannt (Nutzung: 56 %), zwei Drittel kennen die Online-Präsenz des BSI mit der Zielgruppe KRITIS-Betreiber (Nutzung: 44 %), jeweils 56 Prozent die Vorfallsinformationen (Nutzung: 46 %) und sonstige Informationen zur Nachweiserbringung (Nutzung: 40 %).

Die geringste Bekanntheit (36 %) und Nutzung (27%) haben die Management-Informationen.

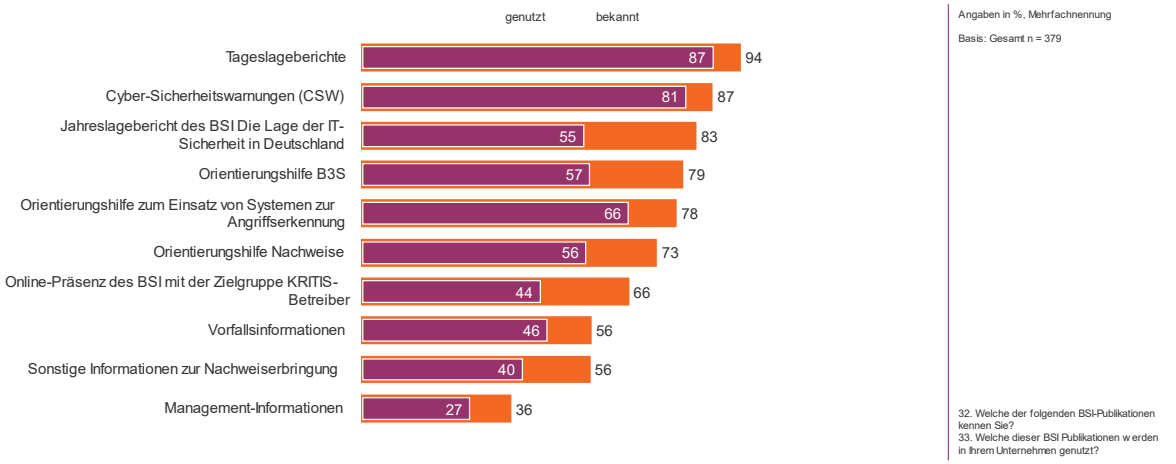

Abbildung 30: Bekanntheit und Nutzung BSI-Publikationen

Mit Ausnahme der von fast allen Befragten genutzten Tageslageberichte sind die BSI-Publikationen bei Großunternehmen besser bekannt als bei KMU. Auch in der Nutzung sind die Großunternehmen

insgesamt aktiver, lediglich die Cyber-Sicherheitswarnungen werden von KMU fast ebenso häufig rezipiert.

Am vergleichsweise wenigsten bekannt und genutzt sind die BSI-Veröffentlichungen bei Unternehmen mit geringer/ mittlerer Vertrautheit mit den IT-SiG. Besonders weit unter dem Durchschnitt liegen die Online-Präsenz (Bekanntheit: 44 %, Nutzung: 27 %) und die Orientierungshilfe zum Einsatz von System zur Angriffserkennung (Bekanntheit: 59 %, Nutzung: 48 %).

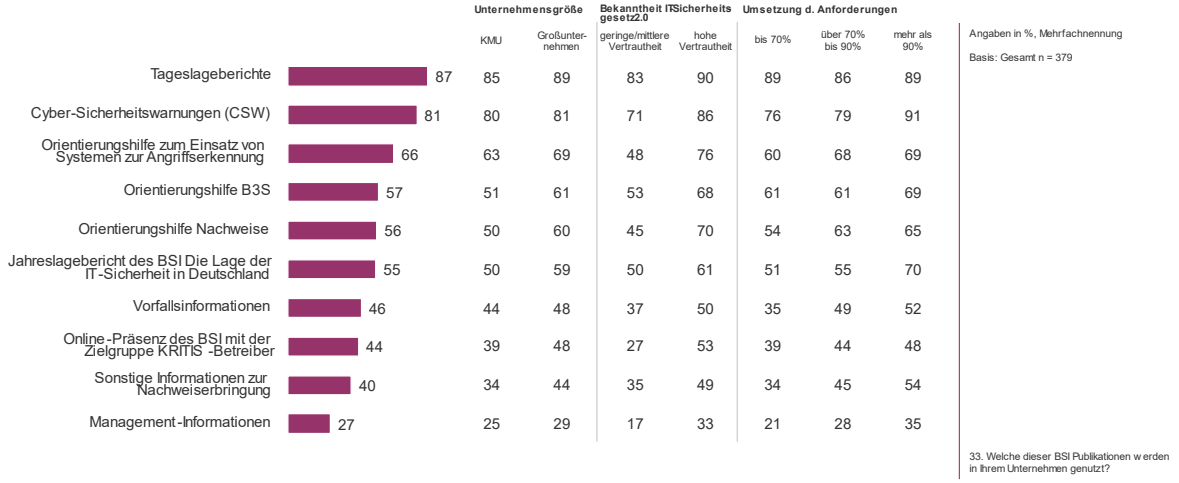

Abbildung 31: Genutzte BSI-Publikationen (nach Teilgruppen)

Für fast alle Unternehmen stellen die BSI-Publikationen einen praktischen Nutzen dar: 95 Prozent haben daraus schon „einige“ (72 %) oder „viele“ (23 %) Handlungen abgeleitet.

Auch Zufriedenheit mit dem Informationsangebot des BSI ist recht hoch. 57 Prozent der Unternehmen äußern sich zufrieden (Top Box: Werte 1/2 auf einer 6-er-Skala), 12 Prozent sogar „sehr“ (Wert 1). Bei 35 % liegt die Zufriedenheit im oberen Mittelfeld (Wert 3), bei 6 Prozent im unteren Mittelfeld (Wert 4); gar nicht zufrieden sind nur 2 Prozent (Werte 5/6).

Die deutlich geringste Zufriedenheit (Top Box: 42 %) äußern Unternehmen, die den IT-Gesetzen nur einen geringen/ keinen Einfluss zuschreiben.

