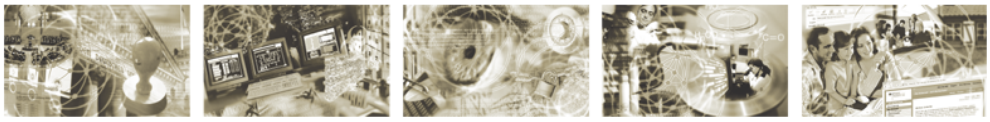
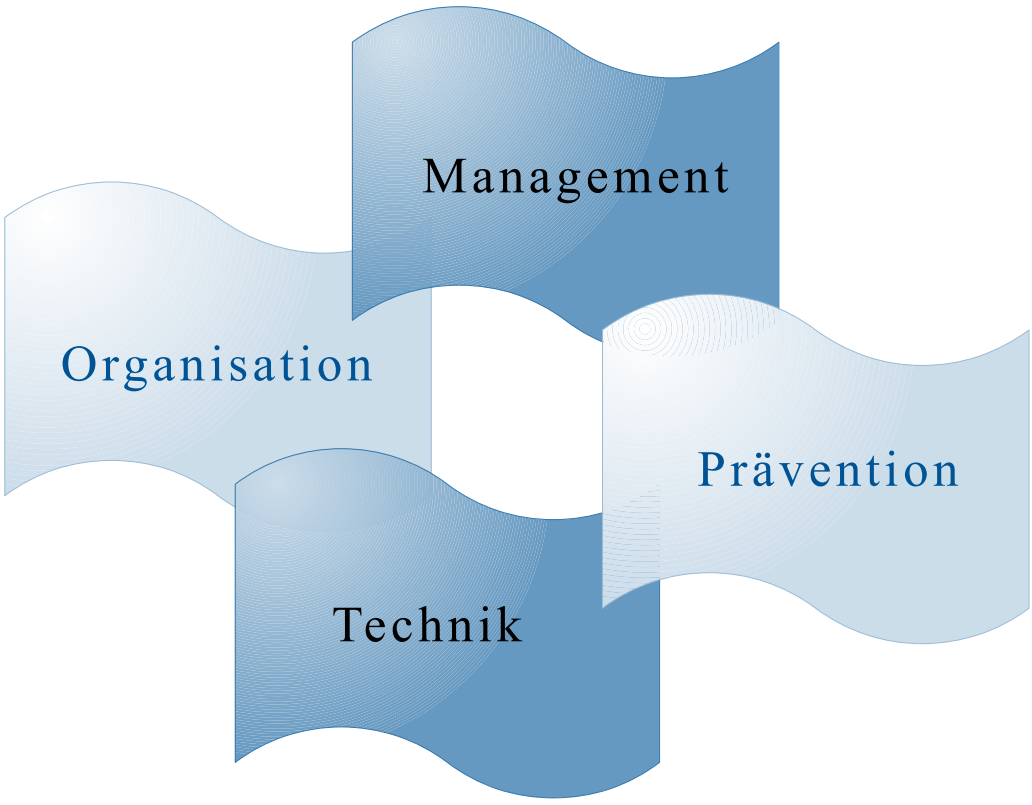
Bundesamt
für Sicherheit in der
Informationstechnik



Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen

Grad der Sensibilisierung des Mittelstandes in Deutschland



Eine Publikation des
Bundesamtes für Sicherheit in der Informationstechnik (BSI)

in Zusammenarbeit mit
secunet Security Networks AG

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: KMU-Sicherheitsstudie@bsi.bund.de
Internet: https://www.bsi.bund.de

Vorwort des Präsidenten

Sehr geehrte Leserinnen und Leser,

„Made in Germany“ ist nach wie vor ein Qualitätsmerkmal, das international anerkannt ist, geschätzt und nachgefragt wird. In diesem Zusammenhang stehen oft und zurecht die großen, weltweit operierenden Konzerne aus Deutschland im Fokus. Die Rolle des deutschen Mittelstands, der als Innovationstreiber fungiert, neue Produkte und Technologien entwickelt und so zum Erfolg der deutschen Wirtschaft entscheidend beiträgt, wird häufig unterschätzt.

In Zeiten elektronischer Geschäftsprozesse und weltweiter Vernetzung ist die effiziente und effektive Nutzung moderner Informationstechnologie genauso wichtig für den Erfolg eines Unternehmens wie Innovationen, wettbewerbsfähige Produkte oder Dienstleistungen und motivierte Mitarbeiter. Informationstechnologie kann jedoch nur dann zum Erfolg beitragen, wenn sie verlässlich arbeitet, oder allgemeiner „sicher“ ist. Datenverluste, Sicherheitslücken in Technik oder Anwendungen oder Ausfälle oder das nicht autorisierte Mitlesen der elektronischen Kommunikation durch Dritte können erhebliche Folgen für die Reputation, in Extremfällen sogar für das Überleben des Unternehmens im Wettbewerb haben. Kleine und mittlere Unternehmen (KMU) in Deutschland sind nicht zuletzt aufgrund des dort vorhandenen Know-hows ein beliebtes Ziel für Online-Kriminelle, Wirtschaftsspione und Produktpiraten, die sich die weitgehend elektronische Verarbeitung von Informationen und das Wissen über Geschäftsprozesse zunutze machen wollen. Ein hohes Niveau an IT-Sicherheit ist daher als ein erheblicher Erfolgsfaktor anzusehen, dieses Niveau zu erreichen und kontinuierlich zu verbessern sollte in der Zielsetzung aller KMU mit besonderer Priorität besetzt sein.

Das IT-Sicherheitsniveau kann jedoch nur weiterentwickelt und verbessert werden, wenn der aktuelle Status bekannt ist und die Beseitigung vorhandener Defizite offen angegangen wird. Das BSI hat in dieser Studie den Ist-Zustand der IT-Sicherheit in kleinen und mittleren Unternehmen in Deutschland abgefragt und analysiert. Es zeigt sich dabei, dass die KMU in bestimmten Unternehmensteilen sehr gut aufgestellt sind, während teilweise in der Steuerung der Unternehmen in Richtung IT-Sicherheit noch Defizite zu verzeichnen sind.

Die Schaffung von IT-Sicherheit ist keine Einzelmaßnahme, sondern immer ein Prozess, der die kontinuierliche Betrachtung und Anpassung verschiedener Faktoren erfordert. Im Rahmen der Studie hat das BSI daher unter anderem die Bereiche Management und Organisation, Infrastruktur und Anwendungen sowie auch Präventionsmaßnahmen analysiert. Dazu wurden sowohl die IT-Leitung als auch die Ebene der Geschäftsführer oder Vorstände befragt, die naturgemäß durchaus unterschiedliche Auffassungen zu den Themen IT und IT-Sicherheit haben können. Beide Sichtweisen sind in die Studie eingeflossen, so dass diese somit ein umfassendes Bild des Ist-Zustands der IT-Sicherheit in KMU abgibt.

Die Studie zeigt neben einem Statusbericht auch deutliche Verbesserungspotenziale und Handlungsempfehlungen auf. Auch vor dem Hintergrund der Cyber-Sicherheitsstrategie für Deutschland dient die Studie allen KMU in Deutschland als Richtschnur und Planungshilfe. Inhalt und Aufbau der Studie können zur Selbstanalyse, zur Verbesserung der IT-Sicherheit und damit auch zur Sicherung ihrer Geschäftsprozesse und des Unternehmenserfolgs verwendet werden.

Ich wünsche Ihnen eine aufschlussreiche Lektüre!

Michael Hange, Präsident des Bundesamts für Sicherheit in der Informationstechnik

Danksagung

Deutschland ist eine wirtschaftlich erfolgreiche Exportnation. Dieser Erfolg beruht nicht nur auf den großen Unternehmen, den „Global-Playern“. Gerade der Mittelstand mit seinem Ideenreichtum, seiner Flexibilität und Innovationsfähigkeit ist das Rückgrat des Wirtschaftsstandortes Deutschland. Dieses „Know-How“ ist ein kostbares Gut, das es zu schützen gilt.

Das Bundesministerium des Innern (BMI) hat deshalb unter Federführung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) die vorliegende Studie initiiert, die der Verbesserung der Informationssicherheit in der deutschen Wirtschaft dienen soll.

Ein besonderer Dank gilt der Arbeitsgemeinschaft für Sicherheit in der Wirtschaft e.V. (ASW) und anderen Stellen für ihre Mitwirkung bei der Gewinnung geeigneter Teilnehmer aus der Wirtschaft für die Studie.

Das BSI bedankt sich bei allen mitwirkenden Unternehmen für ihre Bereitschaft, an umfangreichen Interviews teilzunehmen. Sie haben durch ihre Auskunftsbereitschaft maßgeblich zum Wirtschaftsschutz in Deutschland beigetragen. Der gewährte Einblick in den „Mikrokosmos“ eines jeden Unternehmens weist in der Gesamtschau nicht nur auf die bestehende Gefahrenlage hin, sondern zeigt auch konkrete Wege zur Verhinderung auf – dies gerade auch für die kleinen und mittleren Unternehmen in Deutschland.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Management Summary

Über 99 Prozent der Unternehmen in Deutschland sind dem Bereich der kleinen und mittleren Unternehmen (KMU) zuzuordnen. Aus diesem Grund sind KMU ein wesentlicher Faktor für den Erfolg der deutschen Wirtschaft. Viele wirtschaftliche Prozesse – insbesondere auch im öffentlichen Bereich – hängen mittelbar oder unmittelbar von der Leistungsfähigkeit der KMU ab.

Im Zeitalter elektronischer Geschäftsprozesse ist eine funktionierende und sichere IT-Infrastruktur eine Voraussetzung für diese Leistungsfähigkeit. Daher ist es insbesondere auch aus Gründen der Verlässlichkeit für den öffentlichen Sektor notwendig, dass in Bezug auf die IT-Infrastrukturen die Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität in den KMU gewährleistet werden können.

Diese Studie hat zum Ziel, den Ist-Zustand des IT-Sicherheits- und Krisenmanagements sowie der Sicherheit kritischer IT-Infrastrukturen im Bereich der KMU zu ermitteln. Die Identifikation der kritischen Bereiche verfolgt das Ziel einer Sensibilisierung der verantwortlichen Personen. Durch das Aufzeigen von Verbesserungspotenzialen und das Benennen von Handlungsempfehlungen ist diese Studie zudem eine Planungshilfe für Unternehmen, bietet aber auch eine Orientierung für den öffentlichen Sektor.

Ergebnisse

Die Ergebnisse der Studie machen deutlich, dass die kleinen und mittleren Unternehmen im Bereich der IT-Sicherheit grundsätzlich geeignet aufgestellt sind. Im Durchschnitt werden rund zwei Drittel der in Anlehnung an den IT-Grundschutz abgefragten IT-Sicherheitsmaßnahmen in den Unternehmen umgesetzt. In einzelnen Teilbereichen gibt es jedoch erheblichen Nachholbedarf. Insbesondere im Bereich der geschäftskritischen IT-Sicherheitsprozesse – dem Umgang mit *Sicherheitsvorfällen*, dem *Notfallmanagement* und der *Bewertung der Gefahrenbereiche* zeigen sich deutliche Schwächen.

Überdurchschnittlich viele Sicherheitsmaßnahmen werden dagegen in den Bereichen *Datensicherung*, *Risikobewertung der Geschäftsprozesse*, *Aktualität der Informationen zur Bedrohungslage,* zu *Schwachstellen und Sicherheitsupdates* sowie zur *Absicherung der Netzwerke* umgesetzt.

Bei einer Gesamtbetrachtung der IT-Sicherheitsmanagementprozesse zeigt sich, dass auf Ebene der kleinsten Organisationseinheiten Prozesse organisiert, Eingangswerte und Ergebnis definiert sind. Die Sicherheitsmanagementprozesse sind jedoch nicht aufeinander abgestimmt. Auch ist das Bewusstsein für einen Prozess als Arbeitsgrundlage bei den befragten Unternehmen nicht durchgehend präsent. Anpassungen der Prozesse sind das Ergebnis von Versuch und Irrtum, folgen aber nicht einem vorher festgelegten Konzept. Dies ist insbesondere im Bereich der Vorbeugung von Sicherheitsvorfällen sowie dem Notfallmanagement zu erkennen.

Auch im Bereich der personellen Maßnahmen gibt es in vielen Unternehmen noch Nachholbedarf. Obwohl die Unternehmensleitung aus Sicht aller Befragten die Verantwortung für die Informationssicherheit deutlich sichtbar übernommen hat, zeigen sich in der Verteilung der Funktionen und Aufgaben in der Praxis Spannungsfelder. So benennt nur jedes zweite Unternehmen einen IT-Sicherheitsverantwortlichen. In vielen Fällen wird die IT-Leitung mit dieser Aufgabe beauftragt.

Zudem konnte festgestellt werden, dass es einen erhöhten Abstimmungsbedarf zwischen Geschäftsführung und IT-Verantwortlichen gibt. So wurden von den IT-Verantwortlichen

beispielsweise die IT-Sicherheitsmanagementprozesse und Ergebnisse im Vergleich zur Geschäftsführung tendenziell schlechter eingestuft.

Handlungsempfehlung

Die Ergebnisse zeigen, dass in den Themenbereichen *Bewertung von Gefahrenbereichen, Behandlung von Sicherheitsvorfällen* und *Notfallmanagement* sofortiger Handlungsbedarf besteht. Bei der Behandlung von Sicherheitsvorfällen kommt es darauf an, eine möglichst große Bandbreite von Sicherheitsvorfällen rechtzeitig zu erkennen und angemessen behandeln zu können. Es wird empfohlen, hierauf aufbauend ein Notfallmanagement umzusetzen.

Um ein dauerhaft hohes Niveau an IT-Sicherheit zu erreichen, müssen sowohl die erforderlichen Schutzmaßnahmen umgesetzt, als auch die zugehörigen IT-Sicherheitsmanagementprozesse etabliert und standardisiert werden. Es ist nicht ausreichend, Sicherheitsmaßnahmen umzusetzen, deren Funktionalität und Eignung aufgrund fehlender Prozesse nicht regelmäßig überprüft werden.

Alle Maßnahmen kurzfristig umzusetzen stellt jedoch gerade kleine und mittlere Unternehmen vor große Herausforderungen, da das Thema IT-Sicherheit komplex ist und die in den Unternehmen zur Verfügung stehenden Ressourcen stark begrenzt sind. Daher sollten alle notwendigen Sicherheitsmaßnahmen und -prozesse sukzessive umgesetzt werden. Personellen Engpässen kann beispielsweise mit Präventivmaßnahmen entgegengesteuert werden.

Die Selbsteinschätzung der Unternehmen deutet auf ein hohes Bewusstsein für die Bedeutung der IT-Sicherheit hin. Der Umsetzungsgrad der technischen Maßnahmen trägt dem im Wesentlichen Rechnung. Im Gegensatz hierzu sind die IT-Sicherheitsmanagementprozesse jedoch weder durchgehend vorhanden noch standardisiert. Hier sollten die Schutzmaßnahmen ausreichend dokumentiert und angemessene Qualitätskriterien definiert sein.

Fazit

Das Bewusstsein für Themen der IT-Sicherheit ist in deutschen KMU vorhanden. Auch in technischer Hinsicht sind viele Unternehmen gegen die Gefahren und Angriffe auf ihre IT gerüstet. Die Ergebnisse der Studie lassen allerdings auch Defizite erkennen, die sich negativ auf die Leistungsfähigkeit der Unternehmen auswirken können. Dabei sind vor allem die Präventivmaßnahmen und die IT-Sicherheitsmanagementprozesse zu nennen, denen bislang zu wenig Beachtung geschenkt wird.

Methodik

An der Studie waren 30 kleine und mittlere Unternehmen aus den Branchen produzierendes Gewerbe, Handel und Dienstleistung beteiligt. Die Datenerhebung erfolgte in Form von Interviews sowohl mit der IT-Leitung als auch der Geschäftsleitung, die – wie auch die anschließende Auswertung – von IT-Sicherheitsexperten durchgeführt wurden. Die Ergebnisse wurden in einer zweiten Befragung mit den Unternehmen diskutiert und vertieft. Hier konnten etwaige Fehlinterpretationen identifiziert und korrigiert werden. Diese Vorgehensweise stellte im Unterschied zu bisher verfügbaren Studien eine über den reinen Interviewfragebogen hinausgehende Erfassung und Bewertung des aktuellen Standes der IT-Sicherheit bei den teilnehmenden Unternehmen sicher. Aus Gründen der Vertraulichkeit enthält die vorliegende Studie kumulierte und anonymisierte Ergebnisse.

2 Einleitung

Über 99 Prozent der Unternehmen in Deutschland sind dem Bereich der kleinen und mittleren Unternehmen (KMU) zuzuordnen [Stat 2010]. Somit sind KMU ein wesentlicher Faktor für den Erfolg der deutschen Wirtschaft. Viele wirtschaftliche Prozesse – insbesondere auch im öffentlichen Bereich – hängen mittelbar oder unmittelbar von der Leistungsfähigkeit der KMU ab. Neben den Mitarbeitern und der passenden Unternehmensstrategie bildet vor allem eine funktionierende IT-Infrastruktur die Basis für diese Leistungsfähigkeit. Daher ist es auch aus Gründen der Verlässlichkeit für den öffentlichen Sektor notwendig, dass in Bezug auf die IT-Infrastrukturen die Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität in den KMU gewährleistet werden können. Fehlende oder unzureichend umgesetzte IT-Sicherheitsmaßnahmen können weitreichende Folgen haben, sowohl wirtschaftlich, als auch für die Reputation. Im Zuge der globalen Vernetzung kann das Versenden einer einfache E-Mail ausreichen, um wertvolles Wissen in falsche Hände geraten zu lassen. Auch der zunehmende Einsatz mobiler Endgeräte wie Smartphones und Tablet-Computer sowohl im privaten, als auch im professionellen Umfeld, stellt aufgrund der vielfältigen Schwachstellen [BSI_2011g] eine Herausforderung für die IT-Sicherheitsverantwortlichen der Unternehmen dar [BSI_mE11]. Um IT-Sicherheit zu gewährleisten, ist es daher essenziell, das gesamte Unternehmen einschließlich aller Mitarbeiter in dieses Thema einzubeziehen.

2.1 Zielsetzung der Studie

Ziel dieser Studie ist es, den Status der IT-Sicherheit in Bezug auf die Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität bei ausgewählten KMU zu erheben und zu bewerten sowie den Bedarf an Sensibilisierung, Beratung und Schutz zu ermitteln.

Durch konkrete Handlungsempfehlungen ist diese Studie zudem eine Planungshilfe, die eine systematische Verbesserung des IT-Sicherheitsniveaus für kleine und mittlere Unternehmen aber auch für den öffentlichen Sektor unterstützt.

Die Ziele der Studie sind im Einzelnen:

- **Ermittlung und Bewertung des Ist-Zustands der IT-Sicherheitsmaßnahmen in den Unternehmen.** Anhand eines Fragenkatalogs werden die umgesetzten organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsmaßnahmen ermittelt. Auf Basis dieser Daten wird bewertet, ob ein Sicherheitsniveau vorherrscht, das angemessen und ausreichend ist, die geschäftsrelevanten Informationen zu schützen.
- **Ermittlung und Bewertung der Prozessqualität in Bezug auf die Umsetzung der IT-Sicherheitsmaßnahmen.** Es galt hierbei die Fragen zu beantworten, ob in den teilnehmenden Unternehmen IT-Sicherheitsmanagementprozesse etabliert sind und ob diese geeignet sind, IT-Sicherheitsmaßnahmen effektiv zu steuern.
- **Entwicklung konkreter Handlungsempfehlungen für die Unternehmen.** Auf Basis der erhobenen Daten werden konkrete Handlungsempfehlungen zur Verbesserung der IT-Sicherheit benannt.
- **Gezieltes Aufzeigen der Stärken und Schwächen innerhalb der Sicherheitsprozesse.** Die Stärken und Schwächen der KMU bei der Umsetzung von IT-Sicherheitsprozessen

werden gezielt identifiziert und Handlungsempfehlungen zur Stärkung des deutschen Mittelstands aufgezeigt.

2.2 Erwartungshaltung

Mit der Erfassung und Untersuchung wesentlicher Aspekte kritischer Geschäftsprozesse und IT-Infrastrukturen in KMU etabliert diese Studie das Thema IT-Sicherheit als wichtigen Bestandteil der Absicherung des Unternehmenserfolgs.

Das gezielte Aufzeigen der Stärken und Schwächen innerhalb der IT-Sicherheitsprozesse soll die Sensibilisierung des deutschen Mittelstandes für das Thema IT-Sicherheit erhöhen und sowohl unternehmensinterne als auch übergreifende Abstimmungsprozesse fördern.

In diese Sensibilisierungs- und Abstimmungsprozesse sind nationale Behörden wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie regionale und überregionale Verbände (Industrie- und Handelskammern, Arbeitgeberverbände etc.) eingebunden. Dadurch kann dauerhaft ein Momentum zur Verbesserung der IT-Sicherheit und damit zur Stärkung der deutschen Wirtschaft im internationalen Wettbewerb erreicht werden.

Der Reifegrad der untersuchten IT-Sicherheitsprozesse ist ein Maß für den aktuellen Stand der Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität. Durch die Messung der Qualität der IT-Sicherheitsmanagementprozesse kann eine nachvollziehbare und transparente Bewertung des erreichten IT-Sicherheitsniveaus in den Unternehmen erfolgen.

Die Durchführung der Untersuchung und die Auswertung der Daten durch IT-Sicherheitsexperten in Verbindung mit der individuellen und transparenten Rückmeldung an die Unternehmen führen zu einer qualitätsgesicherten Datengrundlage. Sie erlaubt eine über bislang verfügbare Studien hinausgehende Darstellung der aktuellen Situation in Bezug auf IT-Sicherheit bei KMU in Deutschland.

2.3 Fokus

Die Studie ist auf die Erhebung und Bewertung des IT-Sicherheitsniveaus kritischer Geschäftsprozesse und IT-Infrastrukturen fokussiert. Hierzu wurden Interviews mit Vertretern von 30 Unternehmen durchgeführt, deren Ergebnisse die Grundlage dieser Studie bilden. Eine weitergehende Betrachtung von Dokumenten, Räumlichkeiten, Infrastrukturen oder Umsetzung von Maßnahmen ist nicht erfolgt. Die Anforderungen und Aspekte des Datenschutzes in den KMU waren ebenfalls kein Bestandteil der Interviews und werden somit im Rahmen dieser Studie nicht betrachtet.

Des Weiteren fließen keine Unternehmensspezifika der teilnehmenden Unternehmen in die Studie ein. Es werden ausschließlich anonymisierte Ergebnisse veröffentlicht.

Der Teilnehmerkreis der KMU umfasst die Branchen produzierendes Gewerbe, Handel und Dienstleistungen. In Unternehmen mit mehreren Standorten lag der Schwerpunkt auf der Betrachtung des jeweiligen Hauptstandortes. Weitere Standorte wurden vor allem in Bezug auf die Anbindung an den Hauptstandort betrachtet.

Die erhobenen Daten sind für die teilnehmenden Unternehmen als Planungshilfe zur systematischen Verbesserung ihres individuellen Sicherheitsniveaus anzusehen.

2.4 Aufbau des Dokuments

Das vorliegende Dokument beinhaltet die Ergebnisse der Studie zum Stand der IT-Sicherheit in kleinen und mittleren Unternehmen in Deutschland und ist in die folgenden Kapitel gegliedert:

Kapitel 3 des Dokuments detailliert die Vorgehensweise zum Aufbau und Durchführung der Studie sowie die zur Erfassung und Auswertung der Daten verwendeten Methoden. Des Weiteren werden die allgemeinen Informationen zu den teilnehmenden Unternehmen beschrieben.

In Kapitel 4 erfolgt die detaillierte Auswertung der in den Interviews erhobenen Daten sowie die Benennung der Handlungsempfehlungen. Dabei werden sowohl die positiven als auch die negativen IT-Sicherheitseigenschaften jedes Teilgebiets anhand von Grafiken illustriert, die Ergebnisse interpretiert und Handlungsempfehlungen genannt. Die Ergebnisse und Handlungsempfehlungen aller Teilgebiete werden in einer zusammenfassenden Darstellung, aufgezeigt.

Das Kapitel 5 greift die im Kapitel 2 definierten Ziele auf und stellt diese im Zusammenhang mit den Ergebnissen dar. Daraus folgenden werden im Ausblick Möglichkeiten zur Anhebung des IT-Sicherheitsniveaus genannt.

Kapitel 6 stellt ein erweitertes Stichwort- und Informationsverzeichnis zur Verfügung. Dieses adressiert auch die aktuellen IT-Sicherheitsthemen der teilnehmenden Unternehmen.

3 Methodik

Die zugrunde liegende Methodik der Studie orientiert sich an etablierten IT-Sicherheits-Standards. Damit wird sichergestellt, dass die Ergebnisse im Nachgang auch als Planungshilfe zur Erhöhung des IT-Sicherheitsniveaus in den KMU genutzt werden können.

Die konkreten Fragen sind abgeleitet von Fragestellungen des BSI zum Stand der IT-Sicherheit. Sie berücksichtigen das produzierende Gewerbe, den Handel und die Dienstleistungsbranche. Die Vorgehensweise ist auch geeignet, Unternehmen mit unterschiedlichen Belegschaftsgrößen und Umsatzzahlen zu vergleichen.

In den nachfolgenden Kapiteln werden der inhaltliche Aufbau der Studie, die Methodik zur Erhebung und Auswertung der Daten und allgemeine Informationen zu den teilnehmenden Unternehmen dargestellt.

3.1 Inhaltlicher Aufbau der Studie

Ausgehend von den initialen Fragestellungen des BSI zum Stand der IT-Sicherheit in KMU sowie den in Abschnitt 2.1 definierten Zielen wurden die für die Studie wesentlichen Themenbereiche identifiziert. Zur Statusermittlung in den KMU wurde vom BSI unter anderem die Abhängigkeit der Unternehmen von einer funktionierenden IT wie auch das Bewusstsein in Bezug auf den Wert der Mitarbeiter wie auch der Daten und Informationen hinterfragt. Des Weiteren waren der Umsetzungsgrad der Schutzmaßnahmen zur Absicherung der geschäftskritischen Daten vor internen und externen Manipulationen wie auch die Prozesse zur Aktualisierung des Wissens bzgl. neuer Risikosituationen und Angriffstechniken Gegenstand dieser Fragestellungen. Auch der Stand der Präventionsmaßnahmen zur Handhabung von Notfällen und zur Gewährleistung eines schnellen Wiederanlaufs waren von Interesse. Insbesondere die Frage: „Wie kann das IT-Sicherheitsniveau erhöht werden und wer kann dabei helfen?“ war von Bedeutung.

Diese Fragestellungen wurden detailliert und in Anlehnung an den IT-Grundschutz [BSI 2008] als etabliertem Standard thematisch gruppiert.

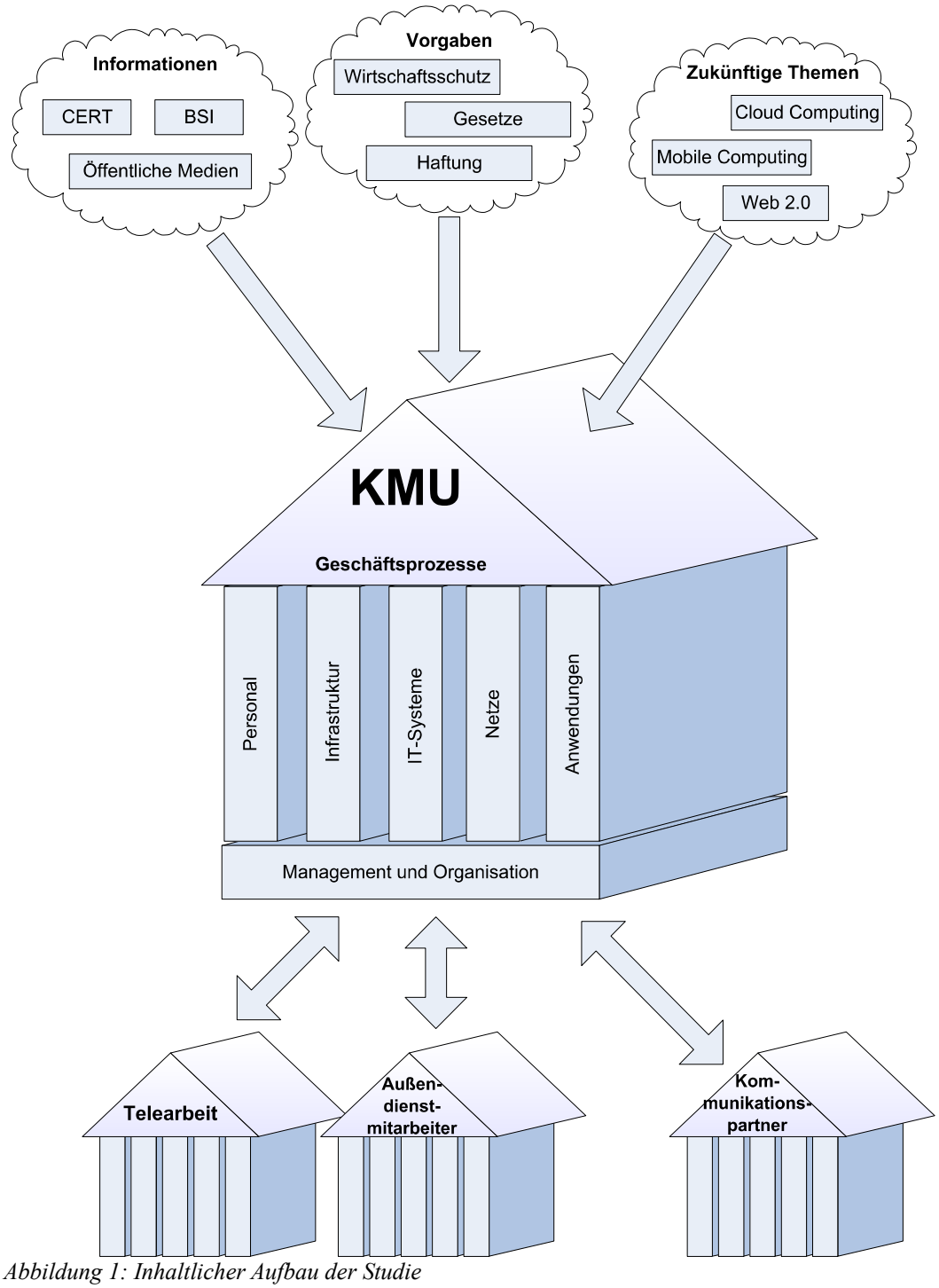


Abbildung 1: Inhaltlicher Aufbau der Studie

Die Abbildung 1 zeigt eine Übersicht der in der Studie betrachteten Themen. Die Themen lehnen sich hierbei an die Vorgehensweise nach IT-Grundschutz sowie an die Struktur der IT-Grundschutz-Kataloge an.

Zur Ermittlung der von den Unternehmen umgesetzten organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsmaßnahmen werden gemäß Abbildung 1 die folgenden Bereiche betrachtet:

- **Personal:** Der Bereich Personal umfasst die Aspekte rund um die Einbindung der Mitarbeiter in die IT-Sicherheitsprozesse sowie die Information und Sensibilisierung der jeweiligen Personen über umgesetzte IT-Sicherheitsmaßnahmen. Hierzu zählen zum Beispiel die Einarbeitung von Mitarbeitern und durchgeführte Schulungsmaßnahmen.
- **Infrastruktur:** Die baulich-technischen Gegebenheiten am Hauptstandort der Unternehmen werden im Rahmen der Infrastruktur betrachtet. Als Beispiele sind die Bereiche Zugangs- und Zutrittskontrolle, Gebäudesicherheit und die Absicherung technischer Infrastrukturen wie Serverräume zu nennen.
- **IT-Systeme:** Dies umfasst die Sicherheitsmechanismen in Bezug auf einzelne IT-Systeme, wie zum Beispiel Server und Laptops.
- **Netze:** In diesem Bereich wird die Vernetzung der IT-Systeme unter Sicherheitsaspekten betrachtet. Als Beispiel sind virtuelle private Netze (VPN) sowie Netz- und Systemmanagement zu nennen.
- **Anwendungen:** Im Rahmen der Studie wird die Kommunikationsanwendung E-Mail betrachtet.

Der Themenkomplex **Management und Organisation** nimmt eine besondere Position ein, da dieser übergreifend steuernd und regulierend auf alle anderen Themenfelder einwirkt und ausschlaggebend für die Qualität und den Umsetzungsgrad von IT-Sicherheitsmaßnahmen sowie den Reifegrad der IT-Sicherheitsprozesse ist. Zu betrachten sind dabei insbesondere die Konzeption, Dokumentation sowie die Prozesssteuerung in den Bereichen:

- Managementsystem für Informationssicherheit (ISMS)
- Sensibilisierung
- Schulungskonzept
- IT-Sicherheitskonzept
- Wissensmanagement
- Datensicherung
- Notfallkonzept

Eine gute IT-Organisation verbunden mit der Umsetzung personeller, infrastruktureller und technischer Sicherheitsmaßnahmen ist ein wesentlicher Faktor für den sicheren Betrieb der kritischen IT-gestützten Geschäftsprozesse.

Des Weiteren werden in der Studie die im Rahmen der **Geschäftsprozesse** genutzten Verbindungen mit unterschiedlichsten Kommunikationspartnern (Kunden, Partner, Dienstleister, Lieferanten, ...) betrachtet, welche durch ihre technische wie organisatorische Ausprägung Einfluss auf die Umsetzung von IT-Sicherheitsmaßnahmen z.B. im Bereich der E-Mail Kommunikation haben können.

Insbesondere die durch die eigenen Mitarbeiter dauerhaft oder anteilig außerhalb des Unternehmens genutzten Kommunikationsmöglichkeiten (Telearbeit, Außendienst, Geschäftsreise, ...) sind hier von Interesse. Durch mobiles Arbeiten und die zunehmende Nutzung von mobilen Endgeräten wie

Notebooks und Smartphones im beruflichen Umfeld entstehen für KMU neue Herausforderungen in Bezug auf die Umsetzung von IT-Sicherheitsmaßnahmen.

Dies gilt auch für die Anbindung weiterer Unternehmensstandorte, insbesondere dann, wenn ein Unternehmen international tätig ist.

Um auf neue Bedrohungen angemessen reagieren zu können, bedarf es einer aktiven Nutzung von Warn- und Informationsdiensten durch die Unternehmen. Hier bietet sich die Nutzung verschiedener öffentlicher (BSI, Online-Medien, Hersteller, ...) wie nicht-öffentlicher Informationsquellen (Verbände, Dienstleister, ...) zwecks Prävention an. Auch die im Rahmen des Wirtschaftsschutzes tätigen Behörden wie die Landesämter für Verfassungsschutz (LfV) sowie das Bundesamt für Verfassungsschutz (BfV) stellen Informationen bereit (siehe Kapitel 6).

Des Weiteren unterliegen die KMU der Anforderung, die im Unternehmen eingesetzten Informations- und Kommunikationstechnologien fortlaufend in Bezug auf neuartige und ggf. richtungsweisende IT-Themen zu bewerten und bei Bedarf zu adaptieren. Beispielhaft seien hier Cloud-Computing, service-orientierte-Architekturen (SOA) aber auch Web 2.0 genannt.

Im Rahmen dieser Studie wird betrachtet, in wieweit die Vorgaben verwendet, die verfügbaren Informationen aufgenommen sowie die zukünftigen Themen berücksichtigt werden.

3.2 Durchführung der Studie

Die Durchführung der Studie durch IT-Sicherheitsexperten wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) inhaltlich und bei den Vor-Ort-Terminen in den Unternehmen begleitet.

Im Unterschied zu bisher verfügbaren Studien auf diesem Themengebiet stellt die Erhebung der Daten wie auch die Auswertung durch IT-Sicherheitsexperten eine über den reinen Interviewbogen hinausgehende Erfassung und Detaillierung des aktuellen Standes der IT-Sicherheit bei den teilnehmenden Unternehmen sicher.

Insgesamt wurden in jedem Unternehmen zwei Workshops durchgeführt. Der erste Termin diente zur Erhebung des Sachstandes. Präsentation und Diskussion der individuellen Ergebnisse erfolgten im zweiten Workshop.

3.2.1 Informationserfassung

Zur Erhebung der Daten wurden im Rahmen eines eintägigen Workshops Interviews mit der Geschäftsführung sowie den IT-Verantwortlichen der Unternehmen geführt.

Die Befragungen erfolgten, sofern möglich getrennt, um unerwünschte Einflüsse auf die Antworten aller Beteiligten zu vermeiden. Dabei kamen zwei aufeinander abgestimmte Fragebögen zum Einsatz. So wurden der Unternehmensleitung eher allgemeine Fragen zum Stand der IT-Sicherheit im Unternehmen gestellt, während mit den IT-Verantwortlichen spezifische und technisch orientierte Fragen diskutiert wurden. Somit konnten gezielt die Einschätzungen der Unternehmensleitung in Bezug auf die Budget- und Ressourcensituation sowie die Gefahrenbereiche, das Risikomanagement und das IT-Sicherheitsmanagement erfasst werden. Aus der Befragung der IT-Leitung ergaben sich konkrete Ergebnisse zum Umfang der umgesetzten IT-Sicherheitsmaßnahmen sowie dem Reifegrad der IT-Sicherheitsprozesse.

Die in Kapitel 3.1 beschriebenen Themengebiete sowie die zur Ermittlung des Reifegrades der jeweiligen IT-Sicherheitsprozesse erforderlichen Fragen werden durch die an den IT-Grundschutz sowie an die Struktur der IT-Grundschutz-Kataloge angelehnten Interviewbögen vollständig abgedeckt. Diese wurden speziell für die vorliegende Studie entwickelt.

Die Interviewbögen basieren auf einer Mischung offener und geschlossener Fragen. Dabei standen unterschiedliche Antwortmöglichkeiten zur Auswahl, die bei verschiedenen Fragen Mehrfachnennung ermöglichten.

Die Leitung und Moderation der Interviews durch die IT-Sicherheitsexperten ermöglichte ein gezieltes und detailliertes Hinterfragen und damit die Erfassung ergänzender Informationen, die über die vorgegebenen Antwortmöglichkeiten hinausgingen. Weiterhin konnten so Missverständnisse vermieden werden. Dies steigert die Qualität der Antworten im Rahmen dieser Studie im Vergleich zu anderen Befragungen (bspw. Online-Befragungen).

Die Unternehmen hatten darüber hinaus die Möglichkeit, in den Interviews zusätzliche Fragen zu IT-Sicherheitsthemen an das BSI zu adressieren. Dies wurde von den Unternehmen intensiv genutzt. Die entsprechenden Informationen stehen im erweiterten Stichwort- und Informationsverzeichnis in Kapitel 6 zur Verfügung.

3.2.2 Unternehmensspezifische Rückmeldung

Ein zweiter Workshop zur Präsentation und Diskussion der individuellen Ergebnisse fand mit den Unternehmensvertretern – zumeist einschließlich der Geschäftsleitung – nach Abschluss der Auswertung statt. Während dieses Termins wurde der aus den Interviews ermittelte Umsetzungsgrad in Bezug auf die organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsmaßnahmen den Unternehmensvertretern ausführlich vorgestellt.

Auf diese Weise bot sich die qualitätsgesicherte Möglichkeit, eventuelle Fehlinterpretationen bei der Datenaufnahme zu identifizieren und in der Studie zu korrigieren. Ergänzend zur transparenten Darstellung der unternehmensspezifischen Ergebnisse wurden in der Diskussion mögliche Handlungsempfehlungen zur Anhebung des IT-Sicherheitsniveaus in Bezug auf ihre praktische Umsetzungsfähigkeit erörtert. Die kumulierten Ergebnisse dieser Diskussion der Handlungsempfehlungen finden sich ebenfalls in Kapitel 4 wieder und sollen zur Sensibilisierung aller deutschen KMU beitragen. Durch die Methodik der direkten Ergebnisbesprechung konnte zudem die Reaktion der im Unternehmen verantwortlichen Personen in Bezug auf die als kritisch identifizierten Bereiche beobachtet werden. Erhöhte Wachsamkeit und Handlungsbereitschaft waren als positiver Nebeneffekt deutlich erkennbar.

3.3 Auswertung

Die im Rahmen der Interviews erhobenen Informationen wurden elektronisch erfasst und ausgewertet. Dies umfasste ebenfalls die Bewertung der Reifegrade der IT-Sicherheitsprozesse.

Die Auswertung der Daten erfolgte hierbei in zwei Schritten. In einem ersten Schritt wurden die individuellen Ergebnisse der Unternehmen auf Basis der unternehmensspezifischen Daten ermittelt. Zusätzlich wurden die durch die IT-Sicherheitsexperten ermittelten ergänzenden Informationen berücksichtigt. Auf Basis dieser Ergebnisse ist im Anschluss das Gesamtergebnis zusammengefasst worden. Dieses enthält die Daten aller Unternehmen in anonymisierter Form. Die detaillierte Vorgehensweise für die Ermittlung des Gesamtergebnisses wird in dem nachfolgenden Unterkapitel 3.3.1 beschrieben.

Der Reifegrad eines IT-Sicherheitsprozesses wurde anhand von Qualitätskriterien bewertet. Diese werden im Kapitel 3.3.2 beschrieben.

3.3.1 Übergreifende Auswertung

Für die übergreifende Auswertung wurden die Inhalte der Studie (vgl. Kapitel 3.1) thematisch zusammengefasst. Die Struktur und damit die Themenkomplexe ergaben sich hierbei aus den initialen Fragestellungen des BSI (vgl. Kapitel 3.1), den Bausteinen der IT-Grundschutz-Kataloge sowie der Betrachtung der IT-Sicherheitsprozesse, insbesondere deren Reifegrad. Die Zuordnung der Inhalte der Studie, repräsentiert durch die Fragen und Antworten aus den Interviewbögen, zu den Themenkomplexen wurde in der Auswertematrix dokumentiert und anschließend im elektronischen Auswertungsformular abgebildet. Die umfassende Abdeckung der in Kapitel 3.1 beschriebenen Inhalte der Studie kann somit nachvollzogen werden.

Für die Auswertung ergeben sich sechzehn Themenkomplexe, die in der nachfolgenden Abbildung 2 eingefärbt dargestellt sind.

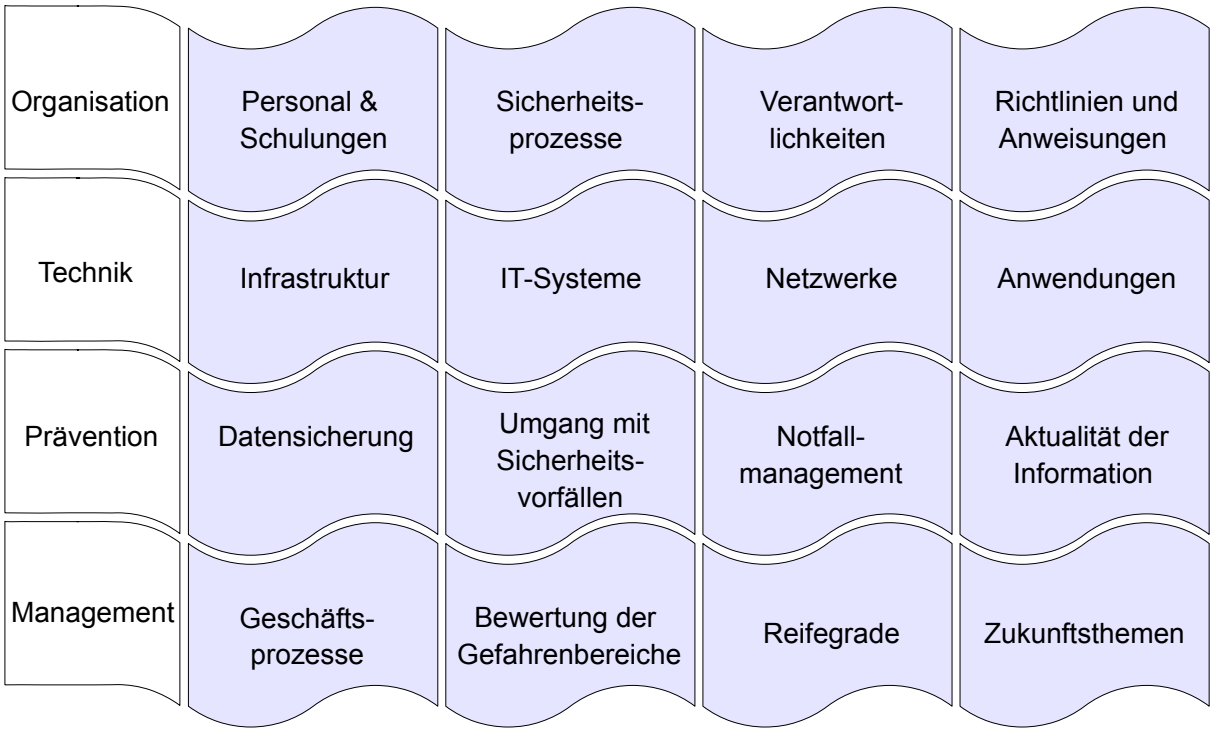


Abbildung 2: Themen der Auswertematrix

Die Themenkomplexe sind dabei zeilenweise zusammengefasst und links neben den Themen in der Farbe weiß dargestellt. Diese sind wie folgt gegliedert:

- **Organisation:** Neben dem Bereich Personal werden die übergeordneten Management- und Organisationsthemen der Schulungs- und Sensibilisierungsmaßnahmen, der Verantwortlichkeiten sowie der Richtlinien und Anweisungen betrachtet. In dem Abschnitt Sicherheitsprozesse werden die Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit als Querschnitt über die diesbezüglichen Antworten bewertet.
- **Technik:** In Anlehnung an die Bausteine B2 bis B5 der IT-Grundschutz-Kataloge werden die Antworten zu den baulich-technischen Gegebenheiten (Infrastruktur) am Hauptstandort des Unternehmens, den IT-Systemen, der Vernetzung der IT-Systeme sowie der Kommunikationsanwendung E-Mail ausgewertet.
- **Prävention:** Bewertet werden die den übergeordneten Management- und Organisationsthemen zuzuordnenden, präventiven Sicherheitsmaßnahmen zum Datenerhalt durch Datensicherung, das Sicherheitsvorfall- und Notfallmanagement zur Erkennung und Umgang mit diesen Ausnahmesituationen sowie die Aktualität der Informationen in Bezug auf gegenwärtige und zukünftige Bedrohungsszenarien.
- **Management:** Die Aspekte der Identifikation der kritischen IT-Geschäftsprozesse sowie deren Risikobewertung in Verbindung mit der Bewertung der für die Unternehmen relevanten Gefahrenbereiche als Aufgaben für das Management werden ausgewertet. Zusätzlich erfolgt eine Betrachtung und Diskussion der Reifegrade der IT-Sicherheitsprozesse. Abschließend werden die Einschätzungen in Bezug auf neuartige, ggf. richtungsweisende IT-Themen bewertet.

Die Auswertematrix ordnet den Themengebieten die einzelnen Fragen und Antworten zu, so dass eine allgemeine Aussage über diese Themen in Bezug auf die betrachteten Unternehmen entsteht. Diese Aufteilung lag ebenfalls den unternehmensspezifischen Rückmeldungen (siehe Kapitel 3.2.2) zugrunde.

In die Bewertung gehen die Antworten ein, welche die Umsetzung von Sicherheitsmaßnahmen unmittelbar adressierten. Hierbei gab es folgende Antwortmöglichkeiten:

- **Maßnahme umgesetzt:** Die abgefragte Sicherheitsmaßnahme ist im Unternehmen umgesetzt.
- **Maßnahme teilweise umgesetzt oder in Planung:** Die Sicherheitsmaßnahme ist in Teilen umgesetzt oder befindet sich in konkreter Planung, die zeitnah umgesetzt werden. Für die vollständige Umsetzung müssen noch weitere Maßnahmen ergriffen werden.
- **Maßnahme nicht umgesetzt:** Die Sicherheitsmaßnahme ist nicht umgesetzt und eine Umsetzung ist in der näheren Zukunft nicht geplant.
- **Nicht bekannt oder nicht beantwortet:** Die Sicherheitsmaßnahme bzw. die Umsetzung der Sicherheitsmaßnahme ist den befragten Personen unbekannt. Dies kann durch mangelndes Wissen oder fehlende Verantwortung für den genannten Unternehmensbereich bedingt sein. Somit können keine Informationen erhoben werden.
- **Nicht zutreffend:** Die Sicherheitsmaßnahme muss im Unternehmen aufgrund der örtlichen Begebenheiten nicht umgesetzt werden. Dies trifft z.B. bei Fragen in Bezug auf die Beteiligung des IT-Sicherheitsbeauftragten in Unternehmensentscheidungen zu, wenn kein IT-Sicherheitsbeauftragter benannt wurde.

Die Antworten der Unternehmen gehen gleich-gewichtet und kumuliert in die Bewertung ein. Pro Themenkomplex werden mehrere Antworten zu einer Gesamtaussage aggregiert.

Die Sicherheitsmaßnahmen bezüglich der Aktualität von Dokumenten bzw. der IT-Sicherheitsprozesse wurden als umgesetzt angesehen, wenn die letzte Prüfung nicht länger als drei Jahre zurücklag. Im Falle, dass aktuell eine Prüfung erfolgte oder geplant war, wurde dies als teilweise umgesetzt gewertet. Antworten mit anderen Zeitangaben wurden als nicht umgesetzt bewertet, da hier von keiner Umsetzung des Sicherheitsprozesses ausgegangen werden kann.

3.3.2 Bewertung des Fortschritts

IT-Sicherheitsmanagement muss sich auf zyklische Prozesse stützen, um effektiv zu sein. Während der IT-Grundschutz als Sicherheitsmanagementsystem konkrete technische Maßnahmen aufzeigt, bietet sich für die Messung der Qualität von Sicherheitsprozessen die Verwendung von Prozess-Reifegrad-Modellen an.

Um einzuschätzen, zu welchem Grad IT-Sicherheit in einem Unternehmen umgesetzt ist und welchen Reifegrad die Prozesse erreicht haben, wird in dieser Studie das Process-Maturity-Model (PMM) als etablierter und in der *Information Technology Infrastructure Library* (ITIL) benutzter Standard verwendet. Die im PMM verwendeten Kategorien sind vergleichbar mit denen der *Capability Maturity Model Integration* (CMMI).