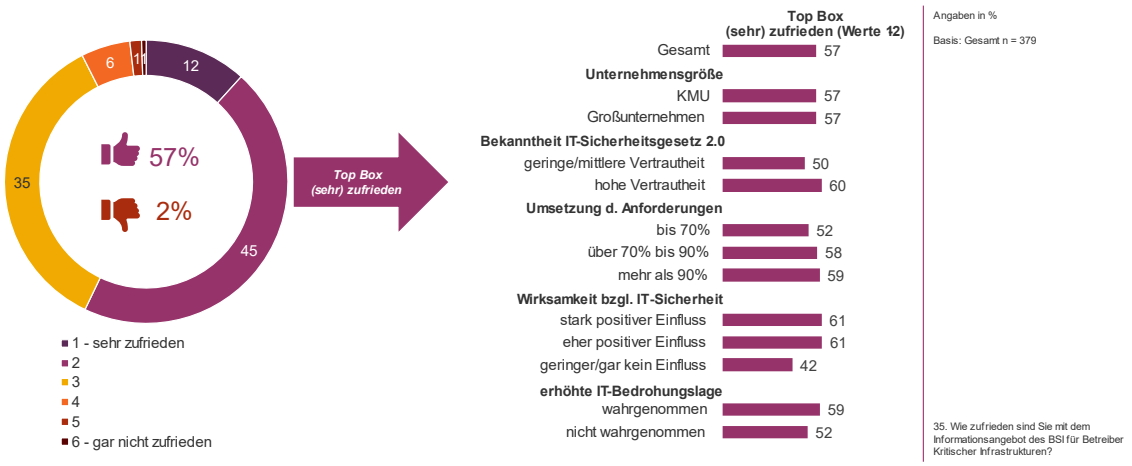

Abbildung 32: Zufriedenheit mit dem Informationsangebot des BSI

7.2 Mehrbedarf und Wünsche an das Informationsangebot des BSI

Die Mehrheit der befragten Unternehmen – 56 Prozent – ist mit dem Umfang des BSI-Informationsangebots zufrieden, 44 Prozent wünschen sich mehr Informationen für KRITIS-Betreiber. Großunternehmen sind hier etwas häufiger (46 %) vertreten als KMU (41 %).

Unternehmen, die eine erhöhte Bedrohungslage wahrnehmen, äußern am häufigsten einen Mehrbedarf (50 %).

Der größte Mehrbedarf besteht bei „zielgruppen-/ branchenspezifische Informationen“ (gewünscht von 27 Prozent der Unternehmen mit Wunsch nach mehr Informationen), gefolgt von „konkreten Lösungsansätze/ Umsetzungshinweisen“ (19 %). 12 Prozent wünschen sich „genauere/ detailliertere Informationen“, jeweils 11 Prozent mehr „Informationen zu bestimmten Themen“ und „praxisbezogene Hinweise/ Beispiele“.

Was die Gestaltung der Publikationen angeht, werden „mehr Struktur/ Übersichtlichkeit“ (7 %) und „barrierefreie Meldungen, z.B. in englischer Sprache“ (6 %) gewünscht. Ebenfalls 6 Prozent würden sich über „Informations-/ Fortbildungsveranstaltungen“ freuen (offene Frage, Mehrfachantworten waren möglich). Einzelne Unternehmen vermissen „schnellere Informationen über Schwachstellen/ Änderungen“ und „mehr Austausch/-programme“ (jeweils 2 %).

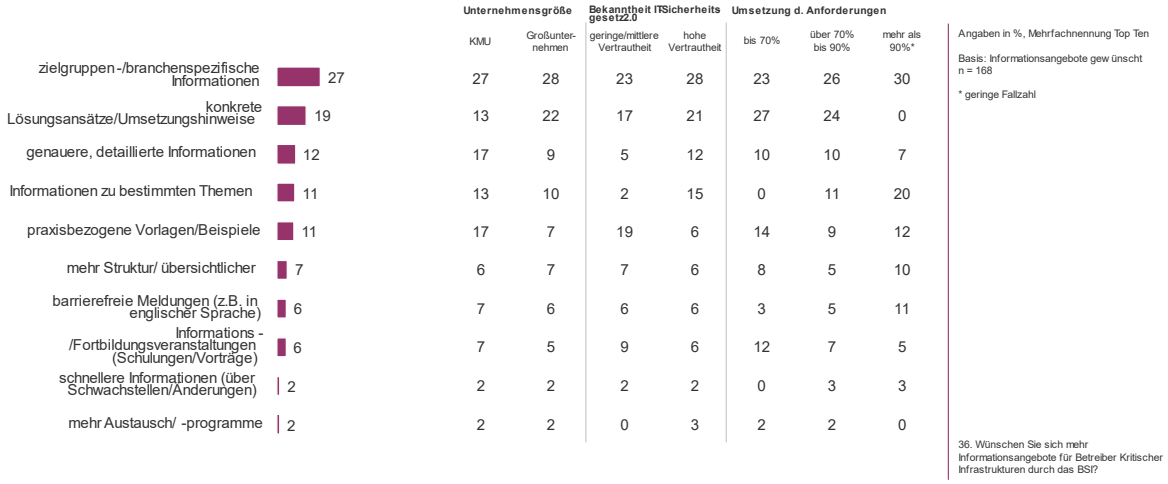

Abbildung 33: Gewünschte Informationsangebote für KRITIS-Unternehmen

7.3 Bekanntheit von im BSI-Gesetz formulierten Anforderungen zum Stand der Technik

38 Prozent der Betreiber kritischer Infrastrukturen, die nicht ausschließlich unter EnWG oder TKG fallen, kennen sämtliche Anforderungen, um die vom BSI-Gesetz formulierte „Absicherung nach dem Stand der Technik“ zu erreichen. Weitere 48 Prozent kennen einige der Anforderungen. 12 Prozent kennen sie „nur ansatzweise“, 2 Prozent gar nicht.

Die Großunternehmen sind hier umfassender informiert (alle Anforderungen: 42 %) als KMU (30 %). Am geringsten ist der Informationsgrad erwartungsgemäß bei Unternehmen mit geringer/ mittlerer Vertrautheit mit der Gesetzeslage (alle Anforderungen: 20 %) und bei Unternehmen, die bisher bis zu 70 Prozent der Anforderungen umgesetzt haben (24 %).