Um die bestehenden Prozesse analysieren und bewerten zu können, werden diese abhängig vom Implementierungsgrad sogenannten Reifegradstufen zugeordnet. Diese Stufen sind in Tabelle 1 detailliert beschrieben.

Ebene	*Beschreibung*	*Messwerte*
0: Unvollständig (Incomplete)	Es gibt keinen Prozess oder eine Aktivitätenfolge. Ein (Prozess-)Ergebnis ist nicht definiert.	Kein Prozess definiert. Kein Ergebnis definiert.
1: Ausgangszustand (Initial)	Chaotisch, eher Projekt als Prozess; Input und Ergebnis sind nicht definiert, Abläufe wiederholen sich nur selten. Einzelne Schritte eines Prozesses werden ausgeführt. Die Schritte sind nicht festgelegt und werden ungeplant variiert. In der Summe entstehen gewünschte Ergebnisse, ohne eine Wiederholbarkeit des Ablaufes und des Ergebnisses.	Prozessschritte nicht festgelegt. Input und Ergebnis nicht definiert. Wiederholbarkeit nicht gegeben.
2: Reproduzierbar (Managed)	Auf Ebene der kleinsten Organisationseinheiten ist der Prozess organisiert; Input und Ergebnis sind definiert. Es liegen definierte Prozessfolgen vor, die angewendet werden. Die Prozesse sind nicht aufeinander abgestimmt. Das Bewusstsein für einen Prozess als Arbeitsgrundlage ist nicht durchgehend präsent. Zukünftige Veränderungen sind das Ergebnis von Versuch und Irrtum.	Prozess ist organisiert. Prozesse sind jedoch nicht abgestimmt. Zukünftige Veränderungen auf Basis von Versuch und Irrtum.
3: Standardisiert (Established)	Arbeitsschritte und Teilprozesse laufen wiederholbar ab. Der Prozess ist dokumentiert. Die Prozesse werden auf der Basis geplanter, strukturierter, feststehender und dokumentierter Beschreibungen gelebt. Die Prozesse sind aufeinander abgestimmt. Rollen und Verantwortlichkeiten sind klar geregelt. Es ist die Struktur vorhanden, in die Messkriterien zur Ermittlung des Erfolges eingefügt werden können.	Prozess ist dokumentiert. Rollen und Verantwortlichkeiten sind klar geregelt.
4: Vorhersehbar (Predictable)	Es existieren für Arbeitsschritte und Teilprozesse Qualitätskriterien. Für die eingeführten Prozesse gibt es Qualitätsziele, die geplant gemessen werden. Auf dieser Basis sind Verbesserungen des Prozesses möglich. Das Ergebnis (Output) des Prozesses ist vorhersehbar und hat eine gute Qualität.	Qualitätsziele sind definiert und werden gemessen. Verbesserungen gezielt möglich.
5: Optimiert (Optimised)	Der Prozess wird unter Auswertung der Qualitätskriterien beständig optimiert. Es findet eine geplante, regelmäßige Verbesserung der Prozesse unter Beachtung der sich weiterentwickelnden Unternehmensziele statt. Schwächen und Stärken der Prozesse sind transparent. Es besteht eine hohe Flexibilität, da die Prozesse optimierbar sind.	Prozesse werden kontinuierlich entsprechend den Messwerten an die Qualitätsziele angepasst. Qualitätsziele werden fortlaufend aktualisiert.

Tabelle 1: Bewertung von IT-Sicherheit in Form von Reifegraden nach PMM

Der Umfang und die Qualität der IT-Sicherheitsmanagementprozesse wurden in den Interviews mit den IT-Verantwortlichen ermittelt und gibt somit die IT-interne Sichtweise wieder. Die Bewertung dieser Prozesse erfolgte anhand der in Tabelle 1 aufgeführten Kriterien.

3.4 Allgemeine Daten der teilnehmenden Unternehmen

Das Institut für Mittelstandsforschung (IfM) in Bonn hat durch Auswertung der vom Statistischen Bundesamt Deutschland bereitgestellten Daten festgestellt, dass 99,6 Prozent der Unternehmen in Deutschland zu den kleinen und mittleren Unternehmen gehören [Stat 2010]. Dies sind rund 3,6 Millionen Unternehmen mit rund 59,9 Prozent der Beschäftigten in Deutschland. Die nachfolgende Abbildung stellt die Verhältnisse grafisch dar.

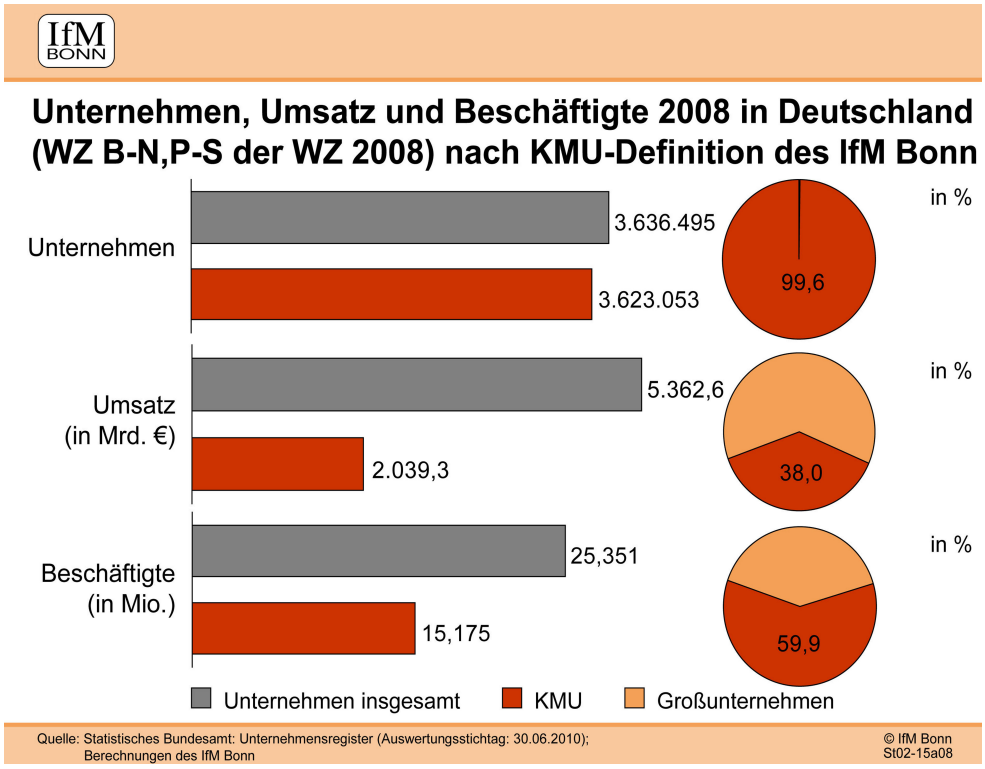


Abbildung 3: Auswertung zu KMU vom IfM

Hierbei definiert das IfM Unternehmen mit bis zu 499 Mitarbeitern und einem Jahresumsatz von bis zu 50 Millionen Euro als kleine und mittlere Unternehmen.

Um eine breitere Aufstellung zu erhalten, wurden im Rahmen der Studie kleine und mittlere Unternehmen in dem nach Schierenbeck [PBS 2005] größeren Rahmen gewählt (vgl. Tabelle 2). Dies berücksichtigt auch Unternehmen, die bezogen auf den Hauptstandort nach IfM als KMU zu betrachten wären, jedoch in der Gesamtmitarbeiterzahl bzw. dem Gesamtumsatz der Unternehmensgruppe über dieser Grenze liegen.

Größenklasse	*Beschäftigungszahlen*
Kleinbetrieb	bis 19
Mittelbetrieb	20 bis 5000
Großbetrieb	über 5000

Tabelle 2: Unternehmensgrößen nach Schierenbeck

Das BSI hat 30 kleine und mittlere Unternehmen gemäß der Definition für KMU nach Schierenbeck aus den Branchen produzierendes Gewerbe, Handel und Dienstleistung für die vorliegende Studie befragt. Die Branchen wurden gewählt, da sie zusammengenommen einen Anteil von ca. 66 Prozent des Bruttoinlandsprodukts der Bundesrepublik Deutschland [BIP2010], sowie die aus Sicht der Beschäftigungszahlen bedeutendsten Wirtschaftssektoren [ArM_2010], den sekundären wie tertiären Sektor, repräsentieren.

Alle an der Teilnahme an der Studie interessierten Unternehmen konnten berücksichtigt werden. Sie teilen sich wie in den nachfolgenden Diagrammen dargestellt nach Branchen, Mitarbeiterzahl und Umsatz im Geschäftsjahr 2009 auf.

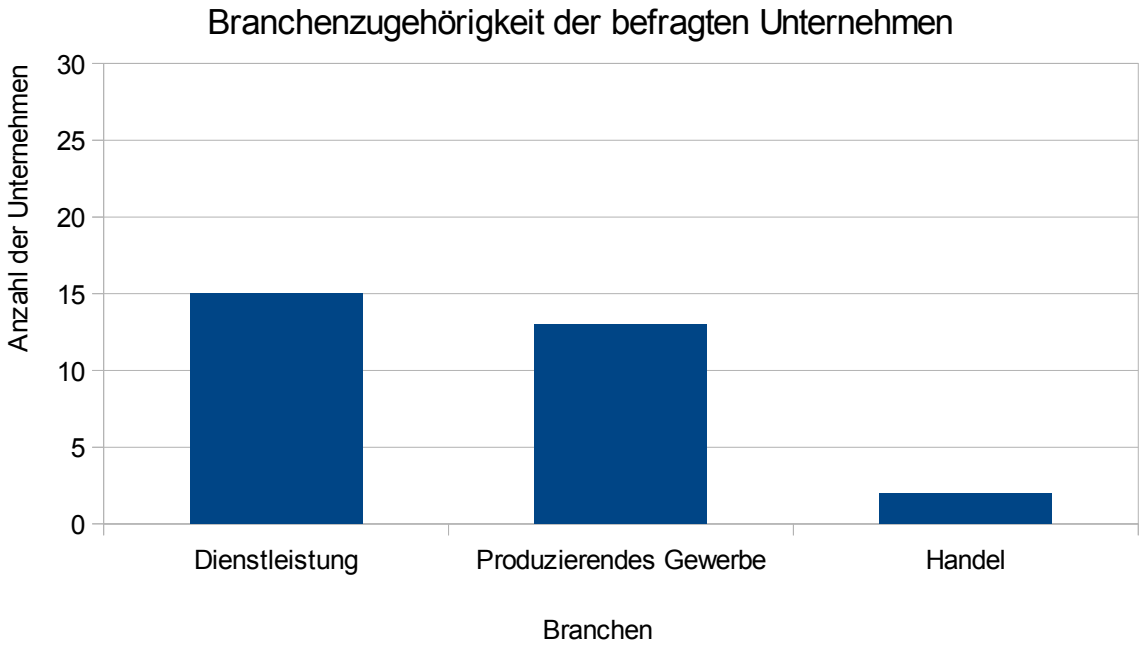


Abbildung 4: Branchenzugehörigkeit der befragten Unternehmen

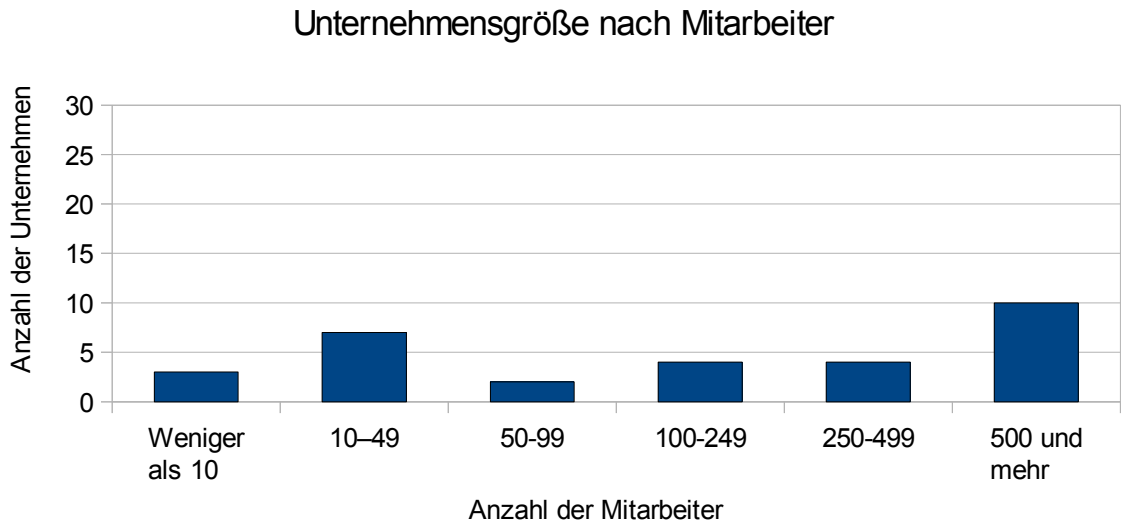


Abbildung 5: Unternehmensgröße nach Mitarbeitern

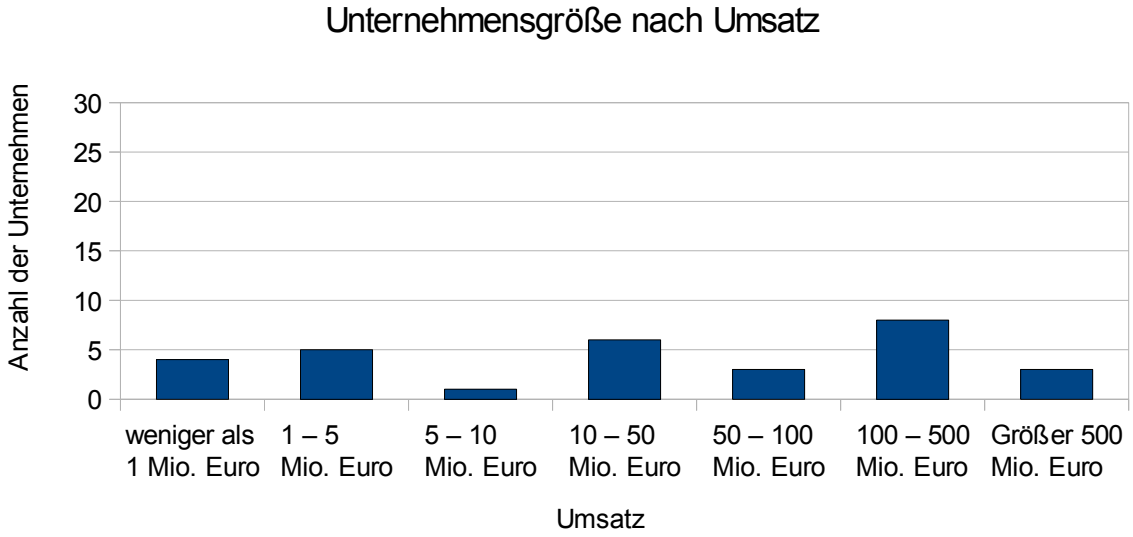


Abbildung 6: Unternehmensgröße nach Umsatz

Insgesamt konnte im Rahmen der Studie ein breites Spektrum, bezogen auf die Unternehmensgröße nach Anzahl der Mitarbeiter bzw. nach Umsatz, betrachtet werden. Neben drei Kleinstbetrieben (weniger als zehn Beschäftigte) wurden auch Unternehmen betrachtet, die weltweit mehr als 500 Mitarbeiter beschäftigen.

Das BSI hatte bundesweit zur Teilnahme an der Studie über ihre Webseite sowie andere Kommunikationswege (Printmedien, etc.) aufgerufen. Die nachfolgende Abbildung zeigt die Hauptstandorte der teilnehmenden Unternehmen.

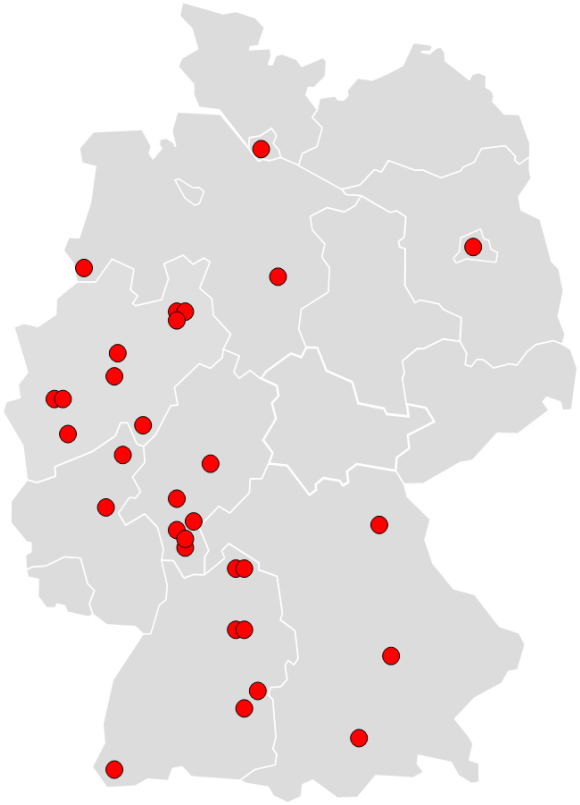


Abbildung 7: Hauptstandorte der teilnehmenden Unternehmen in Deutschland

4 Ergebnisse und Handlungsempfehlungen

Im Folgenden sind die Ergebnisse der Studie zum Stand der IT-Sicherheit in kleinen und mittleren Unternehmen beschrieben. Das Kapitel untergliedert sich in drei Themenbereiche. Zum einen wird in Kapitel 4.1 die betriebsinterne Organisation und die Einschätzung der Unternehmen zum Thema IT-Sicherheit dargestellt. Anschließend erfolgen eine übergreifende Bewertung der Ergebnisse und Handlungsempfehlungen (Kapitel 4.2) und eine detaillierte Darstellung der in Kapitel 3.3.1 definierten Themen. Die Ergebnisse der einzelnen Themengebiete werden in den Unterkapiteln (Kapitel 4.3 bis Kapitel 4.18) beschrieben und die sich daraus ergebenden Handlungsempfehlungen aufgezeigt.

4.1 Betriebsinterne Organisation und Bedeutung der IT-Sicherheit

Mit einer guten betriebsinternen Organisation lässt sich IT-Sicherheit umsetzen. Durch die Benennung entsprechender Funktionsträger – die für spezielle Themenbereiche der IT-Sicherheit verantwortlich sind – können Aufgaben verteilt und die korrekte Umsetzung gewährleistet werden. Eine solche Benennung muss immer durch die Management-Ebene eines Unternehmens erfolgen. Dazu gehört jedoch auch, dass das Management in der Lage ist, den Stand der IT-Sicherheit einzuschätzen.

Diese beiden Aspekte wurden im Rahmen der Studie untersucht. Die nachfolgenden Unterkapitel stellen die Ergebnisse dar.

4.1.1 Funktionsträger im Unternehmen

In Bezug auf die betriebsinterne Organisation und Aufteilung von Funktionen wurde die Unternehmensleitung hinsichtlich der im Unternehmen etablierten Funktionsträger befragt.

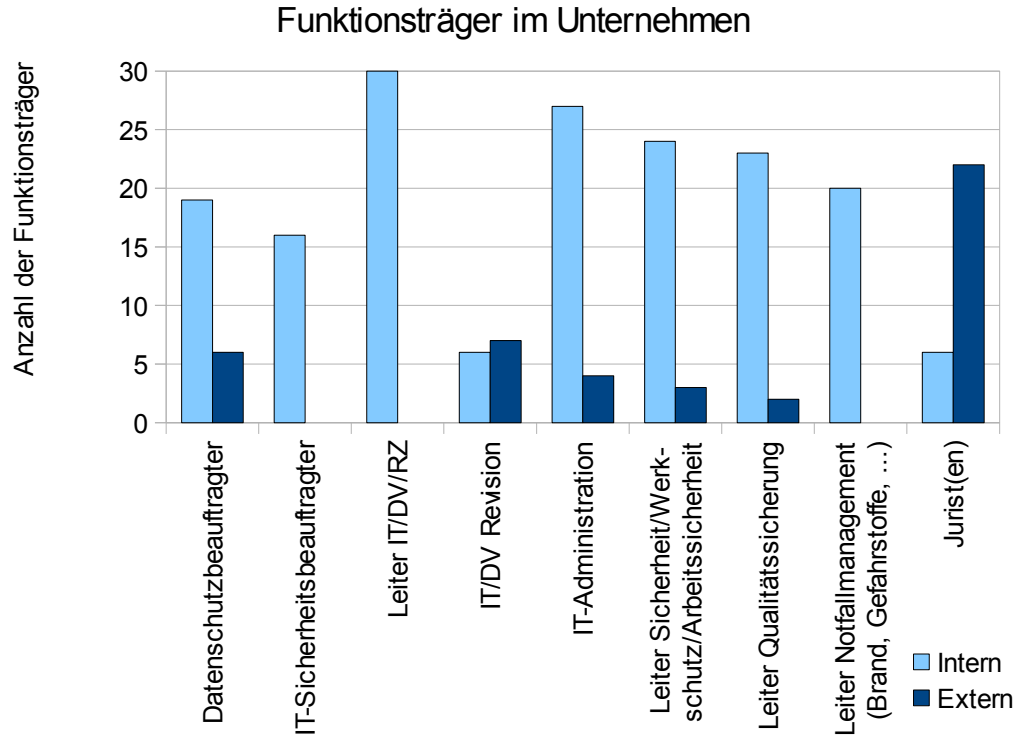


Abbildung 8: Funktionsträger im Unternehmen

Von den 30 befragten Unternehmen haben 25 einen Datenschutzbeauftragten bestellt. Von den fünf Unternehmen, die keinen Datenschutzbeauftragten bestellt haben, handelt es sich bei drei Betrieben um Kleinstunternehmen, welche nach dem Bundesdatenschutzgesetz (BDSG) zur Bestellung eines Beauftragten für den Datenschutz nicht verpflichtet sind [BDSG_4f].

Die zwei verbleibenden Unternehmen unterliegen nach den aus den Interviews vorliegenden Informationen der gesetzlichen Verpflichtung zur Bestellung eines Datenschutzbeauftragten. Dieser wurde nach Eigenauskunft der Unternehmen bisher weder intern noch extern bestellt, so dass hier dringender Handlungsbedarf gegeben ist.

Eine interne IT-Leitungsfunktion bzw. einen IT-Verantwortlichen haben alle Unternehmen benannt. Des Weiteren verfügen 90 Prozent der Unternehmen über eigene IT-Administratoren. Ein Unternehmen hat die IT-Administration vollständig an einen Dienstleister outgesourct. Etwa 15 Prozent der Unternehmen gaben an, dass die internen IT-Administratoren durch externe Kräfte maßgeblich unterstützt werden.

Einen IT-Sicherheitsbeauftragten haben nur knapp über 50 Prozent der befragten Unternehmen benannt. In vielen Fällen wird diese Funktion durch den IT-Verantwortlichen übernommen. Die Mehrheit der IT-Sicherheitsbeauftragten der sechzehn Unternehmen gab weiterhin an, nicht ausreichend in Entscheidungsprozesse eingebunden zu sein und keine ausreichenden Ressourcen zur Umsetzung ihrer Aufgaben zur Verfügung zu haben. Dieses wird in Kapitel 4.5 weiter ausgeführt.

Weitere betriebliche Funktionsträger wie Leiter Sicherheit/Werkschutz/Arbeitssicherheit, Leiter Qualitätssicherung und Leiter Notfallmanagement sind in der Mehrzahl der Unternehmen etabliert.

Insgesamt 43 Prozent der Unternehmen verfügen über eine unternehmensinterne IT-Revision bzw. unterliegen der Revision durch die Unternehmensgruppe. Dies trifft auf alle Unternehmen aus dem Bereich des Handels, sowie auf knapp die Hälfte der Unternehmen aus dem produzierenden Gewerbe und auf ein Drittel der Dienstleister zu.

Unterstützung in juristischen Fragen erhält die Mehrheit der Unternehmen durch externe Kräfte.

4.1.2 Bedeutung der IT-Sicherheit in den Unternehmen

Im Rahmen der Interviewbögen wurden Fragen zur Bedeutung der IT-Sicherheit an die Unternehmen gerichtet. Hierbei wurde die heutige Bedeutung in der Abstufung von „sehr wichtig“, über „wichtig“ bis „nicht wichtig“ ermittelt, sowie eine Zukunftsprognose in den Stufen „Bedeutung steigt“, „Bedeutung unverändert“, „Bedeutung sinkt“ bis „nicht relevant“ abgefragt.