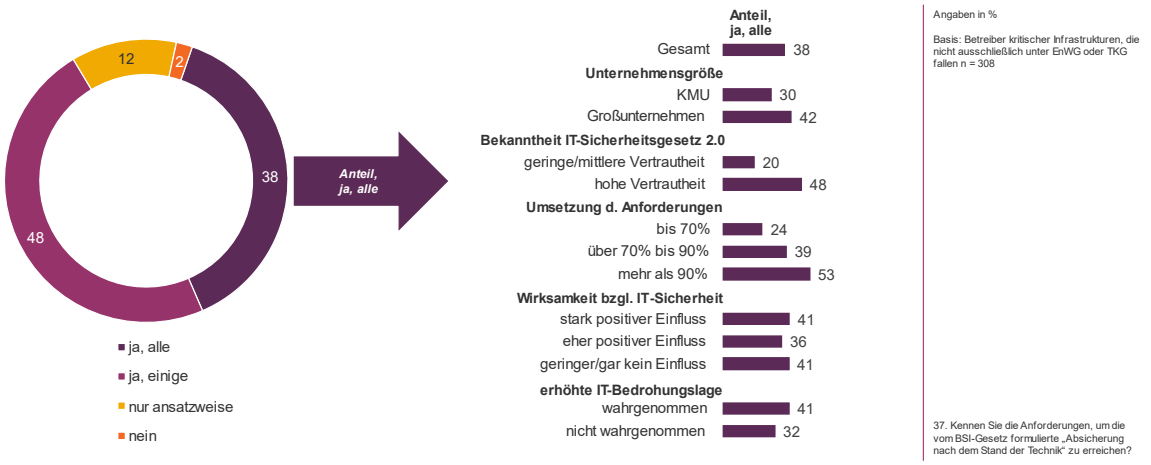

Abbildung 34: Bekanntheit „Absicherung nach dem Stand der Technik“

Eine höhere Bekanntheit haben die inhaltlichen Anforderungen an die Nachweise, die dem BSI alle zwei Jahre vorgelegt werden müssen: 79 Prozent der Unternehmen kennen sie vollständig, 16 Prozent in Teilen und 6 Prozent „nur ansatzweise“. Mit „nein“ antwortete niemand.

Hier sind die Großunternehmen wesentlich besser informiert als die KMU: 86 Prozent kennen alle Anforderungen, bei den kleinen/ mittleren Unternehmen sind es nur 65 Prozent.

Am geringsten ist auch in diesem Bereich der Informationsgrad bei Unternehmen mit geringer/ mittlerer Vertrautheit mit der Gesetzeslage (61 %) und Unternehmen mit einem Umsetzungsstand von bis 70 Prozent (64 %).

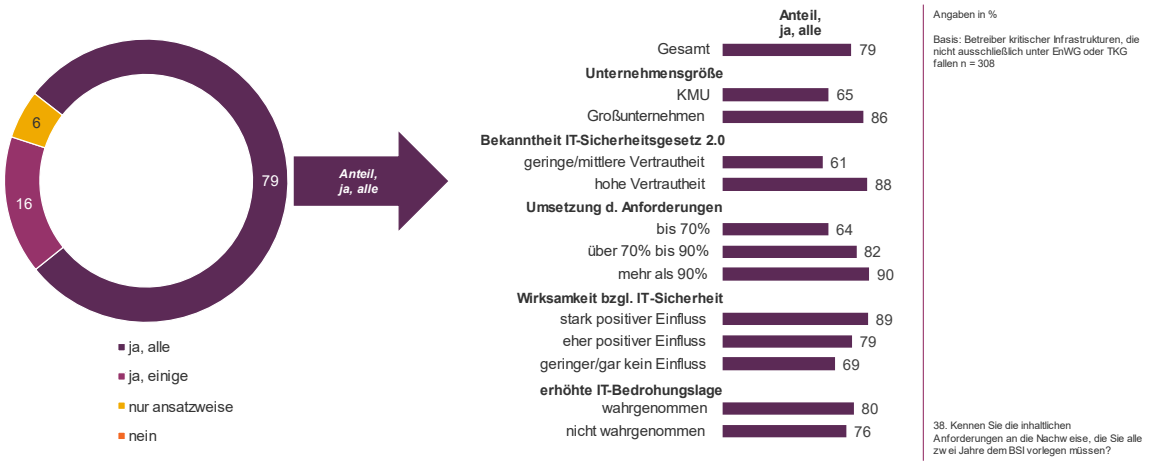

Abbildung 35: Bekanntheit der Anforderungen zur Nachweispflicht

Zwei Drittel der befragten Unternehmen (68 %) haben einen branchenspezifischen Sicherheitsstandard (B3S). Dabei handelt es sich eher um Großunternehmen (72 %) als um KMU (58 %).

69 Prozent der Unternehmen mit B3S sind – unabhängig von ihrer Größe – der Überzeugung, dass dieser Standard ihnen einen Mehrwert bringt.

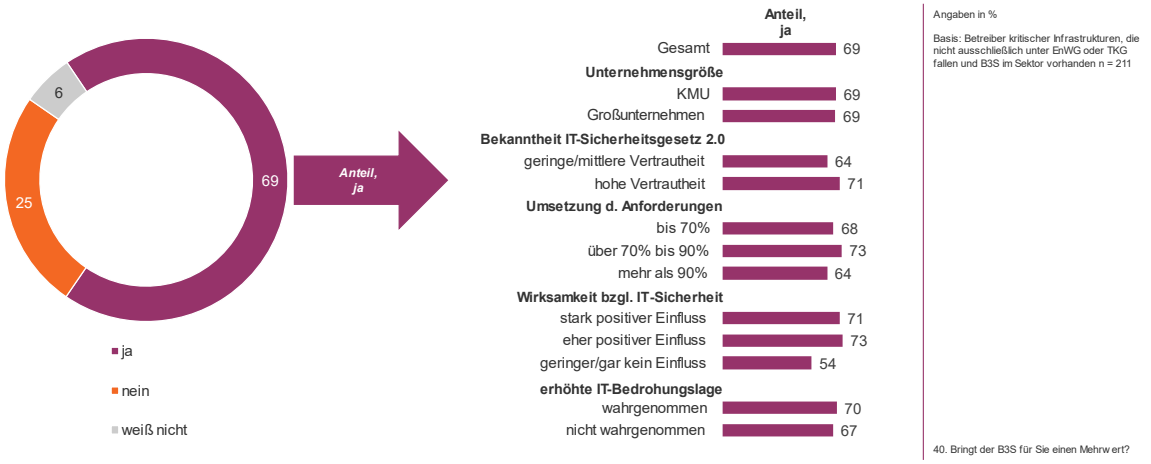

Abbildung 36: Mehrwert des B3S

80 Prozent der Unternehmen, in deren Sektor es einen B3S gibt, verwenden ihn, auch hier zeigen sich keine wesentlichen Unterschiede bei der Firmengröße.

Unternehmen, in deren Sektor es keinen B3S gibt, sind geteilter Meinung, was den Wunsch nach einem branchenspezifischen Sicherheitsstandard angeht: 37 Prozent sind dafür, 31 Prozent sind dagegen, und 32 Prozent sind unentschieden (Antwort: „weiß nicht“).

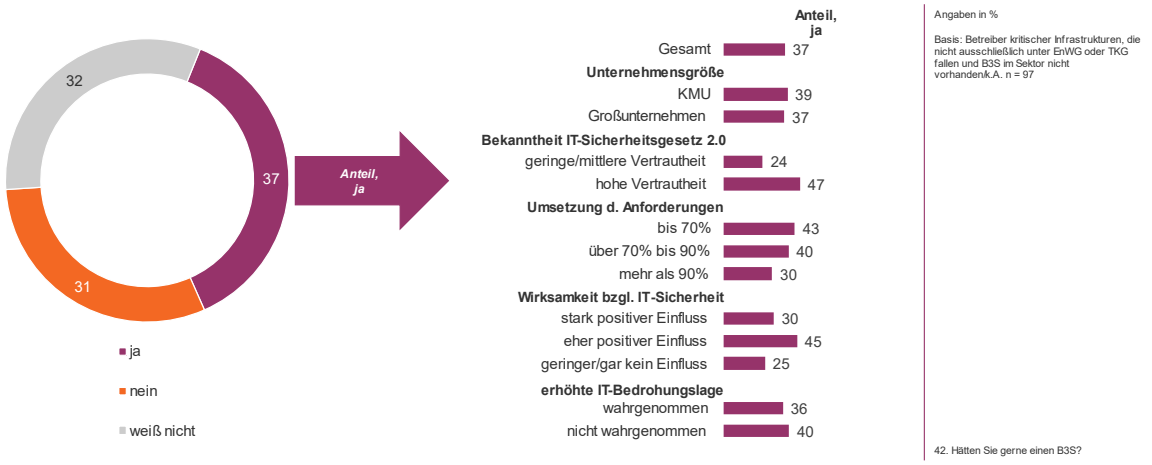

Abbildung 37: Wunsch nach B3S

31 % der befragten Unternehmen haben schon einmal an der Erstellung eines B3S mitgewirkt, Großunternehmen etwas häufiger (33 %) als KMU (27 %).

Zwei Drittel der Unternehmen (66 %) übermittelten bei ihrer Nachweiserbringung gegenüber dem BSI schon einmal Mängel, deren anschließende Beseitigung zu einer Erhöhung der IT-Sicherheit im Unternehmen geführt habe. 11 Prozent machten die gegenteilige Erfahrung: Auf ihren Mängelbericht folgte keine Verbesserung.

Mehr Großunternehmen (70 %) als KMU (58 %) berichten von einer Erhöhung der IT-Sicherheit nach einem Mängelbericht. Daraus kann aber keine größere Zufriedenstellung der Großunternehmen abgeleitet werden – im Gegenteil: dieser Anteil ist bei den KMU sogar leicht höher, da sie insgesamt deutlich seltener (67 %) Mängelberichte übermittelten als die großen Firmen (83 %).

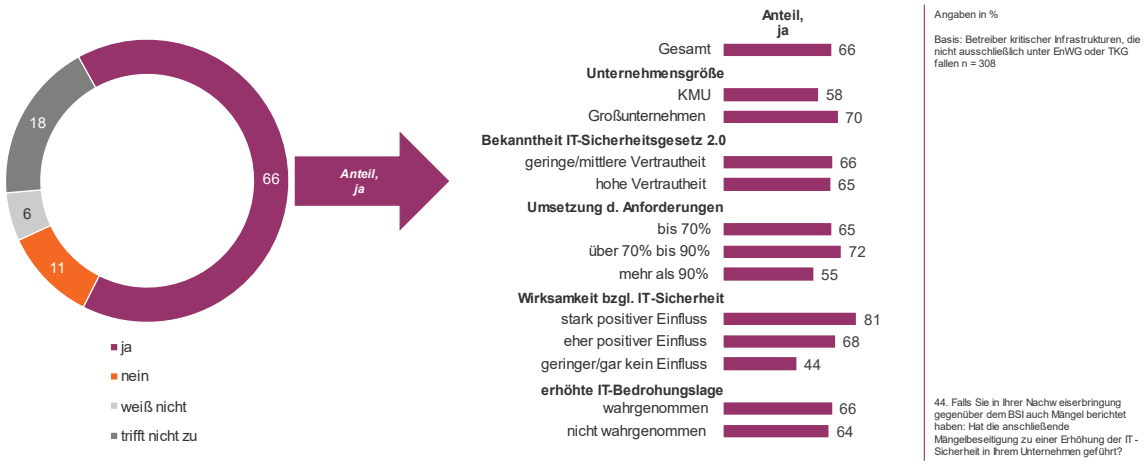

Abbildung 38: Erhöhung der IT-Sicherheit durch Mängelsicherheit

8. UNTERSCHIEDE ZWISCHEN ENWG-/ TKG-BETREIBERN UND ANDEREN KRITIS-BETREIBERN

Das abschließende Kapitel betrachtet auffällige Differenzen (> 5 %) zwischen EnWG- und TKG-Betreibern und KRITIS-Betreibern anderer Sektoren. Um die Trennschärfe zu erhalten, werden nur Fragen dargestellt, die sich an die Gesamtheit der Befragten richteten.