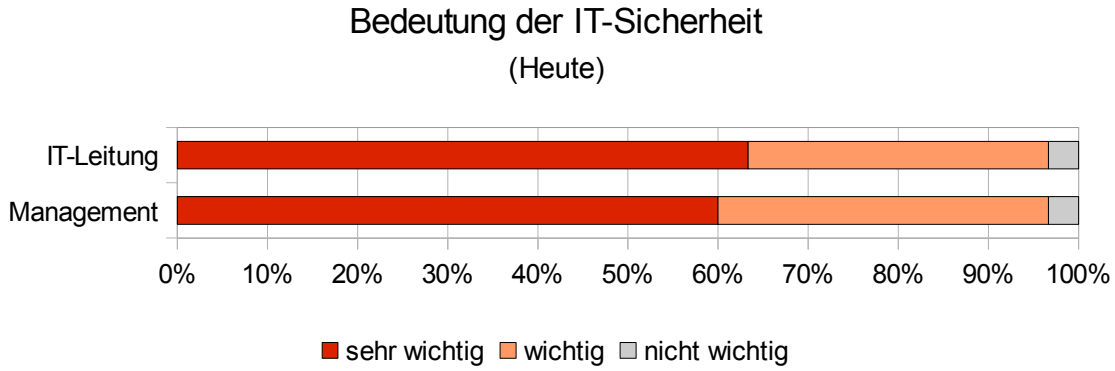


Abbildung 9: Heutige Bedeutung der IT-Sicherheit

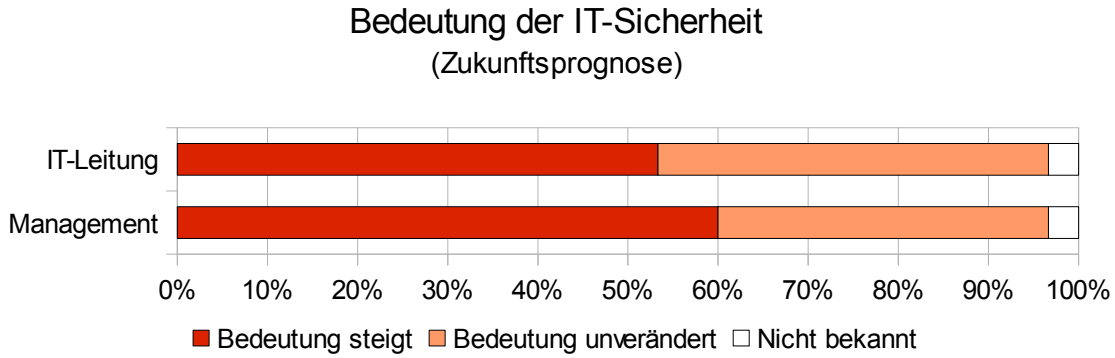


Abbildung 10: Zukünftige Bedeutung der IT-Sicherheit

IT-Sicherheit ist für die teilnehmenden Unternehmen sowohl aktuell als auch in Zukunft von sehr hoher Bedeutung. Mehr als die Hälfte der Befragten ist der Ansicht, dass die Bedeutung der IT-Sicherheit in Zukunft weiter steigen wird.

Die Aussagen und Prognosen der Unternehmensleitungen wie auch der IT-Verantwortlichen der Unternehmen stimmen hierin weitestgehend überein.

Die sehr hohe Bedeutung und das damit verbundene Bewusstsein für IT-Sicherheit in den teilnehmen Unternehmen lässt erwarten, dass die Unternehmen ein hohes IT-Sicherheitsniveau erreichen.

4.2 Übergreifende Bewertung

Die wesentlichen Ergebnisse sowie die abgeleiteten Handlungsempfehlungen wurden zusammengefasst und nachfolgend dargestellt. Im Anschluss erfolgt eine priorisierte Darstellung der Handlungsempfehlungen.

4.2.1 Ergebnisse

Im Rahmen dieser Studie wurde jeder der in Kapitel 3.3.1 definierten Themenkomplexe einzeln ausgewertet und der erreichte Umsetzungsgrad der abgefragten IT-Sicherheitsmaßnahmen bewertet. Die Bewertung erfolgt anhand einer Bewertungsskala, deren Aufbau in der nachfolgenden Tabelle dargestellt ist.

	40 Prozent oder weniger der Maßnahmen sind umgesetzt
	Mehr als 40 Prozent, aber weniger als 80 Prozent der Maßnahmen sind umgesetzt
	80 Prozent oder mehr der Maßnahmen sind umgesetzt
	Keine Bewertung

Tabelle 3: Bewertungsskala

Zur Darstellung der Übergangsbereiche zwischen zwei Bewertungsstufen wurden Farbverläufe basierend auf den Grundfarben verwendet. So wird das ermittelte Ergebnis im oberen Bereich des jeweiligen Themenkomplexes dargestellt und verläuft in den tendierenden Farbverlauf, wenn der ermittelte Wert um maximal fünf Prozent von den in Tabelle 3 definierten Schwellwerten abweicht.

Die Ergebnisse der einzelnen Themenkomplexe sind zusammenfassend in der nachfolgenden Abbildung 11 dargestellt.

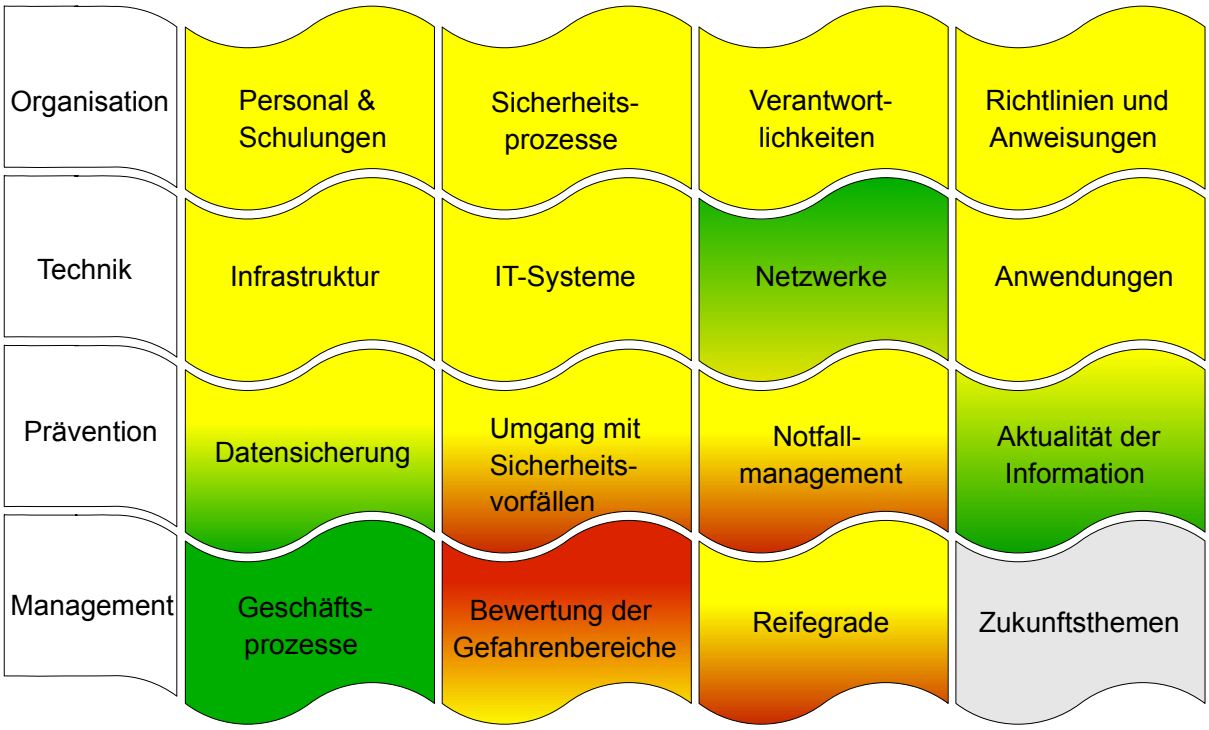


Abbildung 11: Gesamtergebnis der Studie

Die in Abbildung 11 dargestellten Ergebnisse zeigen insgesamt ein eher uneinheitliches Bild. Während im Durchschnitt 64 Prozent der abgefragten IT-Sicherheitsmaßnahmen in den Unternehmen umgesetzt sind, zeigen sich insbesondere bei dem Umgang mit Sicherheitsvorfällen, dem Notfallmanagement, der Bewertung der Gefahrenbereiche sowie den Reifegraden der Sicherheitsprozesse deutliche Abweichungen nach unten. Dagegen ist in den Bereichen Netzwerke, Datensicherung, Aktualität der Informationen und Geschäftsprozesse ein überdurchschnittlicher Umsetzungsgrad der IT-Sicherheitsmaßnahmen festzustellen.

Die Ergebnisse der einzelnen Themenkomplexe werden gemäß der thematischen Gruppierung aus Kapitel 3.3.1 wie folgt zusammengefasst:

Organisation

Im Bereich der Organisationsthemen wird insgesamt ein dem Durchschnittswert von 64 Prozent entsprechender Umsetzungsgrad der IT-Sicherheitsmaßnahmen erreicht.

Es wurde festgestellt, dass die Betreuung von Mitarbeitern in Bezug auf die IT-Sicherheitsthemen in den Unternehmen durchgehend umgesetzt ist. Insbesondere sind die Ansprechpartner zu IT-Sicherheitsfragen benannt und den Mitarbeitern bekannt. Auch werden die Mitarbeiter regelmäßig über Änderungen von Regelungen und deren spezifische Auswirkungen auf einen Prozess oder auf den einzelnen Mitarbeiter informiert. Im Gegensatz hierzu sind Schulungen in den KMU nur teilweise etabliert. Häufig handelt es sich hierbei um allgemeine Informationsveranstaltungen. Spezifische Schulungen zu IT-Sicherheitsmaßnahmen werden nur selten in den befragten Unternehmen durchgeführt.

Insgesamt bemühen sich die Unternehmen, dem Thema der Verantwortlichkeiten geeignet Rechnung zu tragen. In der Praxis zeigen sich in der Verteilung der Funktionen und Aufgaben

jedoch Spannungsfelder. Dementsprechend ist eine durchgehende personelle Funktionstrennung sowie eine eindeutige Aufgabenverteilung oft nicht möglich.

Gerade hier zeigt sich jedoch auch eine Stärke der kleinen und mittleren Unternehmen: Unabhängig von der Aufgabenzuordnung werden die anfallenden Aufgaben durch die jeweils verfügbaren Mitarbeiter erledigt. Im Interview zeigte sich, dass durch dieses Verhalten alle Aufgaben von allen Mitarbeitern durchgeführt werden. Auf Spezialisierungen wird wenig bis keine Rücksicht genommen. Die Verantwortlichkeiten müssen dadurch nicht immer fest an einen Funktionsträger gebunden sein. Vielmehr werden umzusetzende Maßnahmen von den jeweils freien Ressourcen durchgeführt. Umso wichtiger ist es, dass die Unternehmen die Mitarbeiter fortlaufend im Bereich der IT-Sicherheit schulen.

Die Notwendigkeit der Etablierung von Vertreterregelungen, gerade für die kritischen personellen Ressourcen, ist den Unternehmen bewusst. Vereinzelt plant das Management, in diesen Bereichen Unterstützung durch externe Dienstleister wahrzunehmen, sofern nicht ausreichend qualifiziertes Personal im eigenen Unternehmen verfügbar ist.

Obwohl die Unternehmensleitung die Verantwortung für die Informationssicherheit deutlich sichtbar übernommen hat, sind die Maßnahmen zur Regelung der Verantwortlichkeiten nur in der Hälfte der befragten Unternehmen umgesetzt. Nur jedes zweite Unternehmen hat beispielsweise einen IT-Sicherheitsverantwortlichen benannt. In vielen Fällen wird die IT-Leitung mit diesen Aufgaben zusätzlich belastet.

Weiterhin wurde festgestellt, dass definierte Richtlinien und Anweisungen bei der Mehrheit der befragten Unternehmen verfügbar sind. Es sind jedoch große Unterschiede in der Verfügbarkeit einzelner Richtlinien feststellbar. Des Weiteren wird eine regelmäßige Prüfung der vorhandenen Richtlinien auf ihre Eignung nur in etwas mehr als der Hälfte der Unternehmen durchgeführt. Eine Prüfung auf Einhaltung der Richtlinien erfolgt ebenfalls in rund der Hälfte der befragten Unternehmen.

Die für die Definition eines gemeinsamen Verständnisses und zur generellen Ausrichtung des Unternehmens in Bezug auf IT-Sicherheit erforderliche Definition und Bekanntgabe der Sicherheitsziele und -strategien an die Mitarbeiter erfolgt nicht durchgehend.

Technik

Im Bereich der Infrastruktur, IT-Systeme, Netze und Anwendungen wird insgesamt nur ein dem Durchschnittswert aller umgesetzter Sicherheitsmaßnahmen (64 Prozent) entsprechender Umsetzungsgrad der IT-Sicherheitsmaßnahmen erreicht, auch wenn sich der Themenkomplex der Netzwerke deutlich positiv hervorhebt.

Insgesamt ist festzustellen, dass den Bedrohungen durch äußere Angriffe auf die Infrastruktur durch Umsetzung einer Vielzahl von Schutzmaßnahmen Rechnung getragen wird. Es wird jedoch auch deutlich, dass die Schutzmaßnahmen abnehmen, je weiter eine Person in die Räume eines Unternehmens vordringen kann. Dies zeigt sich beispielsweise an den Besprechungs-, Veranstaltungs- und Schulungsräumen. Diese Räumlichkeiten zeichnen sich im Wesentlichen dadurch aus, dass sie von wechselnden Personen bzw. Personenkreisen genutzt werden. Besonders die Nutzung durch Externe erfordert hierbei eine dauerhafte Begleitung auf dem Weg in diese Räumlichkeiten und während des Aufenthaltes. Da es sich hierbei um eine organisatorische Schutzmaßnahme handelt, die aufgrund besonderer Anlässe unter Umständen nicht berücksichtigt wird, sollten zusätzliche technische Maßnahmen, wie zum Beispiel der Schutz der

Netzwerkanschlüsse, erfolgen. Diese werden aber von der Mehrheit der Unternehmen nicht umgesetzt. Gleiches gilt für die Absicherung der Netzwerkzugänge in den Büroräumen.

Im täglichen Einsatz sind besonders die mobilen Endgeräte dem Risiko der Entwendung ausgesetzt. In unberechtigter Hand und mit ausreichend Zeit ist davon auszugehen, dass die Daten gelesen oder manipuliert werden können. Dieses Szenario ist der Mehrheit der Unternehmen bewusst. Allerdings setzen nur die Hälfte der Unternehmen eine Festplattenverschlüsselung für Laptops ein. Die auf Wechselmedien wie z.B. USB-Sticks gespeicherten Daten werden nur von wenigen Unternehmen durch Verschlüsselung gesichert.

Des Weiteren werden zum Schutz vor unbefugtem Datenaustausch von mehr als der Hälfte der Betriebe technische oder organisatorische Schutzmaßnahmen zur Sicherung der Geräteschnittstellen ihrer mobilen Systeme eingesetzt. Als Hinderungsgrund für eine weitergehende Umsetzung wurde von den befragten Unternehmen angegeben, dass die Benutzbarkeit der Systeme höher bewertet wird als deren Sicherheit.

Die Klassifikation von Daten, um entsprechende Zugriffsregelungen oder auch Infrastrukturmaßnahmen wie den Aufbau isolierter Netzwerkbereiche ableiten zu können, erfolgt nur bei der Hälfte der Unternehmen. Des Weiteren wird in der Mehrzahl der Unternehmen ein Vorfall nicht durch eine Auswertung der verfügbaren Protokollierungsinformationen (Log-Daten) erkannt werden können. Dies liegt darin begründet, dass die Mehrheit der Unternehmen die Log-Daten eher anlassbezogen sowie dezentral und manuell auswertet. Eine zeitnahe Detektion möglicher Sicherheitsvorfälle ist somit nicht gewährleistet.

Insgesamt ist das Thema Netzwerksicherheit bei den Unternehmen hinreichend gut etabliert. Schwächen sind eher bei der Nutzung von Standardtechnologien zur Anbindung externer Standorte zu identifizieren. So nutzen einige der befragten Unternehmen bei der standortübergreifenden Kommunikation Multiprotocol-Label-Switching-Netzwerke (MPLS-Netzwerke). Hierbei wird die MPLS-Verbindung, welche typischerweise durch einen Provider bereitgestellt wird, nicht in allen Fällen durch ein VPN geschützt. Ein Schutz der übertragenen Daten gegen unberechtigte Kenntnisnahme oder Manipulation ist in diesen Fällen nicht sichergestellt.

Von den befragten Unternehmen nutzen 97 Prozent das Internet in ihren Geschäftsprozessen. Hierbei ist die E-Mail-Kommunikation die am häufigsten eingesetzte Nutzungsart. Demzufolge wird im Rahmen der Anwendungen schwerpunktmäßig die E-Mail-Kommunikation betrachtet.

Werden hierbei vertrauliche Informationen oder Informationen mit hohem Integritätsanspruch übertragen und besteht eine gewisse Möglichkeit, dass diese Daten Unbefugten zur Kenntnis gelangen oder von diesen manipuliert werden können, sollte ein kryptographisches Verfahren in Betracht gezogen werden. Aus den Befragungen wird deutlich, dass die E-Mail-Kommunikation bei etwas mehr als der Hälfte der teilnehmenden Unternehmen ungesichert erfolgt.

Die Absicherung der E-Mails scheitert häufig an fehlenden technischen Möglichkeiten bzw. der unzureichenden Umsetzung des Schlüsselmanagements. In der Befragung wurde häufig die Begründung angegeben, dass der Kommunikationspartner eine Absicherung der E-Mail-Kommunikation aufgrund des hohen technischen Aufwandes bei der Schlüsselverteilung und -verwaltung ablehnt.

Prävention

Der Bereich der Präventivmaßnahmen ist insgesamt ambivalent zu bewerten. Einerseits sind die Sicherheitsmaßnahmen in Bezug auf die Datensicherung sowie die Aktualität der Informationen zur Bedrohungslage, zu Schwachstellen und Sicherheitsupdates etabliert. So sind im Zusammenhang

mit der Datensicherung lediglich Schwächen in Bezug auf die fortlaufende Prüfung der Aufbewahrungsorte sowie die regelmäßigen praktischen Übungen zur Wiederherstellung von Daten identifiziert worden. Anderseits zeigt sich deutlicher Handlungsbedarf bei der Detektion und Behandlung von Sicherheitsvorfällen sowie im Notfallmanagement.

Aus den Ergebnissen wird deutlich, dass das Management von IT-Sicherheitsvorfällen ein noch zu erschließendes Themengebiet für die Mehrzahl der Unternehmen darstellt. Viele Betriebe haben keine geeigneten Prozesse und Mechanismen im Umgang mit Sicherheitsvorfällen etabliert.

Im Bereich des Notfallmanagements zeigen sich ebenfalls deutliche Schwächen. Betroffen sind hier vor allem die Verfügbarkeit von Notfallkonzepten sowie die Planung und regelmäßige Durchführung von Notfalltests und -übungen. Insgesamt ist das Notfallmanagement bei weniger als der Hälfte der Unternehmen umgesetzt.

Management

Im Bereich der Risikobewertung der Geschäftsprozesse, der Bewertung der Gefahrenbereiche sowie bei den Reifegraden der den Management- und Organisationsthemen zuzuordnenden Sicherheitsprozessen zeigt sich ein zweigeteiltes Bild.

Einerseits kann die IT-Leitung sehr gut über kritische Geschäftsprozesse Auskunft geben, anderseits erfolgt eine regelmäßige Bewertung der Gefahrenbereiche nur in der Minderheit der Unternehmen. In den Fällen, wo eine Bewertung durchgeführt wurde, schätzen sowohl IT-Leitung als auch Management das menschliche Fehlverhalten als die größte Gefahrenquelle für das Unternehmen ein. Sehr ähnlich sind sich die Bewertungen für technische und organisatorische Mängel. Der Gefahrenbereich höhere Gewalt wird als geringstes Risiko für das Unternehmen eingeschätzt.

Im Themenkomplex Zukunftsthemen wurden neuartige Technologien oder Maßnahmen zur Unterstützung der Geschäftsprozesse in den Unternehmen angesprochen. Hierbei wurden die Technologien Cloud Computing, De-Mail/E-Postbrief und neuer elektronischer Personalausweis (nPA), welche aktuell in den Medien sehr präsent sind, diskutiert. Da es sich um noch umzusetzende Technologien in der Mehrheit der Unternehmen handelt, wurde auf eine Bewertung verzichtet.

Zur Ermittlung der Reife der IT-Sicherheitsprozesse wurden diese gemäß den Modellen aus Kapitel 3.3.2 betrachtet. IT-Sicherheitsmanagement muss sich auf zyklische Prozesse stützen, um effektiv zu sein. Die Prozesse sind jedoch nur dann dauerhaft nutzbar, wenn deren Qualität (Erfolg) gemessen und die zukünftige Entwicklung gesteuert wird. Prozesse, deren Abläufe nicht festgelegt oder deren Veränderungen das Ergebnis von „trial-and-error“ sind, werden über kurz oder lang zu Fehlern in den Abläufen und damit zu Lücken im IT-Sicherheitsmanagement führen.

Dagegen bilden Prozesse, die auf der Basis strukturierter und dokumentierter Beschreibungen gelebt werden, die aufeinander abgestimmt und deren Rollen und Verantwortlichkeiten geregelt sind, die Grundlage für ein belastbares IT-Sicherheitsmanagement. Nur eine fortlaufende Bewertung der Qualität sowie ggf. Nachjustierung der Prozesse kann mittel- bis langfristig deren erfolgreiche Anwendung sicherstellen.

In Ergänzung zu den pro Themenkomplex umgesetzten IT-Sicherheitsmaßnahmen zeigen die Reifegrade korrigierend auf, inwieweit die Unternehmen Sicherheitsprozesse zur langfristigen Sicherstellung der Qualität und der Eignung der Sicherheitsmechanismen etabliert haben.

Bei einer Bewertung aller betrachteten Prozesse ergibt sich ein Durchschnittswert von 42 Prozent für die in den befragten Unternehmen implementierten Sicherheitsprozesse. Im Vergleich zum

Durchschnittswert bei der Umsetzung von IT-Sicherheitsmaßnahmen (64 Prozent) wird deutlich, dass es in den Unternehmen in Bezug auf die Sicherheitsprozesse erheblichen Nachholbedarf gibt.

Das nachfolgende Kiviat-Diagramm (Abbildung 12) stellt die Reifegrade der in der Studie betrachteten Sicherheitsprozesse dar[1].

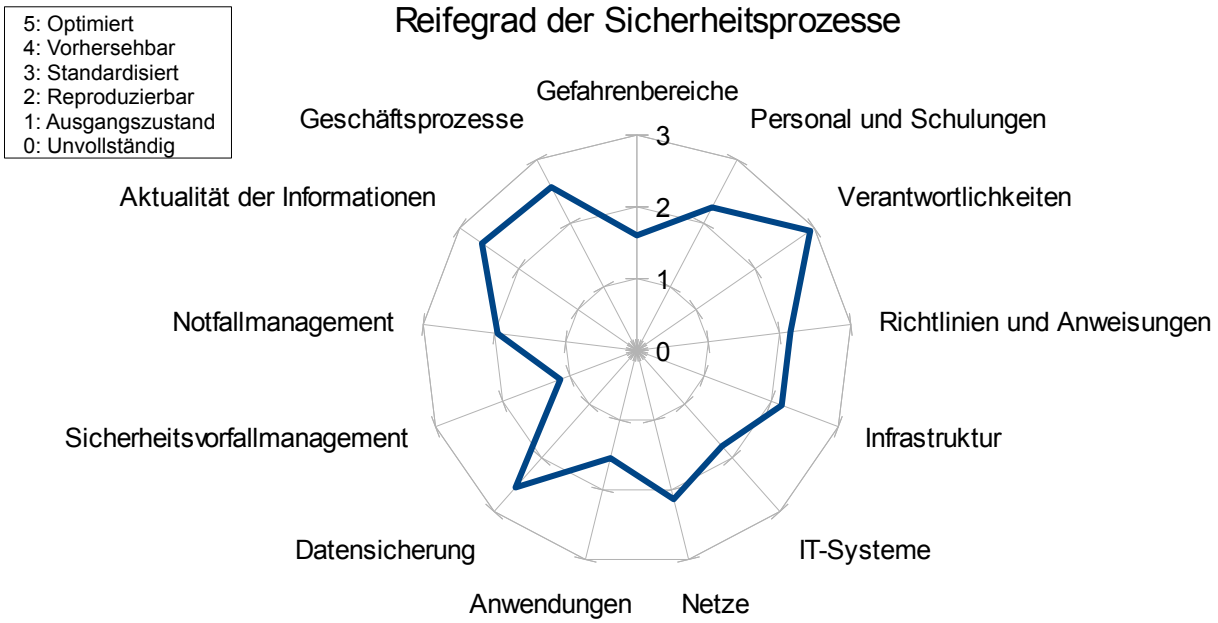


Abbildung 12: Reifegradbetrachtung der Sicherheitsprozesse

Insgesamt ist festzustellen, dass die Ergebnisse in Bezug auf die umgesetzten IT-Sicherheitsprozesse mehrheitlich im Bereich zwischen zwei und drei der Bewertungsskala liegen. Dies entspricht gemäß Tabelle 1 aus Kapitel 3.3.2 dem Bereich zwischen reproduzierbar und standardisiert. Ein optimaler Prozess würde sich im Bereich Fünf wiederfinden, während das Fehlen von Prozessen durch eine Null dargestellt wird.

Damit wird deutlich, dass die Prozesse der Verantwortlichkeit, der Datensicherung, der Aktualität der Informationen und der Risikobewertung der Geschäftsprozesse bereits standardisiert bzw. nahezu standardisiert sind.

Die Prozesse in Bezug auf Personal und Schulungen, Richtlinien und Anweisungen sowie Infrastruktur und Netze sind als reproduzierbar anzusehen. Es liegen hier definierte Prozessfolgen zur Anwendung vor. Die Prozesse sind jedoch nicht aufeinander abgestimmt, zudem ist das Bewusstsein für einen Prozess als Arbeitsgrundlage nicht durchgehend präsent. Zukünftige Veränderungen sind das Ergebnis von Versuch und Irrtum.

Die Reifegrade der IT-Sicherheitsprozesse in Bezug auf IT-Systeme, Anwendungen, Umgang mit Sicherheitsvorfällen, Notfallmanagement und Bewertung der Gefahrenbereiche liegen unter der Schwelle der Ebene zwei. Dies bedeutet, dass diese Prozesse eher chaotisch ablaufen. Einzelne Schritte eines Prozesses werden ausgeführt, die Schritte sind jedoch nicht festgelegt und werden ungeplant variiert. In der Summe entstehen trotzdem die gewünschten Ergebnisse, ohne jedoch eine Wiederholbarkeit des Ablaufes und des Ergebnisses gewährleisten zu können.

1 Es werden zur besseren Lesbarkeit nur die Wertebereiche 0 bis 3 aus der bis 5 reichenden Skala dargestellt.

Die möglichst umfassende Umsetzung von Sicherheitsmaßnahmen sowie die Etablierung geeigneter Prozesse ist die Grundvoraussetzung für das Erreichen eines dauerhaft belastbaren hohen IT-Sicherheitsniveaus. Bei einer gemeinsamen Betrachtung der Ergebnisse aus der Abbildung 11 - Gesamtergebnis der Studie und Abbildung 12 - Reifegradbetrachtung der Sicherheitsprozesse können die Themen bzgl. ihres Gesamtumsetzungsgrades bewertet werden. Daraus ergibt sich die nachfolgende Reihung:

1. Geschäftsprozesse
2. Aktualität der Informationen
3. Datensicherung
4. Verantwortlichkeiten
5. Netzwerk
6. Personal & Schulung
7. Infrastruktur
8. Richtlinien und Anweisungen
9. IT-Systeme
10. Anwendungen
11. Notfallmanagement
12. Bewertung der Gefahrenbereiche
13. Behandlung der Sicherheitsvorfälle

Die nähere Betrachtung zeigt, dass in den Themenkomplexen Geschäftsprozesse, Aktualität der Informationen und Datensicherungen sowohl Schutzmaßnahmen als auch Prozesse geeignet umgesetzt sind. Beim Thema Verantwortlichkeit sind hingegen die Prozesse etabliert, jedoch die Sicherheitsmaßnahmen nicht im vollen Umfang umgesetzt. Im Gegensatz dazu sind im Bereich Netzwerk ausreichend Sicherheitsmaßnahmen etabliert; hier mangelt es jedoch an entsprechenden Prozessen, um die aktuell hohe Güte des IT-Sicherheitsniveaus dauerhaft sicherstellen zu können.

In den Bereichen Personal und Schulungen, Infrastruktur, IT-Systeme, Anwendungen sowie Richtlinien und Anweisungen sind sowohl ein Teil der Sicherheitsmaßnahmen als auch die Prozesse zu Teilen umgesetzt.

Hingegen werden bei den Themenkomplexen Notfallmanagement, Bewertung der Gefahrenbereiche und Behandlung von Sicherheitsvorfällen weniger als die Hälfte der Sicherheitsmaßnahmen umgesetzt. Auch sind die Prozesse nicht reproduzierbar.

4.2.2 Handlungsempfehlungen

Die Ergebnisse zeigen in einzelnen Themenkomplexen sowie bei den Reifegraden der Sicherheitsprozesse einen deutlichen Handlungsbedarf. Zur Erreichung einer dauerhaft belastbaren und hohen IT-Sicherheit müssen sowohl die erforderlichen Schutzmaßnahmen umgesetzt, als auch die zugehörigen Prozesse etabliert sein. Es ist nicht ausreichend, Sicherheitsmaßnahmen umzusetzen, deren Funktionalität und Eignung aufgrund fehlender Prozesse nicht regelmäßig überprüft werden.

Alle Maßnahmen kurzfristig zu realisieren ist gerade im Bereich der KMU, nicht realistisch. Hierfür ist das Thema IT-Sicherheit zu komplex und die in den Unternehmen zur Verfügung stehenden Ressourcen zu begrenzt.

Nachfolgend wird ein Prozess zur Erreichung eines vorgegebenen Sicherheitsziels und der hierzu erforderlichen Sicherheitsmaßnahmen aufgezeigt. Dieser stellt einen Leitfaden zur Umsetzung der in den jeweiligen Themenkomplexen aufgezeigten Handlungsempfehlungen dar.

Zur Etablierung und Umsetzung von Sicherheitsprozessen hat sich in der Praxis das sogenannte Plan-Do-Check-Act-Modell (PDCA-Modell) etabliert. Dieses Modell erlaubt die Umsetzung einer strukturierten und nachhaltigen Vorgehensweise zur Realisierung von IT-Sicherheitsmaßnahmen. Die Elemente des PDCA-Modells sind in der nachfolgenden Abbildung 13 dargestellt.

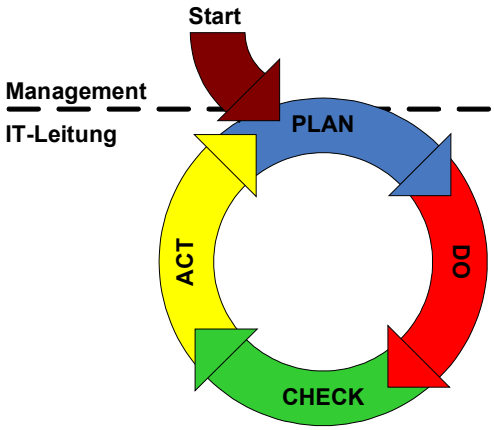


Abbildung 13: PDCA-Zyklus

Im Rahmen dieses Modells werden Abläufe einmalig von der Unternehmensleitung initiiert (Start). Dieser Punkt wird bei einer fortlaufenden Verfolgung des Modells nicht wieder erreicht. Hierüber erfolgt der Einstieg in die Planung und Konzeption (Plan). Diese beginnt immer mit der Festlegung der Ziele. Hierbei sollten als wesentliche Elemente die Sicherheitsziele und -strategien von der Unternehmensleitung definiert werden. Hierzu gehören das Festhalten von rechtlichen Rahmenbedingungen und das Setzen von Prioritäten. Durch die Veröffentlichung der Sicherheitsziele und -strategien im Unternehmen werden das Bewusstsein und die Verbindlichkeit geschaffen.

Mit der Definition der Ziele muss eine Planung erfolgen. Hierzu sollte eine Bestandsaufnahme im Unternehmen durchgeführt werden. So sind die Geschäftsprozesse zu prüfen und, deren Kritikalität zu bestimmen. Auch die Gefahrenbereiche für das Unternehmen sollten im Rahmen dieser Analyse bewertet werden. Darauf aufbauend lässt sich der Schutzbedarf für Daten, Informationen und Geschäftsprozesse definieren. Über diese Maßnahmen ist eine erste Gesamteinschätzung für das Unternehmen zu erhalten. Auf Basis dieser Einschätzung können Sicherheitsmaßnahmen definiert und umgesetzt werden.

Eine möglichst effiziente Umsetzung von IT-Sicherheit bedingt die Einführung eines übergreifenden Sicherheitsmanagements. Dies hat das Ziel, eine strukturierte Vorgehensweise dauerhaft zu etablieren. Der IT-Grundschutz [BSI_2011] beschreibt den Aufbau und die hierfür notwendigen Maßnahmen in Bezug auf das Sicherheitsmanagement im Baustein „B 1.0 Sicherheitsmanagement“. Wichtige Punkte sind hierbei:

- Schaffen von Verantwortlichkeiten und Ansprechpartnern

- Erstellung eines IT-Sicherheitskonzepts
- Genutzte Informationen zur Umsetzung von IT-Sicherheit immer auf den aktuellen Stand halten
- Etablierung von Richtlinien und Anweisungen
- Schulung und Sensibilisierung von Personal

Im Anschluss an die Planungsphase erfolgt die Umsetzung der Sicherheitsmaßnahmen (Do). Dabei können sich die Verantwortlichen an den IT-Grundschutz-Bausteinen B 2 bis B 6 orientieren. Damit ist sichergestellt, dass strukturiert alle umzusetzenden Maßnahmen betrachtet werden.

Nachdem die für das jeweilige Unternehmen relevanten Sicherheitsmaßnahmen für die bestehenden Bausteine realisiert sind, sollte eine Umsetzung der Präventivmaßnahmen angestrebt werden. Präventivmaßnahmen haben in einer ersten Betrachtung keinen aktiven Nutzen, allerdings verhindern sie bei Vorfällen größere Schäden für das Unternehmen. Am deutlichsten wird dies bei der Datensicherung, die als wichtigste Präventivmaßnahme angesehen werden kann. Für verlorene Daten muss das Unternehmen Kosten oder Ressourcen aufbringen. Ziel der Datensicherung ist daher, den Kosten- und Ressourcenaufwand zu minimieren, indem der aktuelle Datenbestand regelmäßig gesichert wird und so für ein teilautomatisiertes Wiedereinspielen zur Verfügung steht. Um sicherzustellen, dass die vorgenommene Datensicherung diesem Zweck genügt, sollte auch eine fortlaufende Prüfung der Wiederherstellbarkeit erfolgen.

Die zweite Priorität bei den Präventivmaßnahmen sollte auf die Behandlung von Sicherheitsvorfällen gelegt werden. Hierbei kommt es darauf an, eine möglichst große Bandbreite von Sicherheitsvorfällen erkennen und entsprechend behandeln zu können.

Abschließend sollte im Unternehmen ein Notfallmanagement umgesetzt werden. Hierfür bedarf es eines vergleichsweise hohen Einsatzes von Ressourcen. Der BSI-Standard 100-4 [BSI 2008] beschäftigt sich mit der Realisierung eines Notfallmanagements. Dabei wird das PDCA-Modell im Themenkontext Notfallmanagement aufgenommen und abgearbeitet.

Die Funktionalität und Eignung einer umgesetzten Schutzmaßnahme muss in regelmäßigen Abständen überprüft werden (Check). Dies kann nur dann erfolgen, wenn die Schutzmaßnahmen entsprechend dokumentiert und Kriterien zur Prüfung definiert sind. Kriterien und Kennzahlen werden im gleichnamigen Abschnitt in Kapitel 6 erläutert. Wichtig ist, dass jedes Unternehmen passende Kriterien definiert und anhand dieser Kriterien die Qualität der umgesetzten Schutzmaßnahmen regelmäßig überprüft.

Aus der fortlaufenden Überprüfung können Umsetzungs- oder Konzeptionsfehler identifiziert werden. Um möglichst effizient solche Fehler zu finden, wird die Begleitung durch externe Dienstleister empfohlen. Hierbei ist wichtig, dass die Verantwortlichkeiten für die Umsetzung und die Prüfung verschiedenen Personen zugeordnet wird. Hierzu bieten sich Funktionsträger wie ein IT-Revisor oder Auditor an. Die erkannten Fehler müssen durch definierte Prozesse vermindert oder das bestehende Risiko geduldet und gemeldet werden (Act). Hierzu sind die Verantwortlichkeiten und die Meldewege klar zu definieren. Die Verminderung oder Meldung von Fehlern hat eine Anpassung der erstellten Pläne und Konzeptionen zur Folge (Plan). Bei einer Verminderung müssen entsprechende Sicherheitskonzepte angepasst und aktualisiert werden. Bei der Meldung von Fehlern sollten die Gefahrenbereiche für das Unternehmen neu bewertet und das Risiko neu eingeschätzt werden.

Der aufgezeigte PDCA-Prozess beschreibt dessen Anwendung auf einen übergreifenden IT-Sicherheitsprozess. Um eine umfassende Steuerungsmöglichkeit für alle Prozesse zu erhalten, ist das Modell in allen Themenkomplexen umzusetzen. Dies ermöglicht die Etablierung eines übergreifenden wie auch themenspezifischen Sicherheitsprozesses. Die Umsetzung der zur Erreichung eines vorgegebenen Sicherheitsziele erforderlichen Sicherheitsmaßnahmen kann so sichergestellt werden.

4.3 Personal und Schulungen

Informiertes und geschultes Personal ist die Grundlage einer sicheren Durchführung von Geschäftsprozessen in Unternehmen. Neben der Information des Personals über die etablierten Prozesse, unternehmensspezifische Regelungen und Handlungsanweisungen sind insbesondere regelmäßige Schulungen zu IT-Sicherheitsmaßnahmen erforderlich um eine Verbesserung des IT-Sicherheitsniveaus zu erreichen.

4.3.1 Themen in den Interviews

Um die Einbindung des Personals im Rahmen der Studie beurteilen zu können, wurden die folgenden Punkte abgefragt:

- **Einarbeitung neuer Mitarbeiter:** Die Einarbeitung neuer Mitarbeiter ist zur zügigen Integration in die bestehenden Prozesse unerlässlich. Darüber hinaus muss das Unternehmen neuen Mitarbeitern bestehende Regelungen und Handlungsanweisungen bekannt machen und auf die sich aus einer Zuwiderhandlung ergebenden Konsequenzen hinweisen. Insbesondere bei der Mitarbeitergewinnung in sicherheitskritischen Betriebsumgebungen empfiehlt es sich, die Mitarbeiter entsprechend zu verpflichten und die Vertrauenswürdigkeit von Mitarbeitern bestätigen zu lassen. Ausgehend vom polizeilichen Führungszeugnis bis hin zur Sicherheitsüberprüfung existieren verschiedene Möglichkeiten, welche jedoch im Einzelfall auf ihre Zulässigkeit zu prüfen sind und ggf. nicht allen Unternehmen zur Verfügung stehen.
- **Kontinuierliche Information der Mitarbeiter:** Es ist unerlässlich, alle Mitarbeiter über Veränderungen der Regelungen und ihre spezifischen Auswirkungen auf einen Prozess oder auf den einzelnen Mitarbeiter zu informieren.
- **Ausscheiden von Mitarbeitern:** Beim Ausscheiden oder Funktionswechsel eines Mitarbeiters ist der Prozess zur Aktualisierung der Zugriffs- bzw. Zugangsrechte aktiv durchzuführen. Entscheidend für die erfolgreiche Durchführung ist, dass der Prozess zur Weiterleitung der Information über das Ausscheiden an die verantwortlichen Stellen zeitnah erfolgt und dass die Durchführung dokumentiert wird.
- **Schulungen vor der Programmnutzung:** Über Schulungen kann dem Personal vermittelt werden, wie unternehmensspezifische Programme genutzt werden. Dies versetzt die Mitarbeiter in die Lage, die Geschäftsprozesse sicher zu realisieren.
- **Schulungen zu IT-Sicherheitsmaßnahmen:** Implementierte IT-Sicherheitsmaßnahmen können sowohl die technischen als auch die organisatorischen Betriebsabläufe stören. Daher sind die Mitarbeiter über Bedeutung und Anwendung von Sicherheitsmaßnahmen zu unterrichten, um im Unternehmen ein Bewusstsein für IT-Sicherheit zu schaffen.

4.3.2 Ergebnisse

Die Befragungsergebnisse der teilnehmenden Unternehmen zu den Punkten Personal und Schulungen sind in der Abbildung 14 dargestellt.

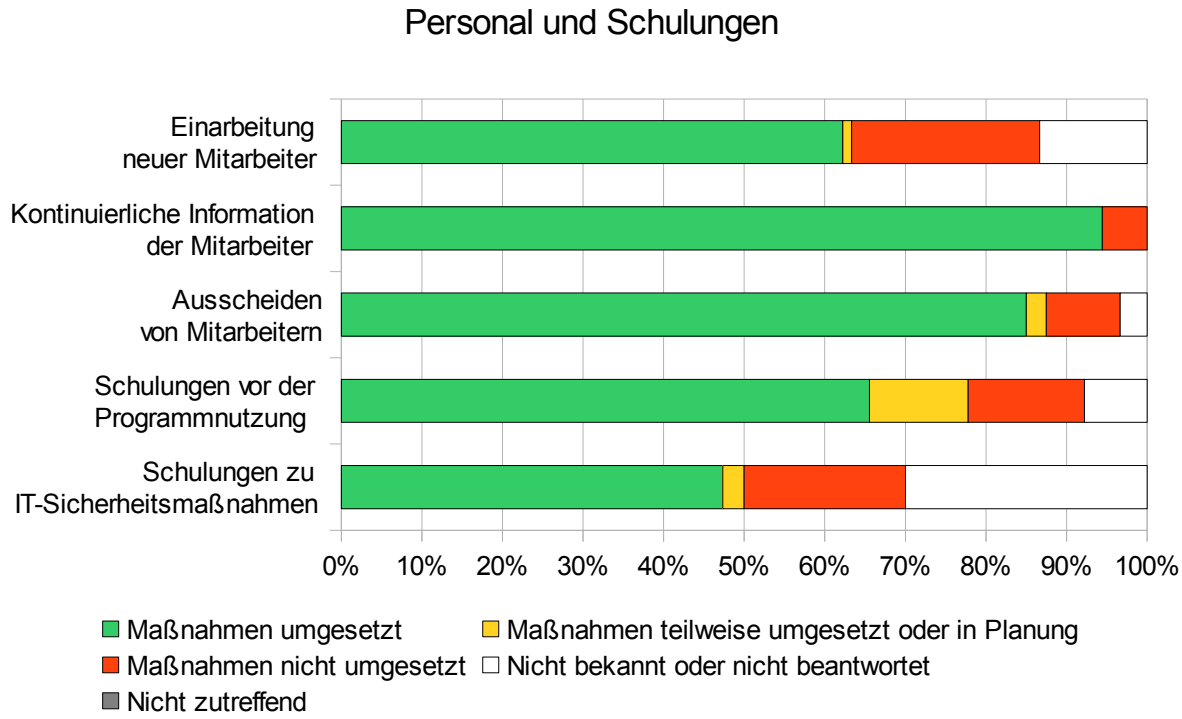


Abbildung 14: Auswertung von Personal und Schulungen

Die Betreuung von Mitarbeitern findet sehr starke Berücksichtigung. Insbesondere sind die Ansprechpartner zu IT-Sicherheitsfragen benannt und den Mitarbeitern bekannt. Auch werden die Mitarbeiter regelmäßig über Änderungen von Regelungen und deren spezifische Auswirkungen auf einen Prozess oder auf den einzelnen Mitarbeiter informiert. Dies erfolgt in den meisten Fällen über E-Mails. Die Bereitstellung erfolgt zudem über eine unternehmensinterne Webseite oder im Rahmen von allgemeinen Informationsveranstaltungen. Thema einer Schulung sind diese Veränderungen jedoch nur in jedem fünften Unternehmen.

Auch für den Fall, dass Mitarbeiter aus bestimmten Geschäftsprozessen oder aus dem Unternehmen ausscheiden, sind die entsprechenden Maßnahmen und Prozesse etabliert. So sind in 86 Prozent der Unternehmen die Aktivitäten in Bezug auf das Ausscheiden von Mitarbeitern geregelt. In drei Viertel der Unternehmen sind diese Regelungen auch adäquat dokumentiert.

Die notwendigen Maßnahmen zur Einarbeitung neuer Mitarbeiter sind jedoch nicht bei allen Unternehmen in geeignetem Umfang umgesetzt. Hier sind deutliche Defizite (roter Balken) zu erkennen. Insbesondere die Prüfungen zur Vertrauenswürdigkeit von Mitarbeitern in sensitiven Bereichen erfolgen in vielen Fällen nicht. Hinzu kommt, dass der Prüfaspekt und die Einarbeitung neuer Mitarbeiter häufig im Verantwortungsbereich der Personalabteilung liegt und daher die befragten Personen keine näheren Angaben hierzu machen konnten.

Schulungen sind im KMU-Bereich nur teilweise etabliert. Häufig handelt es sich hierbei um allgemeine Informationsveranstaltung für alle Mitarbeiter. Eine Schulung vor Programmnutzung erfolgt in vielen Fällen in Form einer Einweisung am Arbeitsplatz durch einen bereits eingearbeiteten Mitarbeiter. Nach Aussage der Befragten wird dies jedoch nicht als vollwertiger Ersatz für eine klassische Schulung angesehen. Ergänzend zu den Einweisungen stehen den Mitarbeitern in 60 Prozent der Fälle anwendungsspezifische Richtlinien zur sicheren Nutzung der IT zur Verfügung.

Schulungen zu IT-Sicherheitsmaßnahmen werden nur bedingt in den befragten Unternehmen durchgeführt. Die Gesamtaussage zu den Schulungen zu IT-Sicherheitsmaßnahmen wird in Abbildung 14 dargestellt. Die Einzelbewertungen, die zu dieser Gesamtaussage führen, werden in der nachfolgenden Abbildung 15 detailliert dargestellt.

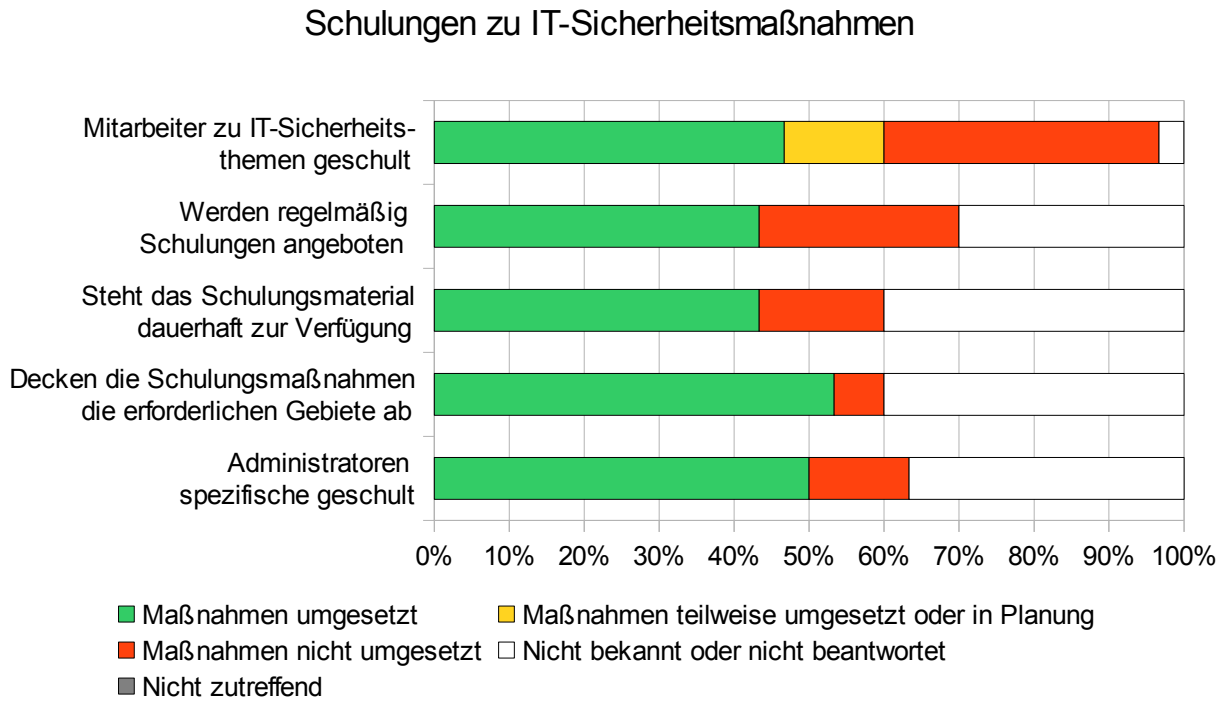


Abbildung 15: Schulungen zu IT-Sicherheitsmaßnahmen

Nur in knapp der Hälfte der Unternehmen finden Schulungen zu IT-Sicherheitsmaßnahmen statt. Knapp 10 Prozent der Unternehmen gaben an, dass eine solche Schulung nur für einen Teil der Mitarbeiter durchgeführt wurde. Häufig wurde mitgeteilt, dass Mitarbeiter der IT-Abteilung nicht zu den IT-Sicherheitsthemen geschult werden. Ein Teil der Geschäftsführung gab dazu an, dass dort eine sehr hohe Motivation zur selbstständigen Weiterbildung besteht und daher IT-Sicherheitsthemen nicht intensiv geschult werden müssten.

Weiterhin ist auffällig, dass die Befragten nicht in allen Fällen darüber Auskunft geben können, ob Schulungen zu IT-Sicherheitsthemen regelmäßig angeboten werden, Schulungsmaterial dauerhaft zur Verfügung gestellt wird bzw. spezifische Schulungen stattfinden (siehe Abbildung 15). In den Interviews wurden diese Punkte daher hinterfragt. Hierbei wurde festgestellt, dass einige Unternehmen eine eigene Schulungsabteilung im Unternehmen betreiben, die sich mit diesen Themen auseinandersetzt. Somit wird die IT-Leitung von diesem Thema entlastet.

4.3.3 Handlungsempfehlungen

Die Ergebnisse zeigen, dass die Unternehmen Handlungsbedarf im Bereich der Einarbeitung neuer Mitarbeiter und der Schulung zu IT-Sicherheitsmaßnahmen haben.