8.1 Unterschiede bei der Umsetzung von Sicherheitsmaßnahmen

Bei der **Umsetzung technischer Sicherheitsmaßnahmen** im Unternehmen (Kap. 4.1.) haben die EnWG-/ TKG-Betreiber einen leichten Vorsprung gegenüber den anderen KRITIS-Betreibern, die insbesondere bei der Segmentierung und Absicherung von Netzen (Differenz: -13 Prozentpunkte) und der Verschlüsselung (-10 Prozentpunkte) einen geringeren Umsetzungsstand vorweisen. Nachholbedarf gegenüber den EnWG-/ TKG-Sektoren haben sie auch bei der Einführung eines Backup-Konzepts, einer Mehr-Faktor-Authentifizierung, Client-Isolation (jeweils -8 Prozentpunkte) und der Härtung von Verzeichnisdiensten (-6 Prozentpunkte).

Umgekehrt sind die Nicht-EnWG-/ TKG-Unternehmen bei der Umsetzung von vier Maßnahmen weiter vorangeschritten: Umsetzung der End Point Protection Gesamtlösung, sichere Software-Entwicklung (Differenz: jeweils +11 Prozentpunkte), DDos Mitigation (+7 Prozentpunkte) und Schnittstellenkontrolle (+5 Prozentpunkte).

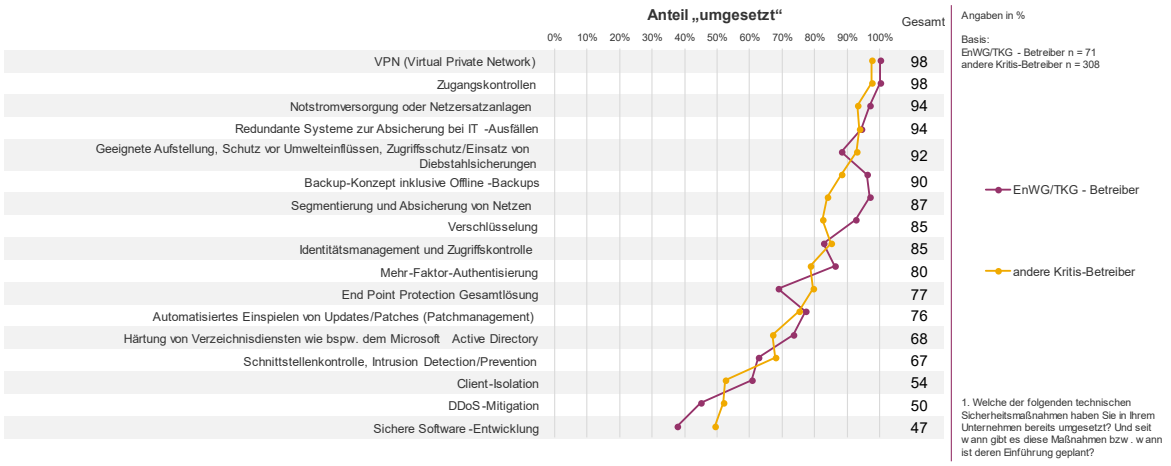

Abbildung 39: Umgesetzte technische Sicherheitsmaßnahmen (nach Betreiber)

Bei der **Implementierung organisatorischer Sicherheitsmaßnahmen** (Kap. 4.2.) liegen die Nicht-EnWG-/ TKG-Betreiber deutlicher hinter den Unternehmen der beiden anderen Sektoren. Die größten Defizite haben sie bei regelmäßigen Notfallübungen (Differenz: -10 Prozentpunkte), Continuity-/ Notfallmanagement (-8), Assetmanagement, Security Operations und Rollentrennung (jeweils -7 Prozentpunkte).

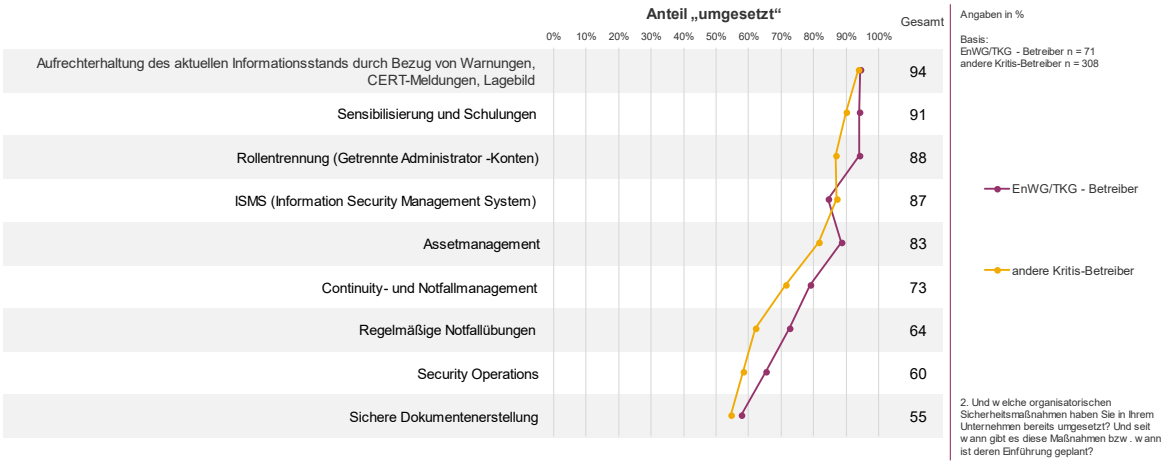

Abbildung 40: Umgesetzte organisatorische Sicherheitsmaßnahmen (nach Betreiber)

Während die Nicht-EnWG-/ TKG-Unternehmen seltener eine erhöhte **IT-Gefährdungslage aufgrund häufigerer Cyber-Angriffe** (Kap. 4.4.) wahrnehmen (nein: 53 Prozent; ja: 44 Prozent), ist die Einschätzung in den Sektoren EnWG/ TKG ausgewogener: Die Hälfte beobachtet eine stärkere Gefährdungslage, die andere Hälfte nicht.

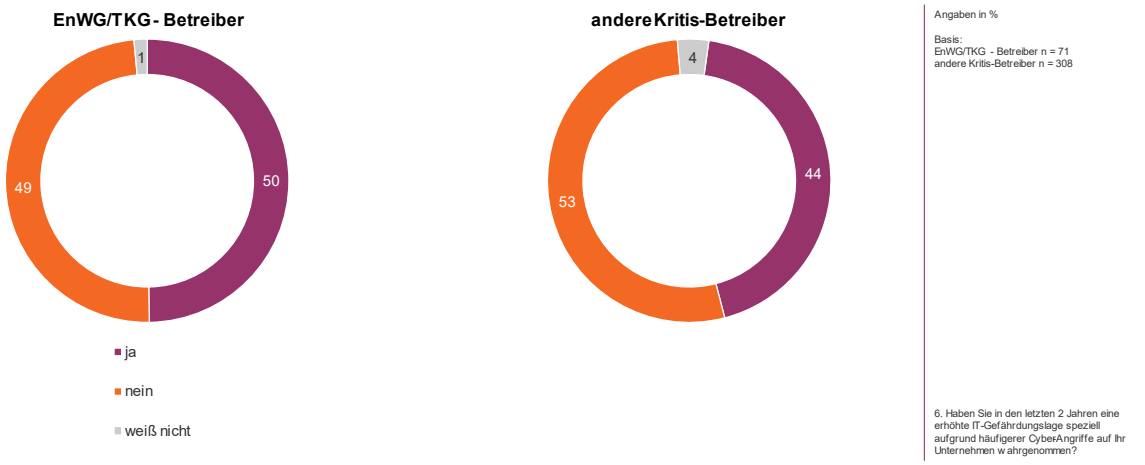

Abbildung 41: Eigene erhöhte IT-Gefährdungslage durch häufigere Cyber-Angriffe (nach Betreiber)

8.2 Unterschiede beim Stand der IT-Entwicklung und Umgang mit Sicherheitsvorfällen

EnWG-/ TKG-Unternehmen denken den Aspekt der **Informationssicherheit im Zuge der (weiteren) Digitalisierung von Geschäftsprozessen** (Kap. 5.1.) etwas häufiger von Anfang an mit (61 %) als die anderen KRITIS-Betreiber (55 %).

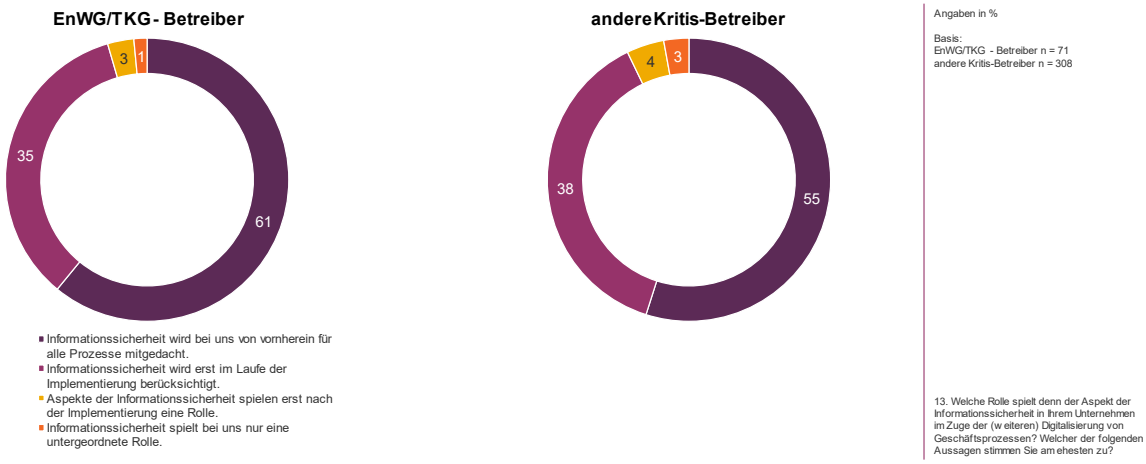

Abbildung 42: Informationssicherheit im Kontext der Digitalisierung von Geschäftsprozessen (nach Betreiber)

Bei der **Kommunikation von Sicherheitsvorfällen** (Kap. 5.2.) unterscheiden sich die Angaben der beiden Vergleichsgruppen nur graduell – mit einer Ausnahme: EnWG-/ TKG-Betreiber informieren häufiger kooperierende Unternehmen (60 %) als die anderen KRITIS-Unternehmen (50 %).

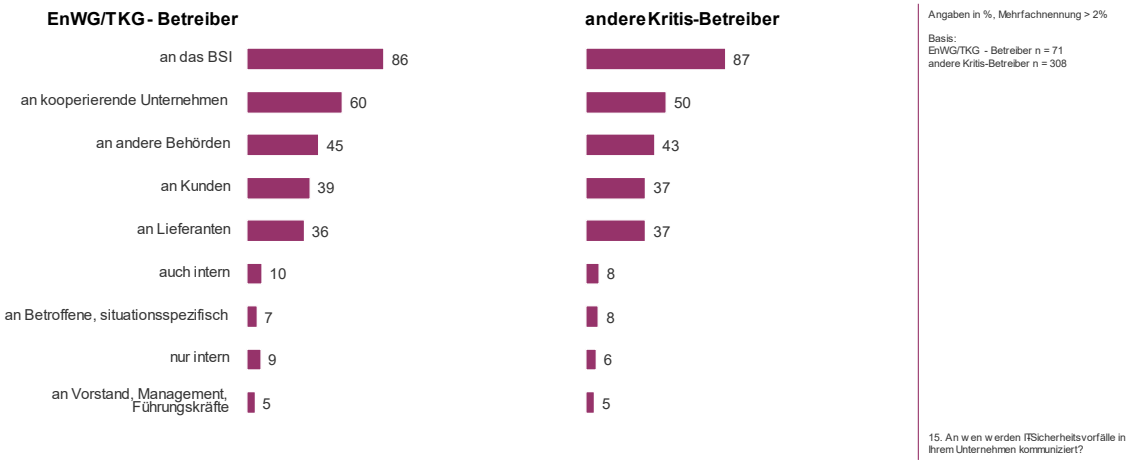

Abbildung 43: Kommunikation von IT-Sicherheitsvorfällen (nach Betreiber)

Einen deutlichen Unterschied gibt es bei der **Beseitigung von Sicherheitslücken** (Kap. 5.2.): Nicht-EnWG-/ TKG-Unternehmen beheben sie am häufigsten nach Priorisierung im Rahmen einer Risikobewertung (45 %), nur jedes vierte (24 %) beseitigt sie sofort nach deren Entdeckung. Bei EnWG-/ TKG-Betreibern hingegen liegen die umgehende Beseitigung (35 %) und die Priorisierung/ Risikobewertung (34 %) etwa gleichauf.