Die Prüfung der Vertrauenswürdigkeit von neuen Mitarbeitern ist durch die gesetzlichen Rahmenbedingungen (z.B. Datenschutzbestimmungen) nur eingeschränkt möglich. Bei Neueinstellungen kann von Bewerbern ausschließlich ein polizeiliches Führungszeugnis verlangt werden. Die Überprüfung der Vertrauenswürdigkeit der Mitarbeiter kann aber entscheidend für die Wahrung der Grundwerte sein. Dies gilt insbesondere in sensitiven Bereichen, wie zum Beispiel der Administration von Netzen und Systemen.

Kurzfristig können die Überprüfungen durch Bestätigung der beruflichen Qualifikationen bei Ausbildungsstätten und früheren Arbeitgebern erfolgen. Die Vertrauenswürdigkeit kann zusätzlich durch eine vertragliche Verpflichtung des Mitarbeiters ergänzt werden.

Für das Thema Schulungen vor Programmnutzung und Schulungen von IT-Sicherheitsmaßnahmen können übergangsweise bereits stattfindende Schulungen genutzt werden, um aktuelle Informationen zur IT-Sicherheit an die Mitarbeiter zu vermitteln.

Mittelfristig sollten hierfür jedoch eigene Schulungen im Unternehmen realisiert werden. Hierfür gibt der IT-Grundschutz [BSI_2011] in der Maßnahme „M 3.45 Planungen von Schulungsinhalten zur Informationssicherheit“ unterstützende Hinweise.

Schulungen ermöglichen es den Mitarbeitern auch, konkrete Fragen zu stellen und Antworten von Experten zu erhalten. Weiterhin haben Schulungen für IT-Sicherheitsmaßnahmen den Effekt, das Verständnis für den Einsatz zu verbessern. Dabei kann vermittelt werden, aus welchen Gründen bestimmte Maßnahmen auch Restriktionen erfordern. Organisatorische Maßnahmen lassen sich somit leichter realisieren und durchsetzen.

Langfristig ist die Realisierung eines Schulungs- und Sensibilisierungskonzepts im Unternehmen anzustreben. Besonders für die Schulungen zu IT-Sicherheitsmaßnahmen sollte ein solches Konzept mit den folgenden Kernthemen berücksichtigt werden (vgl. IT-Grundschutz [BSI_2011] Maßnahme „M 3.5 Schulung zu Sicherheitsmaßnahmen“):

- Sensibilisierung für Informationssicherheit
- Mitarbeiterbezogene Informationssicherheitsmaßnahmen
- Produktbezogene Sicherheitsmaßnahmen
- Verhalten bei Auftreten von Schadsoftware
- Bedeutung der Datensicherung und deren Durchführung
- Umgang mit personenbezogenen Daten
- Einweisung in Notfallmaßnahmen
- Vorbeugung gegen Social Engineering

Wichtig bei einem Schulungs- und Sensibilisierungskonzept ist die regelmäßige Wiederholung der Maßnahmen. Es reicht nicht aus, einen Mitarbeiter einmal im gesamten Arbeitsverhältnis zu schulen. Durch die Regelmäßigkeit ist dem Mitarbeiter bekannt, wann die nächste Schulung erfolgt. Eine entsprechende Vorbereitung auf die Schulung und ein Einplanen in den Arbeitsablauf sind somit möglich.

4.4 Sicherheitsprozesse

Die Umsetzung von Sicherheitsprozessen ist ein wesentlicher Bestandteil der Realisierung eines Managementsystems für Informationssicherheit. Hierbei sind Prozesse zur Wahrung der Vertraulichkeit, der Integrität und der Verfügbarkeit zu etablieren.

4.4.1 Themen in den Interviews

In diesem Rahmen wird der Umsetzungsgrad der Sicherheitsprozesse in Bezug auf die Grundwerte als Querschnittsthema quantitativ betrachtet. Im Unterschied hierzu, sind die Reifegrade ein Qualitätskriterien für den Entwicklungsstand eines IT-Sicherheitsprozesses und beziehen sich auf den jeweils betrachten Prozess. Diese werden in Kapitel 4.17 bewertet.

- **Vertraulichkeit:** Zur Bewertung der Vertraulichkeit werden die Aussagen der Unternehmen zur Absicherung der Kommunikationsverbindungen, dem Einsatz von Verschlüsselungs- und Signaturlösungen und dem Einsatz von Authentifizierungsverfahren ausgewertet.
- **Integrität:** Die Betrachtung der Prozesse zur Sicherung der Integrität wertet vor allem die Verpflichtung zur Dokumentation sowie den Stand und die Nachvollziehbarkeit der Dokumentation aus.
- **Verfügbarkeit:** Die Prozesse zur Aufrechterhaltung der Verfügbarkeit umfassen die Redundanz der kritischen Systeme, die Konzepte zur Wiederaufnahme und zum Wiederanlauf, die Praxistauglichkeit des Sicherheitsvorfalls- und Notfallmanagements sowie die technische und organisatorische Durchführung der Datensicherung.

4.4.2 Ergebnisse

Die Ergebnisse für die befragten Unternehmen sind in der Abbildung 16 dargestellt.

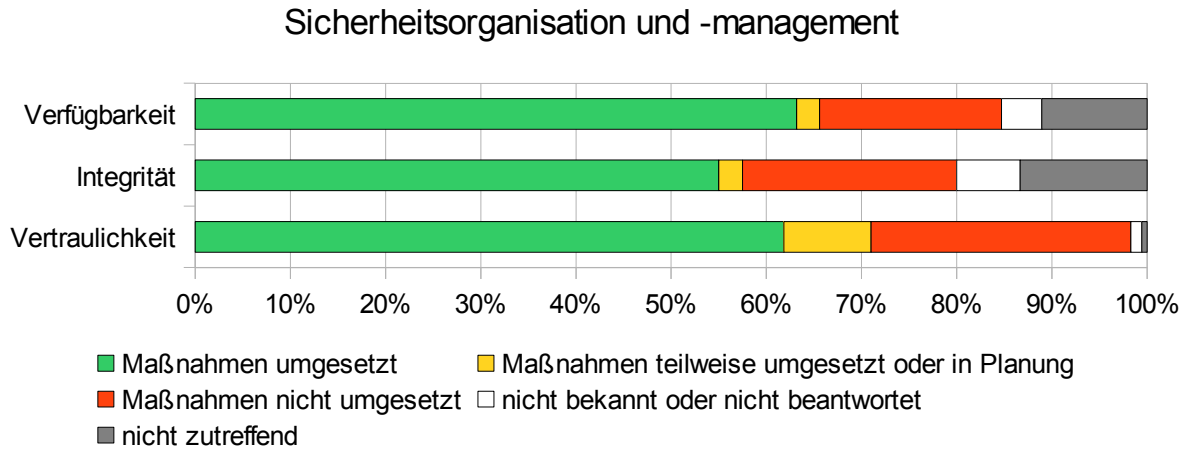


Abbildung 16: Auswertung Sicherheitsprozesse

Aus der Darstellung in Abbildung 16 wird deutlich, dass in den Unternehmen die Sicherheitsmaßnahmen zur Wahrung der Vertraulichkeit und der Verfügbarkeit nur jeweils zu zwei Dritteln umgesetzt sind. Maßnahmen zur Sicherung der Integrität sind nur zu 55 Prozent vorhanden.

Insbesondere die Vertraulichkeit der Kommunikationsverbindungen ist bei Verwendung von E-Mail unzureichend umgesetzt. Hier setzt nur jedes fünfte Unternehmen Verschlüsselungs- und/oder Signaturlösungen ein. Hingegen sind in mehr als 86 Prozent der Fälle Netzwerkverbindungen durch Verwendung von VPN und Webverbindungen durch den Einsatz von SSL insgesamt gut geschützt.

Während die Durchführung der Datensicherung technisch und organisatorisch in über 90 Prozent der Unternehmen umgesetzt ist, kann die Verfügbarkeit kritischer IT-Systeme durch den Aufbau redundanter Systeme nur bei zwei Drittel der Unternehmen als gegeben angesehen werden.

Weitere Schwächen sind beim Sicherheitsvorfall- und Notfallmanagement sowie den Konzepten zum schnellen Wiederanlauf ersichtlich. Die zur Sicherstellung der Verfügbarkeit erforderlichen Regelungen und Konzepte sind nur bei der Hälfte der Unternehmen umgesetzt.

Die Integrität von Informationen betreffende Sicherheitsprozesse sind in den befragten Unternehmen weniger stark ausgeprägt. So wird für die Wahrung der Integrität mehr auf das menschliche Urteilsvermögen vertraut. Die Korrektheit der Informationen bzw. die Funktionsfähigkeit der Systeme wird in vielen Unternehmen sporadisch geprüft, jedoch sehr häufig nicht dokumentiert. So wird nur in 30 Prozent der Unternehmen die Prüfung von Maßnahmen dokumentiert. Dies wird oftmals mit der Unternehmensgröße begründet. So ist in kleineren Unternehmen nur eine Person für die Prüfung verantwortlich. In größeren Unternehmen hingegen sind aufgrund der Aufgaben- und Verantwortungsverteilung vermehrt Dokumentationen zu finden.

4.4.3 Handlungsempfehlungen

Der in diesem Rahmen quantitativ bewertete Umsetzungsgrad der Sicherheitsprozesse bezieht sich als Querschnittsthema auf die in dieser Studie betrachteten Themenkomplexe.

Demzufolge sind die direkten Handlungsempfehlungen den einzelnen Themenkomplexen zu entnehmen. Jedoch ist nach Umsetzung von Maßnahmen im Rahmen der Sicherheitsprozesse zu prüfen, ob die Grundwerte der Vertraulichkeit, Verfügbarkeit und Integrität erfüllt sind.

4.5 Verantwortlichkeiten

Zur Durchsetzung von Sicherheitsmaßnahmen in einem Unternehmen ist es wichtig, dass die Unternehmensleitung die Verantwortung hierfür übernimmt. Zusätzlich sollten für die Abgrenzung der Aufgabengebiete, aber auch zur Vermeidung von Zuständigkeitslücken die Verantwortlichkeiten für alle wesentlichen Aufgaben, insbesondere im Informationssicherheitsprozess, nachvollziehbar geregelt sein. Nur bei klar definierten Verantwortlichkeiten und einer klaren Verteilung von Aufgaben und Befugnissen können die Geschäftsprozesse eines Unternehmens optimal gestaltet und ein angemessenes Sicherheitsniveau gewährleistet werden.

4.5.1 Themen in den Interviews

Zur Bewertung der Regelungen in Bezug auf die Verantwortlichkeiten wurden die folgenden Kriterien geprüft:

- **Übernahme der Verantwortung durch die Unternehmensleitung:** Zur Durchsetzung von Sicherheitsmaßnahmen in einem Unternehmen ist es wichtig, dass die Unternehmensleitung diese selbst vorlebt und die Verantwortung hierfür übernimmt. Diese Verantwortung bezieht sich ebenfalls auf die Früherkennung und Minimierung von möglichen Risiken für den Betrieb. Dazu gehören auch solche, die aus unzureichender Informationssicherheit entstehen. Die Geschäftsführung sollte regelmäßig über mögliche Risiken und Konsequenzen aufgrund fehlender Informationssicherheit aufgeklärt werden.
- **Allgemeine Regelungen der Verantwortlichkeiten im Bereich der IT:** Für alle wesentlichen Aufgaben und Geschäftsprozesse in Bezug auf die in einer Institution genutzte Informationstechnologie sollten die Verantwortlichkeiten nachvollziehbar geregelt sein. Die Aufgaben sollten dabei so zugeschnitten sein, dass es keine Überschneidungen zwischen ähnlichen Aufgaben gibt, aber auch keine Zuständigkeitslücken. Des Weiteren sollte festgelegt sein, welche Funktionen nicht miteinander vereinbar sind, also auch nicht von einer Person gleichzeitig wahrgenommen werden dürfen. Es sollte auch bei der Zuordnung der Personen zu den jeweiligen Funktionen eine Vertreterregelung berücksichtigt werden.
- **Regelungen der Verantwortlichkeiten zu Sicherheitsfragen:** Dauerhaft ein angemessenes Sicherheitsniveau zu gewährleisten, erfordert ein systematisches Vorgehen sowie einen kontinuierlichen und zielgerichteten Sicherheitsprozess. Diesen zu initiieren, zu steuern und zu kontrollieren ist Aufgabe der Leitungsebene. In Abhängigkeit von der Größe des Unternehmens kann diese Aufgabe an eine dedizierte Person, den IT-Sicherheitsbeauftragten delegiert werden. Um seine Aufgaben wahrnehmen zu können, sind diesem ausreichend Ressourcen zur Verfügung zu stellen. Des Weiteren muss der IT-Sicherheitsbeauftragte frühzeitig in die relevanten Entscheidungsprozesse eingebunden werden.

4.5.2 Ergebnisse

Das Gesamtergebnis in Bezug auf die Regelung der Verantwortlichkeiten in den befragten Unternehmen ist in der Abbildung 17 dargestellt.

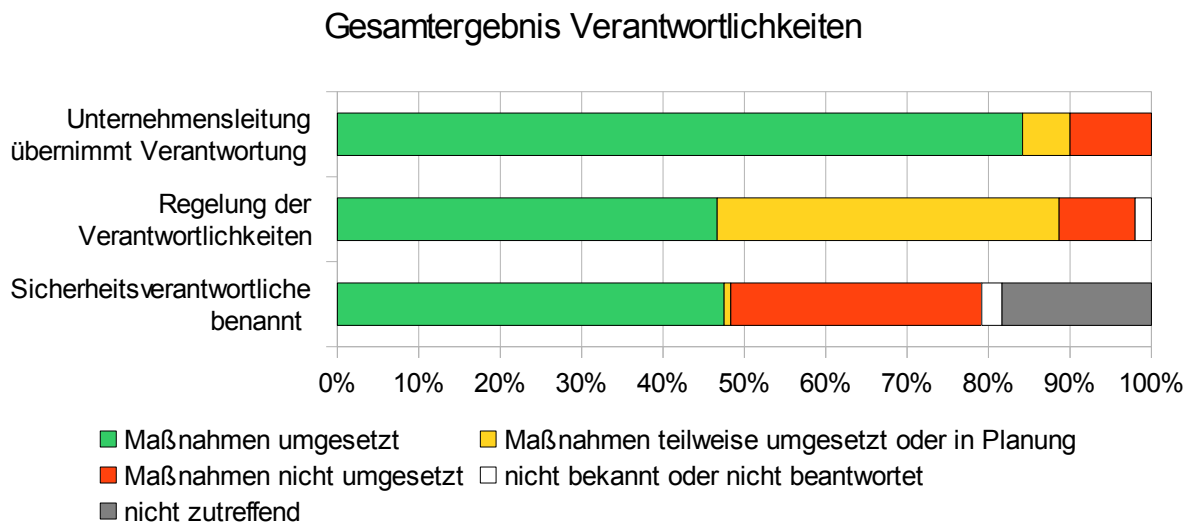


Abbildung 17: Gesamtergebnis Verantwortlichkeiten

Die Unternehmensleitung hat aus Sicht aller befragten Personen deutlich die Verantwortung in Bezug auf die IT-Sicherheit übernommen. So lässt sich in 86 Prozent der Unternehmen die Geschäftsführung regelmäßig zu möglichen Risiken und Konsequenzen aufgrund fehlender Informationssicherheit aufklären. Dies erfolgt hauptsächlich (80 Prozent) durch Personen aus dem eigenen Unternehmen. In 40 Prozent der Unternehmen werden diese durch externe Dienstleister unterstützt. Die positive Eigeneinschätzung der Geschäftsführung in Bezug auf das Vorleben der IT-Sicherheitsmaßnahmen – 90 Prozent sehen dies als gegeben an – wird nur bei zwei Drittel der Unternehmen von der IT-Leitung geteilt. Jeder fünfte IT-Leiter gibt an, dass die Vorgaben zur IT-Sicherheit von der Geschäftsführung nicht umgesetzt werden.

Ihre Verantwortung bei der Umsetzung von IT-Sicherheitsmaßnahmen unterstreicht die Unternehmensleitung auch durch die geäußerte Bereitschaft, in IT-Sicherheitsmaßnahmen zu investieren. Dies wurde jedoch von den Unternehmen nicht mit exakten Zahlen belegt. Im Bereich der produzierenden Unternehmen liegt ein typischer Wert für die Investitionen in die IT, welche das Budget für IT-Sicherheitsmaßnahmen umfasst, im Bereich von 2 bis 3 Prozent bezogen auf den Umsatz.

Die Unternehmen bemühen sich, dem Thema der Verantwortlichkeiten geeignet Rechnung zu tragen. In der Praxis zeigen sich in der Verteilung der Funktionen und Aufgaben jedoch Spannungsfelder. So sind nur in jedem fünften der befragten Unternehmen die gemäß der IT-Grundschutz-Maßnahme M 2.1 empfohlenen Verantwortlichkeiten umfassend definiert. Des Weiteren können aufgrund der begrenzten personellen Ressourcen im Unternehmen und einer nochmals deutlich geringeren Anzahl von Mitarbeitern in der IT-Abteilung personelle Funktionstrennungen nur bedingt aufrecht erhalten werden. Eine durchgehende personelle Funktionstrennung ist nur bei jedem dritten Unternehmen gegeben. Auch die eindeutige Aufgabenverteilung ist so oft nicht möglich.

Gerade hier zeigt sich jedoch auch eine Stärke der kleinen und mittleren Unternehmen: Unabhängig von der Aufgabenzuordnung werden die anfallenden Aufgaben durch den jeweils verfügbaren Mitarbeiter erledigt. In den Interviews wurde häufig darauf hingewiesen, dass die Unternehmen eher die Generalisten als die Spezialisten als Mitarbeiter bevorzugen.

Die Notwendigkeit der Etablierung von Vertreterregelungen, gerade für die kritischen personellen Ressourcen, ist den Unternehmen bewusst. Vereinzelt plant das Management, in diesen Bereichen Unterstützung durch externe Dienstleister wahrzunehmen, sofern nicht ausreichend qualifiziertes Personal im eigenen Unternehmen verfügbar ist. So sind bei 73 Prozent der Unternehmen die Vertretungsregelungen umgesetzt. In 60 Prozent der Fälle stehen ausreichend qualifizierte Vertreter bereit.

Hinsichtlich der klaren Benennung der Verantwortung für IT-Sicherheit sind die Unternehmen nicht optimal aufgestellt. Die Einzelbewertungen, die zu dieser Gesamtaussage führen, sind der nachfolgenden Abbildung 18 zu entnehmen.

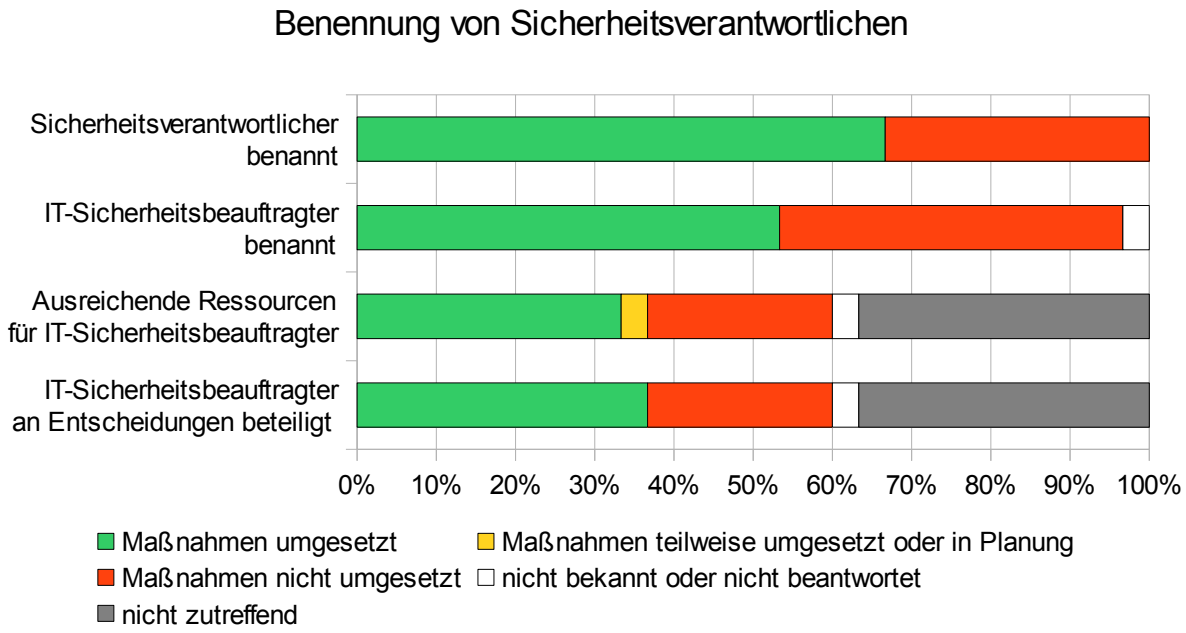


Abbildung 18: Benennung von Sicherheitsverantwortlichen

In zwei Drittel der Unternehmen sind IT-Sicherheitsverantwortliche durch die Unternehmensleitung benannt. Hierbei handelt es sich in 16 von 30 Fällen um die dedizierte Rolle des IT-Sicherheitsbeauftragten. Diese Rolle wird in den meisten Fällen mit einem Mitarbeiter aus der IT-Abteilung besetzt. In den Unternehmen, die keinen IT-Sicherheitsbeauftragten bzw. keinen Sicherheitsverantwortlichen benannt haben, werden deren Aufgaben typischerweise durch die IT-Leitung übernommen.

Bei einer Hinterfragung der zur Verfügung stehenden Ressourcen wurde offen gelegt, dass nur noch bei knapp einem Drittel der Unternehmen der IT-Sicherheitsbeauftragte ausreichend Ressourcen für die Durchführung der Tätigkeiten erhält. Hier sind insbesondere zeitliche Engpässe genannt worden. So hat der IT-Sicherheitsbeauftragte nicht nur diese Funktion inne, sondern muss auch Aufgaben aus dem laufenden Betrieb wahrnehmen. Ähnlich sieht es bei der Einbindung des IT-Sicherheitsbeauftragten in die relevanten Entscheidungen – gerade durch die Geschäftsführung – aus. Auch hier wird dieser nur bei ca. einem Drittel der Unternehmen geeignet in die Entscheidungsprozesse integriert. Dies hat zur Folge, dass der IT-Sicherheitsbeauftragte häufig nur noch informiert wird und nicht mehr beratend tätig ist.

Obwohl die Unternehmensleitung die Verantwortung für die Informationssicherheit deutlich sichtbar übernommen hat, sind nur in der Hälfte der befragten Unternehmen die Maßnahmen zur Regelung der weiteren Verantwortlichkeiten umgesetzt. Insbesondere erfolgt die Benennung von IT-Sicherheitsbeauftragten nur bei jedem zweiten Unternehmen. In vielen Fällen wird die IT-Leitung mit diesen Aufgaben zusätzlich belastet.

Durch die deutlichen Schwächen bei der Abgrenzung der Aufgabengebiete sowie der Definition der Verantwortlichen kann es zu Zuständigkeitslücken kommen, so dass ein angemessenes Sicherheitsniveau nicht immer gewährleistet werden kann.

4.5.3 Handlungsempfehlungen

Es sollte kurzfristig eine Überprüfung der Regelungen zu den Verantwortlichkeiten, zur Aufgabenverteilung und der personellen Funktionstrennung erfolgen, um Überschneidungen sowie Zuständigkeitslücken zu identifizieren.

Anschließend sind die noch nicht abgedeckten Verantwortlichkeiten für alle wesentlichen Aufgaben, insbesondere im Informationssicherheitsprozess, nachvollziehbar durch explizite Zuweisung der Verantwortlichkeiten und Befugnisse an Rollen bzw. Organisationseinheiten zu regeln. Die Zuweisungen sind zu dokumentieren.

Einige Unternehmen haben von einer Motivationssteigerung bei den Mitarbeitern berichtet, die nach expliziter Zuweisung der Verantwortlichkeiten und Befugnisse eingetreten ist.

Alle Unternehmen, die IT-gestützte Geschäftsprozesse abwickeln, sollten einen IT-Sicherheitsbeauftragten benennen. Die Aufgaben eines IT-Sicherheitsbeauftragten sind im IT-Grundschutz des BSI unter der Maßnahme „M 2.193 – Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit“ beschrieben. Für die Erfüllung der Funktion muss die verantwortliche Person im erforderlichen Umfang von ihren sonstigen Aufgaben im Unternehmen freigestellt sein. Des Weiteren ist diese Person in alle relevanten Entscheidungsprozesse direkt mit einzubeziehen, so dass die notwendigen IT-Sicherheitsmaßnahmen adressiert und realisiert werden können.

Mittelfristig ist die Funktionstrennung festzulegen und zu begründen, warum diese Funktionen nicht miteinander vereinbar sind und somit nicht von der gleichen Person wahrgenommen werden dürfen. Vorgaben hierfür können aus den Aufgaben selbst oder aus gesetzlichen Bestimmungen resultieren. Beispiele dafür sind:

- Rechteverwaltung und Revision,
- Netzadministration und Revision,
- Programmierung und Test bei selbst erstellter Software,
- Datenerfassung und Zahlungsanordnungsbefugnis,
- Revision und Zahlungsanordnungsbefugnis.