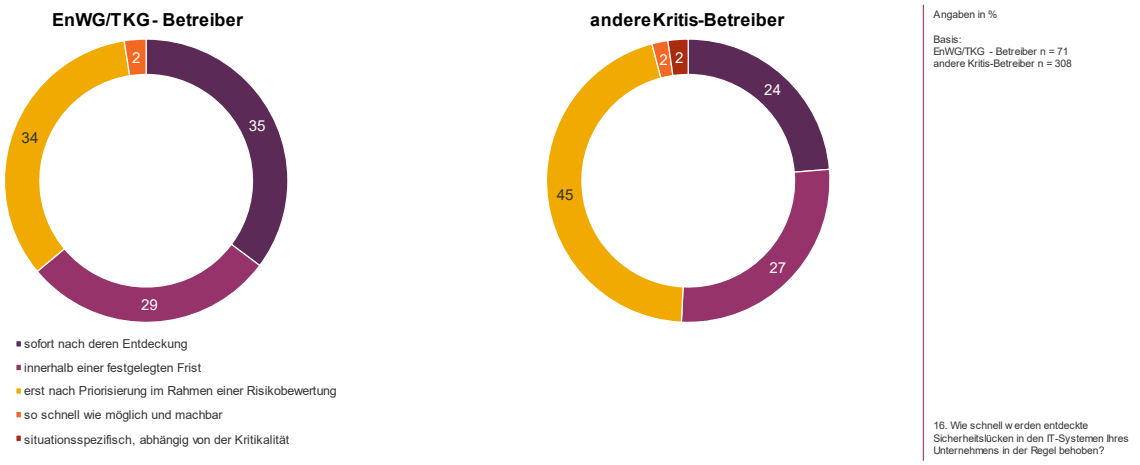

Abbildung 44: Behebung von Sicherheitslücken im IT-System (nach Betreiber)

8.3 Unterschiede bei Nutzung der BSI-Publikationen und Wünsche an das BSI

Vier der abgefragten **BSI-Publikationen** (Kap. 7.1.) werden von Nicht-EnWG/ TKG-Betreibern deutlich häufiger genutzt als von EnWG-/ TKG-Unternehmen: die beiden Orientierungshilfen B3S (63 % - EnWG/TKG: 35 %) und Nachweise (61 % - EnWG/TKG: 38 %), sonstige Informationen zur Nachweiserbringung (44 % - EnWG/TKG: 24 %) und der BSI-Jahreslagebericht (57 % - EnWG/TKG: 48 %). Bei den anderen Veröffentlichungen gibt es kaum Unterschiede in der Nutzung.

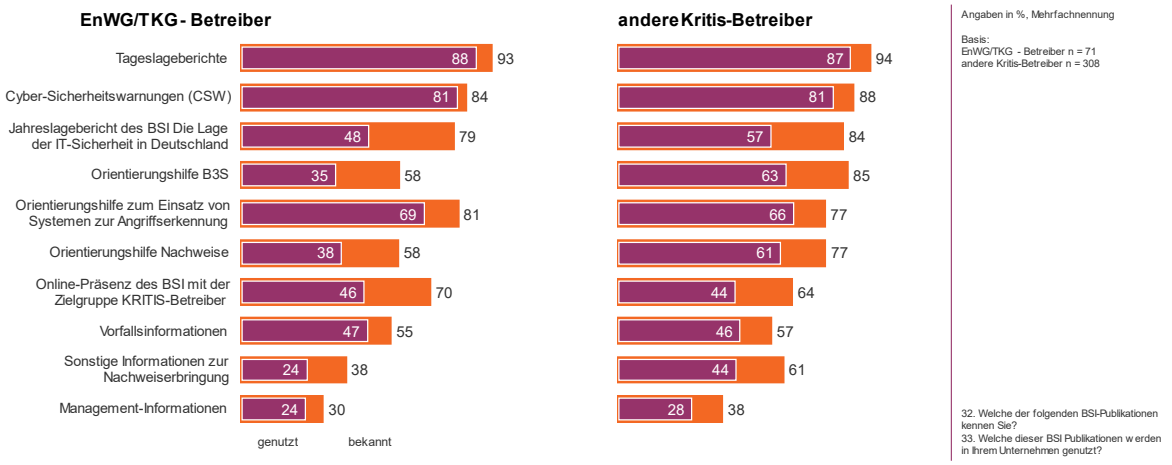

Abbildung 45: Bekanntheit und Nutzung BSI-Publikationen (nach Betreiber)

Unternehmen aus den Sektoren EnWG/ TKG **wünschen sich häufiger** als die anderen KRITIS-Betreiber „zielgruppen-/ branchenspezifische Informationen“ (32 % - Nicht-EnWG/ TKG: 26 %), „genauere, detailliertere Informationen“ (20 % - Nicht-EnWG/ TKG: 9 %), und „Informationen zu speziellen Themen“ (16 % - Nicht-EnWG/ TKG: 10 %). Den Wunsch nach Informations-/ Fortbildungsveranstaltungen äußerten hingegen ausschließlich Vertreter anderer KRITIS-Sektoren (8 %).

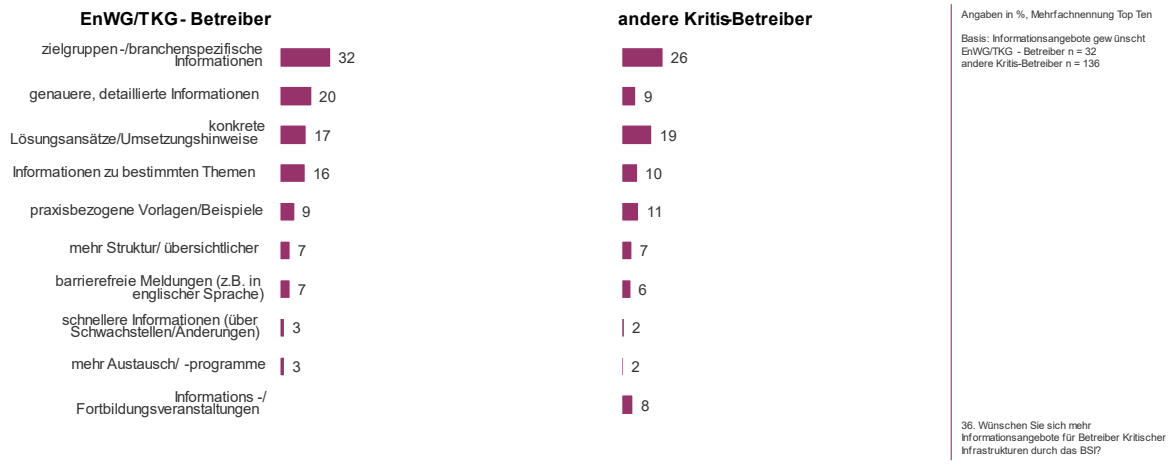

Abbildung 46: Gewünschte Informationsangebote für KRITIS-Unternehmen (nach Betreiber)

9. FAZIT

Aus den Ergebnissen der Befragung lässt sich eine Wirksamkeit der in den IT-Sicherheitsgesetzen formulierten Maßnahmen und Ziele bei den KRITIS-Betreibern ablesen. Dass es noch Defizite in der Umsetzung gibt, liegt eher an den Rahmenbedingungen, unter denen die Unternehmen agieren müssen, als an den Inhalten der Gesetzgebung.

Der Hauptgrund für die Einführung von IT-Sicherheitsmaßnahmen ist für die KRITIS-Unternehmen zwar stärker die aktuell erhöhte IT-Bedrohungslage als die IT-Gesetzgebung, doch diese spielt ebenfalls eine wichtige Rolle, insbesondere für kleine und mittlere Unternehmen, die seltener schon selbst Opfer von Cyber-Angriffen wurden.

Trotz der wahrgenommenen oder auch persönlich erfahrenen Gefährdungslage ist der Anteil der Unternehmen, die bereits (nahezu) alle gesetzlichen Forderungen umgesetzt haben, zum Teil noch nicht zufriedenstellend hoch.

Das liegt jedoch ganz überwiegend nicht daran, dass die IT-Sicherheitsgesetze zu unbekannt sind oder ihrer Wirksamkeit nicht vertraut wird - im Gegenteil: Die meisten Unternehmen sind mit den beiden IT-SiG gut, meist sogar sehr gut vertraut.

Auch die Notwendigkeit der vollständigen Umsetzung der gesetzlichen Vorgaben erhält eine sehr hohe Zustimmung, fast alle Betriebe halten den Maßnahmenkatalog für sinnvoll, und auch ihr Einfluss auf die interne IT-Sicherheit wird mehrheitlich als positiv eingeschätzt.

Die IT-Sicherheitsgesetze, die als Reaktion auf die gestiegene Gefährdungslage entstanden, haben insofern eine wichtige begleitende Funktion für die Unternehmen. Sie helfen dabei, das Problembewusstsein und das Gefühl der Dringlichkeit auch bei den Betrieben, die bisher nicht von Cyber-Angriffen betroffen waren, hoch zu halten und geben Unternehmen einen Rahmen, der sie dabei unterstützt, mit der Bedrohungssituation umzugehen. Anhand der konkreten Vorgaben können sie Schritt für Schritt ihre Abwehrmechanismen verbessern und dabei stets ablesen, wie weit sie vorangeschritten sind und an welchen Stellen noch Lücken bestehen.

So setzte in Folge des geänderten IT-SiG die überwiegende Mehrheit der Unternehmen neue Sicherheitsmaßnahmen um oder zog sie zeitlich vor – nach der Einführung der IT-SiG 1.0 und 2.0 lässt sich ein Schub bei der Umsetzung bzw. Planung von Sicherheitsmaßnahmen beobachten –, implementierte Überwachungssysteme und Audits und führte Schulungen zu den IT-SIG durch. So gut wie alle Betriebe denken Informationssicherheit im Kontext der Digitalisierung mit, dokumentieren Sicherheitsvorfälle und kommunizieren sie ans BSI.

Die Defizite in ihren internen IT-Sicherheitssystemen werden vor allem mit dem hohen finanziellen und zeitlichen Aufwand begründet, denen vielerorts Personalmangel und Budgetknappheit - bei häufig wirtschaftlich mäßiger Lage des Unternehmens - gegenüberstehen. Recht häufig fehlt es auch an dem nötigen Knowhow.

Zwischen der Vertrautheit mit den IT-SiG und dem Umsetzungsstand der gesetzlichen Vorgaben lässt sich ein Zusammenhang beobachten: In Unternehmen, die die Gesetzgebung und die Anforderungen „Absicherungen nach dem Stand der Technik“ und zur Nachweispflicht nicht gut kennen, ist der Umsetzungsstand auch überdurchschnittlich häufig niedriger.

Hier müssen Wege gefunden werden, diesen Firmen die Gesetzesinhalte nahe zu bringen, das nötige Sicherheitsbewusstsein und Hintergrundwissen zu stärken.

Potenzial bieten die BSI-Publikationen, die in diesen Unternehmen weniger bekannt sind und seltener rezipiert werden. Ihre Bekanntheit und Verbreitung, vor allem der Orientierungshilfen, sollte erhöht werden. Daneben würden sicherlich alle Firmen davon profitieren, im Angebot des BSI mehr konkrete und praxisbezogene Umsetzungshinweise sowie möglicherweise auch niedrigschwelligere Informationen zu finden, die den Einstieg in das Thema erleichtern.

ABBILDUNGSVERZEICHNIS