Weitergehende Maßnahmenempfehlungen zur Adressierung des aufgezeigten Handlungsbedarfs sind den Abschnitten M2.1, M2.5 und M2.336 der IT-Grundschutz-Kataloge [BSI 2008] zu entnehmen.

4.6 Richtlinien und Anweisungen

Ausschließlich mündliche gegebene Anweisungen sind in der Regel nicht nachhaltig und geraten schnell in Vergessenheit. Daher sollten Richtlinien und Anweisung in schriftlicher Form dokumentiert werden. Besonders bei wachsenden Unternehmen muss frühzeitig mit einer solchen Dokumentation begonnen werden, um langfristig die Arbeitsaufwände zur Pflege der Dokumentation zu minimieren und die Verfügbarkeit und Aktualität der Richtlinien und Anweisungen sicherstellen zu können.

4.6.1 Themen in den Interviews

Im Rahmen der Studie wurden die Unternehmen nach der Verfügbarkeit unterschiedlicher Richtlinien und Anweisungen befragt. Die folgenden Kriterien sind hierbei zugrunde gelegt worden:

- **Verfügbarkeit von Richtlinien und Anweisungen:** Der IT-Grundschutz empfiehlt die Bereitstellung von zielgruppengerechten Richtlinien und Anweisungen, welche die einzelnen Sicherheitsthemen bedarfsgerecht darstellen. Als Kriterium wird die Verfügbarkeit ausgewählter Richtlinien geprüft.
- **Einhaltung von Richtlinien und Anweisungen:** Die Einhaltung von Richtlinien und Anweisungen sollte in einem Unternehmen in regelmäßigen Abständen kontrolliert und bei Missachtung entsprechend mit Konsequenzen belegt werden. Neben der Einhaltung wird ebenfalls die regelmäßige Kontrolle auf Eignung der Richtlinien bewertet.
- **Verfügbarkeit von Sicherheitszielen und -strategien:** Es wird geprüft, ob von der Unternehmensleitung die allgemeinen Sicherheitsziele und die Sicherheitsstrategie formuliert wurden. Des Weiteren wird bewertet, ob die Mitarbeiter über die Sicherheitsziele und -strategien informiert wurden.

4.6.2 Ergebnisse

Die Aussagen der befragten Unternehmen sind in der Abbildung 19 zusammenfassend dargestellt.

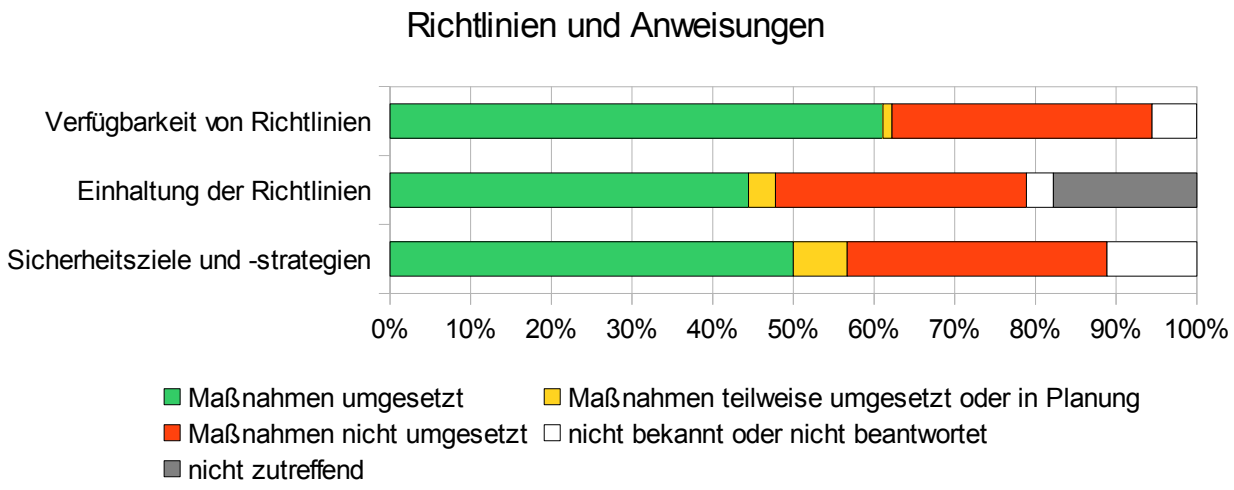


Abbildung 19: Auswertung Richtlinien und Anweisungen

Im Rahmen der Studie wurde nach der Verfügbarkeit der folgenden Richtlinien gefragt:

- Sicherheitsrichtlinie für Besucher
- Sicherheitsrichtlinie für Fremdpersonal
- Regelungen zum Informationsaustausch
- Richtlinie zur Verwendung von Wechselmedien
- Sicherheitsrichtlinie für Patch-/Update-Management
- Sicherheitsrichtlinie zum Arbeitsplatz
- Sicherheitsrichtlinie zur Internet- und E-Mail-Nutzung
- Sicherheitsrichtlinie zum mobilen Arbeiten und Telearbeit
- Sicherheitsrichtlinie zur Telefonarbeit.

Insgesamt kann festgestellt werden, dass diese Richtlinien bei rund zwei Drittel der befragten Unternehmen verfügbar sind. Jedoch sind große Unterschiede in der Verfügbarkeit einzelner Richtlinien feststellbar, wie der nachfolgenden Abbildung 20 zu entnehmen ist.

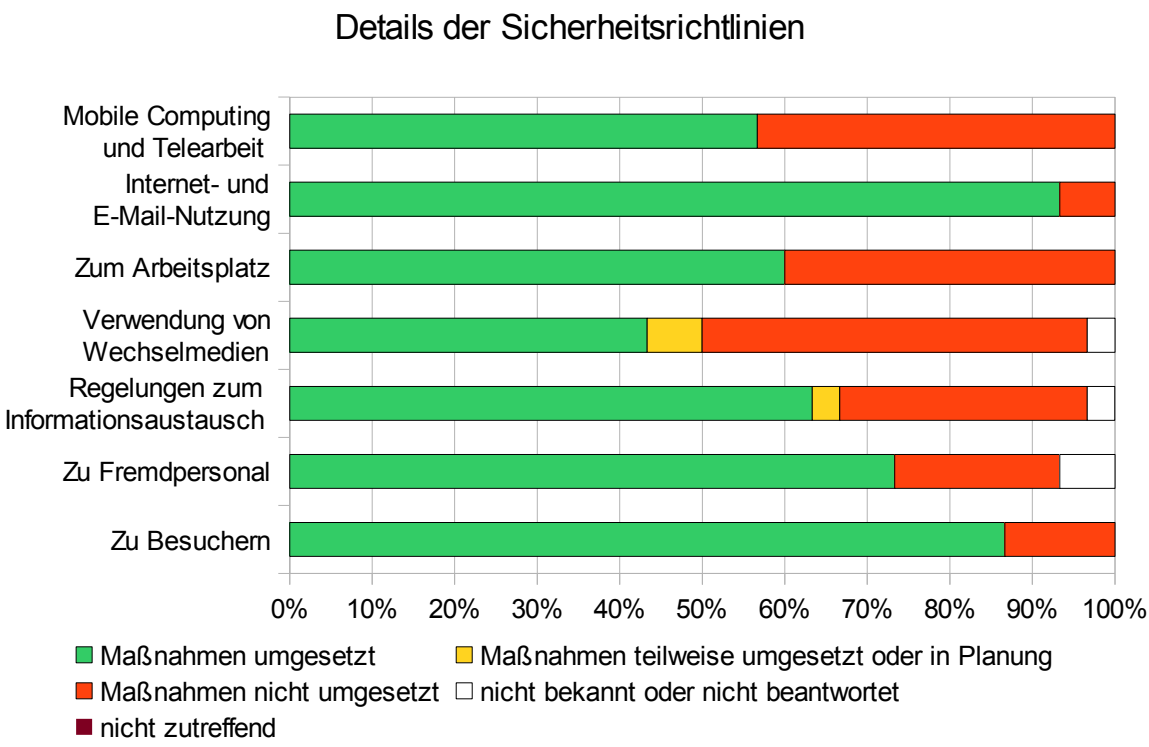


Abbildung 20: Detaillierte Betrachtung der Sicherheitsrichtlinien

Positiv hervorzuheben ist, dass die Sicherheitsrichtlinien zu Besuchern sowie der Internet- und E-Mail-Nutzung Standard in den Unternehmen sind. Allerdings sind erste Defizite bereits bei den Regelungen zu Fremdpersonal, den Richtlinien zum Informationsaustausch und den Anweisungen zum Arbeitsplatz zu erkennen.

Während drei Viertel der Unternehmen angaben, dass im Durchschnitt 24 Prozent der mobilen Endgeräte außerhalb des Unternehmens zum Einsatz kommen, sind Regelungen hierzu nur bedingt verfügbar. So ist eine Richtlinie zur Verwendung von Wechselmedien wie z.B. USB-Sticks nur bei 43 Prozent und zu „Mobile Computing und Telearbeit“ nur bei etwas mehr als 50 Prozent der Unternehmen verfügbar.

Ein angemessenes Sicherheitsniveau kann für die mobilen Endgeräte somit nicht zuverlässig sichergestellt werden. Auch über die Bedrohungen durch den Einsatz von Wechselmedien sowie die im Unternehmen etablierten Schutzmaßnahmen werden die Mitarbeiter nur eingeschränkt informiert.

Des Weiteren ist bei der Informationserhebung festgestellt worden, dass viele der genannten Richtlinien nicht als einzelne Dokumente verfügbar sind, sondern als Gesamtwerk im Unternehmen existieren. Die einzelnen Richtlinien sind somit nicht immer strikt voneinander abzugrenzen.

Die Verfügbarkeit von Richtlinien impliziert auch die regelmäßige Überprüfung in Hinblick auf:

1. Eignung der Richtlinie für den Einsatz
2. Einhaltung der Richtlinie durch die betroffenen Mitarbeiter

Eine fortlaufende Prüfung der vorhandenen Richtlinien auf weitergehende Eignung wird von 56 Prozent der Unternehmen durchgeführt. Dies bedeutet, dass nahezu jedes zweite Unternehmen auf eine Eignungsprüfung verzichtet. In vielen Fällen wird dies damit begründet, dass eine Anpassung der Richtlinien eher reaktiv auf Änderungen im Unternehmen erfolge.

Eine Prüfung auf Einhaltung der Richtlinien wird von rund der Hälfte der Unternehmen durchgeführt. Bei jedem zweiten Unternehmen besteht die Gefahr, dass das Sicherheitsniveau durch uninformierte Mitarbeiter gesenkt werden könnte.

Die Sicherheitsziele und -strategien sind die Basis für einen ordnungsgemäßen Umgang mit Informationen innerhalb aller Geschäftsprozesse sowie zur Realisierung von Sicherheitsmaßnahmen und -prozessen im Unternehmen. Diese sind in weniger als zwei Drittel der Unternehmen festgelegt. Rund die Hälfte der Unternehmen gab an, dass Ziele und Strategien auch durch die Unternehmensleitung unterschrieben sind. Weniger als die Hälfte der Unternehmen hat die Mitarbeiter auf die Sicherheitsziele und -strategien hingewiesen. Dies macht deutlich, dass das Thema ausschließlich durch die IT-Leitung, ggf. in Abstimmung mit der Unternehmensleitung, bearbeitet wird. Allerdings wurde aus den Gesprächen deutlich, dass viele Unternehmen diese Sicherheitsziele und -strategien auf Basis bestehender Leitlinien realisiert haben.

4.6.3 Handlungsempfehlungen

Kurzfristig sollte jedes Unternehmen eine Bestandsaufnahme durchführen und die Verfügbarkeit von Richtlinien und Anweisungen prüfen.

Zusätzlich können kurzfristig stichprobenartige Prüfungen auf Einhaltung durch die Mitarbeiter durchgeführt werden. Dies zeigt den Verantwortlichen den Kenntnisstand des Personals sowie den Umsetzungsgrad der bestehenden Richtlinien auf und gibt Hinweise auf fehlende Praxistauglichkeit. Darüber hinaus reaktiviert diese Vorgehensweise das Bewusstsein der Mitarbeiter in Bezug auf die im Unternehmen gültigen Richtlinien und Anweisungen.

Mittelfristig sind fehlende Sicherheitsrichtlinien zu ergänzen bzw. zu aktualisieren. Damit können technische Lücken durch organisatorische Maßnahmen geschlossen werden. Die Bereitstellung neuer bzw. aktualisierter Richtlinien sollte allen Mitarbeitern bekannt gegeben werden. Dies kann beispielsweise initial im Rahmen einer Schulung und zu einem späteren Zeitpunkt zur Auffrischung per E-Mail erfolgen.

Langfristig muss ein Prozess zur regelmäßigen Prüfung und Aktualisierung von Richtlinien und Anweisungen etabliert werden. Nur so können diese einen Mehrwert für das Unternehmen darstellen. Dazu gehört auch die Definition der Sicherheitsziele und -strategien, die von IT-Leitung und Unternehmensleitung gemeinschaftlich erarbeitet und durch die Unternehmensleitung verabschiedet werden muss.

4.7 Infrastruktur

Ein Gebäude umgibt die stationären Arbeitsplätze, die verarbeiteten Informationen sowie die aufgestellte Informationstechnik und gewährleistet für diese somit einen äußeren Schutz. Der Zutritt zu schutzbedürftigen Gebäudeteilen und Räumen ist zu regeln und zu kontrollieren.

4.7.1 Themen in den Interviews

Für eine Einschätzung der Umsetzung der Schutzmaßnahmen in der Infrastruktur werden die folgenden Gesichtspunkte betrachtet:

- **Zutrittskontrollanlage:** Gebäude bilden den äußeren Rahmen, um Geschäftsprozesse durchführen zu können. Die stationären Arbeitsplätze, die verarbeiteten Informationen sowie die aufgestellte Informationstechnik werden durch diese geschützt. Der Zutritt zu schutzbedürftigen Gebäudeteilen und Räumen ist zu regeln und zu kontrollieren. Die Maßnahmen reichen dabei von einer einfachen Schlüsselvergabe bis zu aufwendigen Identifizierungssystemen. Die Umsetzung dieser Sicherheitsmaßnahmen zum Schutz vor unberechtigtem Zutritt wird geprüft.
- **Serverraum:** Ein Serverraum ist kein ständig besetzter Arbeitsplatz, er wird nur sporadisch und zu kurzfristigen Arbeiten betreten. Zu beachten ist jedoch, dass im Serverraum aufgrund der Konzentration von IT-Geräten und Daten ein deutlich höherer Schaden eintreten kann als zum Beispiel in einem Büroraum. Diese IT-Systeme bedürfen besonderem Schutz. Eine Schutzmaßnahme ist, die Räumlichkeiten, in denen sich die IT-Systeme befinden, vor unberechtigtem Zutritt zu schützen. Neben den Maßnahmen zum Schutz gegen Manipulation werden ebenfalls die Mechanismen gegen Ausfall der IT-Systeme durch höhere Gewalt untersucht.
- **Besprechungs-, Veranstaltungs- und Schulungsräume:** In Besprechungs-, Veranstaltungs- und Schulungsräumen halten sich sehr häufig unternehmensfremde Personen auf. Diese sind bereits an den äußeren Schutzmaßnahmen vorbeigeführt worden. Aufgrund der IT-basierten Geschäftsprozesse stellen ungesicherte Netzwerkdosen daher ein Sicherheitsrisiko dar. Im Rahmen der Studie wird die Sicherung der Netzwerkanschlüsse in diesen Räumlichkeiten sowie Regelungen zur Begleitung und Beaufsichtigung unternehmensfremder Personen geprüft.
- **Büroräume:** Der Büroraum ist ein Raum, in dem sich ein oder mehrere Mitarbeiter aufhalten, um dort der Erledigung ihrer Aufgaben eventuell auch IT-unterstützt nachzugehen. Insbesondere wird hier die Sicherung der Netzwerkanschlüsse in den Büroräumen geprüft.

4.7.2 Ergebnisse

Das zusammenfassende Ergebnis zur Infrastruktur ist in Abbildung 21 dargestellt.

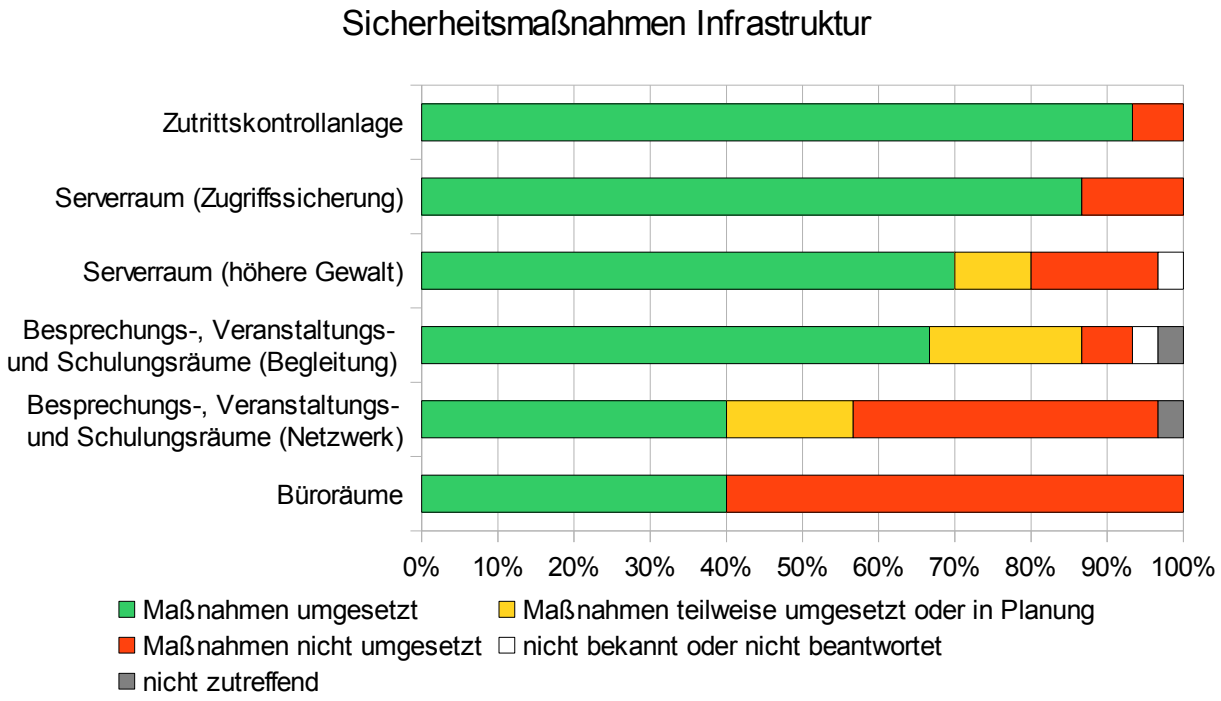


Abbildung 21: Auswertung Infrastruktur

Die Ergebnisse zur Infrastruktur zeigen einen hohen Umsetzungsgrad der Schutzmaßnahmen im Rahmen der Zutrittskontrollanlagen. Danach haben nur zwei der besuchten Unternehmen aktuell keine effektive Zutrittskontrolle umgesetzt. Die weiteren Unternehmen setzen in 21 Fällen auf eine automatisierte Zutrittskontrollanlage, während sieben Unternehmen ausschließlich eine personell gestützte Zutrittskontrolle nutzen. Bei mehr als der Hälfte der befragten Unternehmen sind die baulichen Gegebenheiten derart gestaltet, dass der Zugang zu den Gebäuden zusätzlich durch eine Umzäunung gesichert werden konnte.

Die Serverräume werden in 29 Fällen von den Unternehmen selbst betrieben. In fünf dieser Unternehmen werden zusätzlich Kapazitäten externer Dienstleister in der Bereitstellung von Rechenzentrumsdienstleistungen genutzt. Lediglich ein Unternehmen hat den Betrieb der Server vollständig an einen externen Dienstleister ausgelagert. Der Zutritt zu den Serverräumen wird in 90 Prozent durch Zutrittskontrollanlagen gesichert. Bei zwölf Unternehmen werden hierfür Schließsysteme genutzt.

Eine weitere Gefahrenquelle stellt der Ausfall der IT-Systeme durch höhere Gewalt dar. Um jederzeit einen zuverlässigen Betrieb der Systeme gewährleisten zu können, sind entsprechende Maßnahmen zum Schutz der Serverräume vor höherer Gewalt umzusetzen. Dies setzen 70 Prozent der Unternehmen vollständig um. Knapp 20 Prozent der Unternehmen gaben an, zum Schutz gegen höhere Gewalt keine Maßnahmen umgesetzt zu haben. Dies ist auch vor dem Hintergrund bedenklich, dass einzelne Unternehmen von Vorfällen aufgrund höherer Gewalt berichteten.

Besprechungs-, Veranstaltungs- und Schulungsräume zeichnen sich im Wesentlichen dadurch aus, dass sie von wechselnden Personen bzw. Personenkreisen genutzt werden. Besonders die Nutzung durch Externe erfordert die Umsetzung weiterer Schutzmaßnahmen. Eine Schutzmaßnahme ist die dauerhafte Begleitung auf dem Weg in diese Räumlichkeiten und während des Aufenthaltes. Dies

schreiben rund zwei Drittel der Unternehmen vor. Da es sich um eine organisatorische Schutzmaßnahme handelt, die aufgrund besonderer Anlässe unter Umständen nicht berücksichtigt wird, sollten zusätzliche technische Maßnahmen, wie zum Beispiel der Schutz der Netzwerkanschlüsse, erfolgen. Dies wird von 40 Prozent der Unternehmen geeignet umgesetzt. Jedes sechste Unternehmen setzt die erforderlichen Maßnahmen nur teilweise um, so dass ein unberechtigter Zugriff auf das interne Netzwerk und die Daten des Unternehmens nicht ausgeschlossen werden kann.

Die Absicherung des Netzwerkes in den Büroräumen erfolgt in vergleichbarer Weise. Des Weiteren haben 60 Prozent der Unternehmen Richtlinien in Bezug auf den Arbeitsplatz und die Abwesenheit der Mitarbeiter definiert. Diese regeln die Aufbewahrung von Dokumenten und Daten sowie die Frage, ob Büros bei Abwesenheit der Mitarbeiter grundsätzlich zu verschließen sind.

Insgesamt zeigt sich aus der Grafik, dass den Bedrohungen durch äußere Angriffe auf die Infrastruktur durch Umsetzung einer Vielzahl von Schutzmaßnahmen Rechnung getragen wird. Die Abbildung 21 zeigt aber auch, dass die Schutzmaßnahmen abnehmen, je weiter eine Person in die Räume eines Unternehmens vordringen kann.

4.7.3 Handlungsempfehlungen

Die Absicherung der stationären Arbeitsplätze, der verarbeiteten Informationen sowie der aufgestellten Informationstechnik erfolgt durch die umgebenden Gebäude. Diese gewährleisten somit einen äußeren Schutz und ermöglichen es, den Zutritt zu schutzbedürftigen Gebäudeteilen und Räumen zu regeln und zu kontrollieren.

Erstes Ziel externer Angriffe auf das Unternehmen ist der unberechtigte Zutritt zu den Gebäuden. Daher ist eine Form der Zutrittskontrolle für jedes Unternehmen unabdingbar. Dies kann – sofern baulich keine technische Lösung möglich ist – durch personelle Maßnahmen umgesetzt werden. Die Umsetzung sollte kurzfristig erfolgen. Hierzu kann das bestehende Personal genutzt werden. Langfristig sollte die Umsetzung einer automatisierten Zutrittskontrollanlage angestrebt werden. Generell ist darauf zu achten, dass der Zutritt nur für berechtigte Personen autorisiert wird. Sofern die Möglichkeiten gegeben sind, können unterstützende Perimeterschutzmaßnahmen, wie beispielsweise ein Zaun, umgesetzt werden. Dies hat bauliche Veränderungen an der Infrastruktur zur Folge und kann nur mit einer längerfristigen Planung umgesetzt werden.

In Gebäuden, die durch mehrere Unternehmen gemeinschaftlich genutzt werden, ist es erforderlich, die Räumlichkeiten des eigenen Unternehmens klar abzugrenzen. Insbesondere auf die Sicherung der Notausgänge gegen unberechtigte Nutzung, zum Beispiel durch Verwendung einer Gefahrenmeldeanlage, ist zu achten. Dies ist durch einen Sicherheitsprozess regelmäßig zu überprüfen.

Der Schutz der Serverräume gegen unberechtigten Zutritt kann durch die Umsetzung folgender Maßnahmen erreicht werden:

- Mechanisches Schließsystem
- PIN und/oder Keycard
- Videoüberwachung
- Biometrische Merkmale

Eine Möglichkeit, den Zutrittsschutz kurzfristig zu realisieren, ist die Verwendung eines mechanischen Schließsystems. Dies setzt voraus, dass der Serverraum als eine abgetrennte Räumlichkeit für IT-Systeme existiert. Alle weiteren genannten Schutzmaßnahmen können aufgrund ihrer Komplexität nur mittel- bis langfristig realisiert werden.

IT-Systeme sollten in einem geeigneten Raum mit entsprechenden Schutzmaßnahmen betrieben werden. Zu diesen Schutzmaßnahmen gehören die folgenden:

- **Brandmeldeanlage** – zur Meldung von überhöhter Temperatur und Feuer im Serverraum.
- **Handfeuerlöscher** – zur Behebung kleinerer Brände durch das Personal im Unternehmen. Hierbei sollte auf die geeignete Handfeuerlöscherklasse geachtet werden.
- **Vermeidung von wasserführenden Leitungen in der Nähe des Serverraumes** – zum Schutz vor möglichen Wasserschäden.
- **Klimatisierung** – zum Schutz vor Überhitzung in abgeschlossenen Räumlichkeiten, in denen technische Infrastruktur betrieben wird.
- **Fernmeldeanlage** – zur Weitergabe von Störungsmitteilungen. Besonders wichtig ist dies, sofern das Unternehmen oder eine Wachzentrale nicht 24 Stunden täglich und sieben Tage die Woche durch qualifiziertes Personal besetzt ist.

Sofern diese Maßnahmen nicht schon für die bestehenden Serverräume realisiert sind, sollte kurzfristig auf alternative Räumlichkeiten, die dem Schutzbedarf eher entsprechen ausgewichen werden. Ist eine solche Räumlichkeit nicht verfügbar, sollte mittelfristig entsprechende Räumlichkeiten aufgebaut oder die Auslagerung an einen geeigneten Dienstleister erwogen werden.

Um ein Unternehmen zu schützen, müssen die öffentlichen Besprechungs-, Veranstaltungs- und Schulungsräume, die durch unternehmensfremde Personen genutzt werden können, zusätzlich gesichert werden. Insbesondere ungesicherte Netzwerkdosen stellen hierbei ein Sicherheitsrisiko dar. Hierüber können Zugriffe auf IT-Systeme des Unternehmens erfolgen, die Sicherheitsvorfälle oder Notfälle zur Folge haben können. Aus dieser Nutzung heraus ergibt sich eine Gefährdungslage, die kaum mit der anderer Räume vergleichbar ist. Das Hauptaugenmerk ist dabei, neben den üblichen Gefährdungen für Räume aller Art, die Gefährdung durch den "Spieltrieb" anwesender und unbeobachteter Personen. Die Schutzmaßnahmen für Besprechungs-, Veranstaltungs- und Schulungsräume können kurzfristig realisiert werden. Eine erste Maßnahme kann die Trennung der beschalteten aber ungesicherten Netzwerkanschlüsse vom internen Netzwerk des Unternehmens sein. Alternativ kann die Aufschaltung eines, vom internen Netz, isolierten Gastnetzes als geeignete Maßnahme angesehen werden.

Weiterhin sind alle Mitarbeiter darauf hinzuweisen, welche Räumlichkeiten für unternehmensfremde Personen offenstehen. Mittelfristig muss diese Anweisung in Form von Richtlinien dokumentiert und den Mitarbeitern zur Kenntnis gebracht werden. Langfristig ist ein Konzept zur Absicherung der Netzwerkanschlüsse im Unternehmen zu realisieren. Hierbei empfiehlt sich, dedizierte Gastnetzwerke zu definieren, welche strikt vom Unternehmensnetzwerk zu trennen sind.

Für die Belegung der Netzwerkdosen in den Büroräumen gelten ähnliche Regelungen. Es sollten auch hier ungenutzte Netzwerkanschlüsse nicht dauerhaft beschaltet sein. Diese Schutzmaßnahme kann kurzfristig realisiert werden und stellt eine Art des Grundschutzes dar.

Die regulär genutzten Netzwerksanschlüsse sind darüber hinaus derart zu sichern, dass diese nur durch berechtigte IT-Komponenten genutzt werden können. Diese Maßnahme wäre auch geeignet,

um von Mitarbeitern mitgebrachte private IT-Endgeräte an der Nutzung des Netzwerks zu hindern. Hierfür müssen weitere Schutzmaßnahmen mittel- bis langfristig umgesetzt werden, so beispielsweise eine MAC-Adressenfilterung oder höherwertige Authentifizierungsmaßnahmen wie Network Access Control (NAC).

4.8 IT-Systeme

Informationen sind ein wesentlicher Wert für Unternehmen und Behörden und müssen daher angemessen geschützt werden. Die meisten Informationen werden heutzutage mit Informationstechnik (IT) erstellt, gespeichert, transportiert oder weiterverarbeitet. Moderne Geschäftsprozesse sind heute in Wirtschaft und Verwaltung ohne IT-Unterstützung längst nicht mehr vorstellbar. Eine zuverlässig funktionierende Informationsverarbeitung ist ebenso wie die zugehörige Technik für die Aufrechterhaltung des Betriebes unerlässlich. Unzureichend geschützte Informationen stellen einen häufig unterschätzten Risikofaktor dar, der für manche Unternehmen existenzbedrohend sein kann. Dabei ist ein vernünftiger Informationsschutz ebenso wie eine Grundsicherung der IT schon mit verhältnismäßig geringen Mitteln zu erreichen.

4.8.1 Themen in den Interviews

Für die Ermittlung des Schutzes der IT-Systeme wurden die folgenden Kriterien im Rahmen der Studie betrachtet:

- **Einsatz geeigneter Authentisierungsverfahren:** IT-Systeme aller Art sollten grundsätzlich sicherstellen, dass sich alle Benutzer, die darauf zugreifen möchten, authentisieren müssen. Es wird daher geprüft, ob geeignete Authentisierungsverfahren und Nutzungsrichtlinien in den Unternehmen etabliert sind.
- **Sicherung von Geräteschnittstellen:** Über die Geräteschnittstellen jedes IT-Systems können Daten eingebracht bzw. auf andere IT-Systeme oder Speichermedien übertragen werden. Besonders gefährdet sind die Geräteschnittstellen, die nicht durch die Infrastruktur des Unternehmens geschützt werden. Um das Unternehmen vor diesem Problem zu schützen, können organisatorische oder technische Schutzmaßnahmen umgesetzt werden. Die Umsetzung der Schutzmaßnahmen in den befragten Unternehmen wird in diesem Kriterium genauer betrachtet.
- **Einsatz von Speichermedienverschlüsselung:** Um zu verhindern, dass trotz aller Vorsichtsmaßnahmen von einem gestohlenen tragbaren IT-System schutzbedürftige Daten ausgelesen werden können, sollte ein Verschlüsselungsprogramm eingesetzt werden. Dies gilt ebenfalls für alle Speichermedien, die sich zeitweise außerhalb des Unternehmens befinden.
- **Klassifikation der Unternehmensdaten:** Anhand einer Risikobetrachtung der Daten und Informationen sollte deren Relevanz für das Unternehmen eingestuft und der entsprechende Schutzbedarf ermittelt werden. Auf Grundlage dieser Ergebnisse sollten die Daten klassifiziert werden. Hieraus sollten entsprechende Zugriffsregelungen oder auch Infrastrukturmaßnahmen, wie beispielsweise der Aufbau isolierter Netzwerkbereiche, abgeleitet werden.

- **Auswertung von Log-Daten:** Das Auswerten von Log-Daten ist eine Kontrollmaßnahme zur Überprüfung von IT-Systemen. Um eine umfassende Übersicht über alle Systeme zu gewährleisten, sollten auf allen IT-Systemen Log-Daten geschrieben und entsprechend ausgewertet werden. Da Abweichungen sporadisch auftreten, sollten die Auswertungen in regelmäßigen Abständen durchgeführt werden.
- **Redundanz kritischer IT-Systeme:** Die Verfügbarkeit der IT-Systeme ist elementar für die Durchführung von Geschäftsprozessen. Dabei sind besonders die kritischen IT-Systeme so zu betreiben, dass ein Ausfall vermieden wird.

4.8.2 Ergebnisse

Die Ergebnisse für die befragten Unternehmen sind in der Abbildung 22 zusammengefasst.

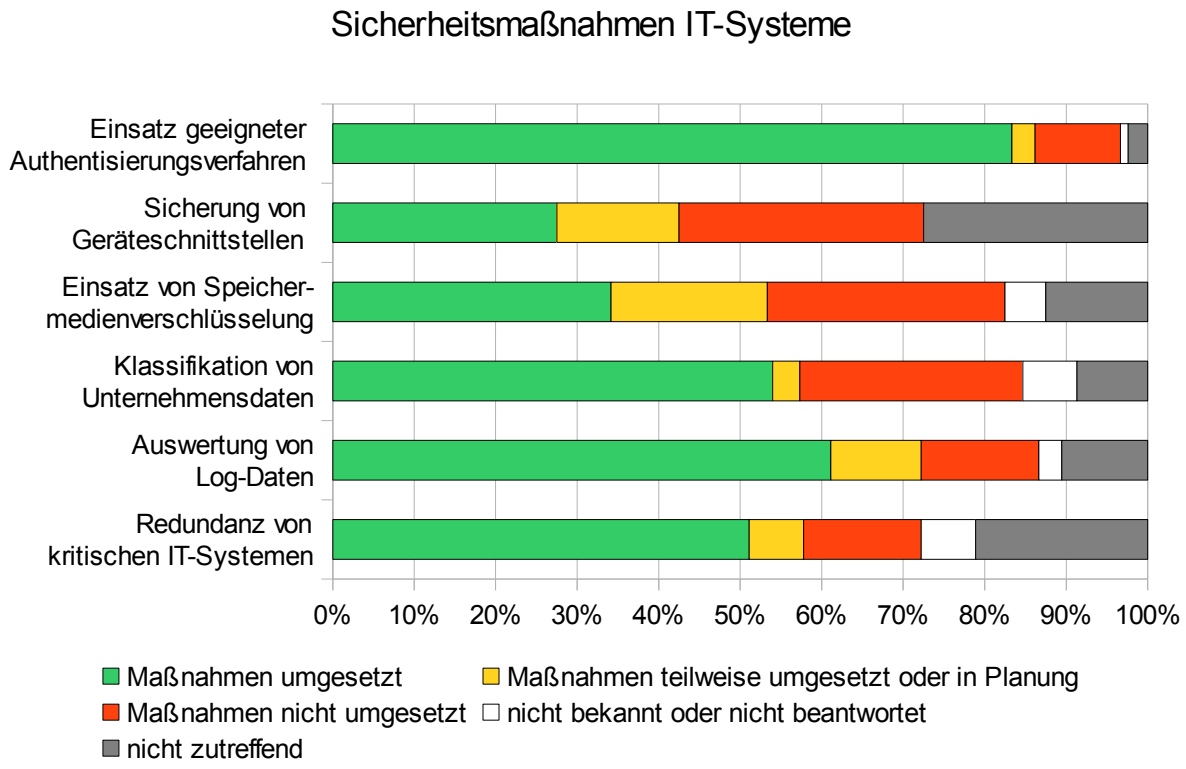


Abbildung 22: Auswertung IT-Systeme

Die befragten Unternehmen setzen die Sicherheitsmaßnahmen zum Schutz der IT-Systeme nur teilweise um. Aus der Ergebnisdarstellung in Abbildung 22 wird deutlich, dass ein geeignetes Authentisierungsverfahren von mehr als 80 Prozent der Unternehmen umgesetzt wird. Dies erfolgt hauptsächlich durch eine Authentisierung mit Benutzernamen und Passwort. Als zentrales Authentifizierungssystem setzen die Unternehmen mehrheitlich ein Active-Directory-System ein.

Die technische Umsetzung einer Authentisierungsmaßnahme ist jedoch nicht ausreichend. Eine Richtlinie für die Zuweisung von Benutzerrechten haben rund 80 Prozent der Unternehmen umgesetzt, wobei diese nur von 63 Prozent in regelmäßigen Abständen geprüft und aktualisiert wird. Auch die Qualität von Passwörtern kann eine Aussage über die Eignung der Authentisierung

geben. Nach IT-Grundschutz „M 2.11 Regelung des Passwortgebrauchs“ [BSI_2011] wird eine Mindestlänge von 8 Zeichen bei einem Wechselintervall von 90 Tagen für den normalen Schutzbedarf als ausreichend angesehen.

Insgesamt prüfen zwei Drittel der Unternehmen auf die Verwendung von schwachen Passwörtern. Eine Mindestlänge der Passwörter wird von 26 Unternehmen eingefordert. Die Bandbreite liegt hierbei zwischen fünf und zwölf Zeichen. In zwei Drittel der Unternehmen ist eine Mindestlänge von acht Zeichen definiert. Einen regelmäßigen Wechsel der Passwörter sehen dabei 23 Unternehmen vor. Als Intervall werden Werte zwischen 30 Tagen und einem Jahr angegeben. In elf Unternehmen beträgt das Wechselintervall 90 Tage.

Mehr als die Hälfte der befragten Unternehmen hat technische oder organisatorische Schutzmaßnahmen zur Sicherung der Geräteschnittstellen etabliert. Eine vollständige Sicherung aller Schnittstellen wird von rund sieben Prozent der Unternehmen erreicht. In den anderen Unternehmen werden ausgesuchte Geräteschnittstellen gesichert. Als Grund für die fehlenden oder nur teilweise umgesetzten Schutzmaßnahmen wurde von den befragten Unternehmen angegeben, dass die Benutzbarkeit der Systeme höher bewertet werde als die Sicherheit.

Besonders mobile Speichermedien und IT-Endgeräte sind dem Risiko ausgesetzt, dass diese dem rechtmäßigen Nutzer entwendet werden. In unberechtigter Hand und mit ausreichend Zeit ist davon auszugehen, dass die Daten gelesen oder manipuliert werden können. Um dieses Szenario zu vermeiden, wird die Schutzmaßnahme der Speichermedienverschlüsselung von knapp zwei Drittel der Unternehmen aktiv eingesetzt. Kein Unternehmen schützt alle Speichermedien. Eine Festplattenverschlüsselung auf Laptops haben über die Hälfte der Unternehmen im Einsatz. Wechselmedien wie z.B. USB-Sticks werden von 20 Prozent der Betriebe verschlüsselt. Die Dokumentation der entsprechenden Maßnahmen führen weniger als die Hälfte der Unternehmen durch. Obwohl ein Bewusstsein für sensible Daten in den befragten Unternehmen vorhanden ist, werden die entsprechenden Schutzmaßnahmen nicht in einem ausreichenden Maß ergriffen.

Dass risikobehaftete Daten im Unternehmen vorhanden sind, wurde von 90 Prozent der befragten Unternehmen bejaht. Im Gegensatz dazu werden entsprechende Handlungen zur Klassifikation der risikobehafteten Daten jedoch nur von der Hälfte der Unternehmen vorgenommen. Ein geringer Teil der Befragten gab an, dass eine Umsetzung sich in Planung befindet. Die Separierung der Daten auf getrennte Systeme nimmt ebenfalls knapp über die Hälfte der Unternehmen vor. Eine entsprechende aktualisierte Dokumentation zur Klassifizierung liegt nur bei 40 Prozent der Unternehmen vor. Trotz vorhandenem Bewusstsein werden lediglich in 50 Prozent der Unternehmen Maßnahmen zur Klassifikation oder Separierung risikobehafteter Daten umgesetzt.

Die Erkennung von Funktionsstörungen oder Vorfällen erfolgt durch das Auswerten von Log-Daten im Unternehmen. So werten grundsätzlich 97 Prozent der Unternehmen ihre Log-Daten aus. Bei der Art der Auswertung sind jedoch qualitative Unterschiede festzustellen. So werten knapp 17 Prozent der Unternehmen ihre Log-Daten vollautomatisiert aus, während die restlichen Betriebe die Auswertung hauptsächlich manuell und in wenigen Fällen teilautomatisiert durchführen. Die Log-Daten werden bei 20 Prozent der Unternehmen ausschließlich zentral und bei zwei Drittel der Unternehmen ausschließlich dezentral protokolliert. Drei Unternehmen gaben an, dass sie eine Mischform aus zentraler und dezentraler Protokollierung im Unternehmen anwenden. Die Systemzeit kann gerade bei einer dezentralen Protokollierung einen entscheidenden Hinweis auf Unregelmäßigkeiten geben. Diese wird bei 97 Prozent der Unternehmen regelmäßig abgeglichen. Nachdem ein Hinweis in den Log-Daten entdeckt wurde, müssen Konsequenzen folgen. Hier haben 93 Prozent der Unternehmen einen entsprechenden Meldeweg etabliert bzw. können diese

Information an die zuständige Person weitergegeben. Eine entsprechende Dokumentation zur Auswertung von Log-Daten haben nur 20 Prozent der Unternehmen.

Ein wichtiger Faktor für die Durchführung von Geschäftsprozessen ist die Verfügbarkeit von IT-Systemen. Besonders die kritischen IT-Systeme sollten dabei redundant betrieben werden. Dies erfolgt bei zwei Drittel der Unternehmen. Dabei betreiben zehn Unternehmen die redundanten Systeme am gleichen Standort in einem anderen Gebäude und drei Unternehmen an einem externen Standort. Der Datenabgleich erfolgt bei 18 Unternehmen permanent und bei einem Unternehmen automatisch in Intervallen. Alle weiteren Unternehmen nehmen den Datenabgleich manuell vor.

Insgesamt zeigt sich aus der Grafik, dass die Schutzmaßnahmen zur Absicherung von Geräteschnittstellen sowie die zur Speichermedienverschlüsselung nicht ausreichend in den Unternehmen umgesetzt sind. Des weiteren besteht Handlungsbedarf bei der Klassifikation risikobehafteter Daten und dem redundanten Betrieb kritischer IT-Systeme.

4.8.3 Handlungsempfehlungen

IT-Systeme aller Art sollten grundsätzlich sicherstellen, dass sich alle Benutzer, die darauf zugreifen möchten, authentisieren müssen. Nur so kann verhindert werden, dass unautorisierte Personen Zugriff auf die Dienste erlangen, die das System anbietet, oder auf die Daten, die auf dem System gespeichert sind. Für den Schutz der IT-Systeme sollten nicht nur technisch, sondern auch qualitativ hinreichend gute Sicherheitsmaßnahmen etabliert werden. Eine kurzfristige und mit geringem Aufwand zu realisierende Maßnahme ist die Anhebung der Mindestlänge bei Passwörtern auf acht Zeichen in Verbindung mit einem Wechselintervall von maximal 90 Tagen, wie in IT-Grundschutz „M 2.11 Regelung des Passwortgebrauchs“ [BSI_2011] empfohlen. Diese ist mit einer Überprüfung auf schwache Passwörter bei der Erstellung zu verbinden. Diese Kombination der Sicherheitsmechanismen verhindert zuverlässig das Durchprobieren von Passwörtern (auch mit technischen Mitteln). Die Mitarbeiter sollten zur Nutzung und auf den Umgang mit Passwörtern hingewiesen und zu einem sicheren Umgang verpflichtet werden. Die Notwendigkeit hierzu kann durch Schulungsmaßnahmen unter der Verwendung von Beispielen sehr deutlich dargestellt werden.

Über die Geräteschnittstellen jedes IT-Systems können Daten eingebracht bzw. auf andere IT-Systeme oder Speichermedien übertragen werden. Besonders gefährdet sind die Geräteschnittstellen, die nicht durch die Infrastruktur des Unternehmens geschützt werden. Dies trifft besonders auf die mobilen IT-Systeme zu. Die standardisierten und generalisierten Schnittstellen, wie beispielsweise USB oder Bluetooth, sind hierbei besonders gefährdet. Es könnte zum Beispiel unkontrolliert Software von externen Systemen oder Laufwerken eingespielt werden oder Daten unberechtigt und unbemerkt auf Wechselmedien kopiert werden. Um das Unternehmen vor diesem Problem zu schützen, können organisatorische oder technische Schutzmaßnahmen umgesetzt werden. Es sollte kurzfristig eine organisatorische Anweisung erfolgen, dass die Geräteschnittstellen nicht ohne Bedenken genutzt werden sollten. Sofern die Geschäftsprozesse es ermöglichen, sollten alle Geräteschnittstellen bei einem Einsatz der IT-Systeme außerhalb des Hauses geschützt werden. Mittelfristig können technische Maßnahmen die Geräteschnittstellen sichern. Sofern der Bedarf an beliebigem Austausch von Daten im Rahmen der Geschäftsprozess besteht, können Präventivmaßnahmen für den Schutz des Unternehmensnetzes erfolgen. So entwickelte das BSI im Rahmen des Projekts Janus eine Wechseldatenträgerschleuse, welche die Wechselmedien vor der Datenübernahme in das Unternehmensnetz auf mögliche Gefährdungen prüft (vgl. Kapitel 6 - Abschnitt „Device-Sicherheit“). Dies kann auch manuell durch einen separaten Rechner, beispielsweise in der IT-Leitung, erfolgen. Dieser Rechner ist nur an ein

Gastnetz angeschlossen und besitzt aktuelle Virenscanner, um eine Überprüfung der Wechseldatenträger zu ermöglichen.

Gegen den Verlust von Daten sollte kurzfristig eine Speichermedienverschlüsselung für Wechseldatenträger sowie die mobilen Endgeräte eingesetzt werden. Hier sind verschiedene Angebote auf dem Markt verfügbar. Dieses sollte sobald als möglich zu einer Komplettdatenverschlüsselung ausgebaut werden, um im Falle der mobilen Endgeräte neben den Nutzdaten auch die Betriebssystemdaten zu schützen.

Ein Unternehmen verwaltet auf den IT-Systemen eine Vielzahl von Daten. Diese haben unterschiedliche Wichtigkeiten für das Unternehmen. Anhand einer Risikobetrachtung der Daten und Informationen muss deren Relevanz für das Unternehmen eingestuft und der entsprechende Schutzbedarf ermittelt werden. Nicht jeder Mitarbeiter muss alle Daten lesen oder verändern können. Für eine Klassifizierung von Daten sollten mindestens die folgenden Merkmale festgelegt werden:

- Dateneigentümer wie beispielsweise technischer Leiter und Geschäftsführung
- Zugriffsrechte hinsichtlich des Lesens von Daten beispielsweise für jedermann oder bestimmte Mitarbeiter
- Geheimhaltungsstufe wie beispielsweise allgemein zugänglich, intern, unternehmenskritisch oder personenbezogen

Auf Basis dieser Merkmale können Klassifikationen vorgenommen werden. Das Bewusstsein für den Umgang mit risikobehafteten Daten sollte im Unternehmen geschaffen werden. Weiterhin sollten risikobehaftete Daten auf separierten Systemen verwaltet werden.

Das Auswerten von Log-Daten der Rechner ist elementar für das Erkennen von Störungen oder Vorfällen. Um eine umfassende Übersicht über alle Systeme zu gewährleisten, müssen auf allen IT-Systemen Log-Daten geschrieben und entsprechend ausgewertet werden. Nur so können Abweichungen im laufenden Betrieb der IT-Systeme identifiziert werden, die auf fehlenden bzw. fehlerhaften Programmen basieren oder durch Sicherheitslücken zustande kommen. Da diese Abweichungen sporadisch auftreten, sollte die Auswertung regelmäßig und zeitnah zu Meldungen erfolgen, die über zentrale Kontaktstellen eingehen. Unterstützend können hierfür Softwaresysteme eingesetzt werden. Optimal ist eine zentrale Protokollierung mit einer automatisierten Auswertung und einer Fernmeldefunktion. Somit werden die Verantwortlichen zeitnah über Störungen und Vorfälle informiert. Diese Umsetzung der Lösung kann jedoch nur mittel- bis langfristig angestrebt werden.

Langfristig sollte das Betreiben redundanter IT-Systeme angestrebt werden. Bis dahin muss das Risiko für das Unternehmen tragbar sein, denn ein Betreiben von redundanten Systemen mit einem permanenten oder automatisiert in Intervallen durchgeführten Abgleich bedarf zusätzlicher Hardware und eines Konzepts zur Realisierung.

Alle Sicherheitsmaßnahmen zu den IT-Systemen sollten mittel- bis langfristig dokumentiert und in regelmäßigen Abständen aktualisiert werden. Somit kann die Nachvollziehbarkeit der Sicherheitsmaßnahmen gewährleistet werden.

4.9 Netze

IT-Systeme sind in vielen der teilnehmenden Unternehmen eine technische Grundlage für die Realisierung der Geschäftsprozesse. Die IT-Systeme sind über Netze zum Zweck des Datenaustausches sowie der Nutzung bzw. Bereitstellung von Diensten und Anwendungen miteinander verbunden. Zur Anbindung von Unternehmensteilen an anderen Standorten, der Mitarbeiter im Außendienst sowie der Heim- und Telearbeitsplätze und selbstverständlich zur Kommunikation mit den Kunden und Geschäftspartnern werden Netzverbindungen genutzt. Um schutzbedürftige Daten über nicht vertrauenswürdige Netze, wie beispielsweise das Internet, zu übertragen, sind Sicherheitsmaßnahmen zu realisieren. Zur effektiven und effizienten Verwaltung der Netzwerke sind weitere IT-Sicherheitsmaßnahmen erforderlich.

4.9.1 Themen in den Interviews

In Bezug auf die Netze sind die folgenden Kriterien betrachtet worden:

- **Einsatz von VPN**: Der Einsatz von VPN ermöglicht den Schutz der Daten beim Transport.
- **Netz- und Systemmanagement:** Ein wesentlicher Aspekt des Schutzes des Netzwerks ist eine effektive und effiziente Verwaltung und Steuerung der Netzwerkkomponenten und IT-Systeme. Als technische Maßnahme werden in der Regel Netzwerk- und Systemmanagementsysteme eingesetzt, welches den aktuellen Status der Netze und Systeme automatisierte anzeigen und ggf. die Steuerung ermöglichen.

4.9.2 Ergebnisse

Das Ergebnis für die teilnehmenden Unternehmen ist in der Abbildung 23 dargestellt.

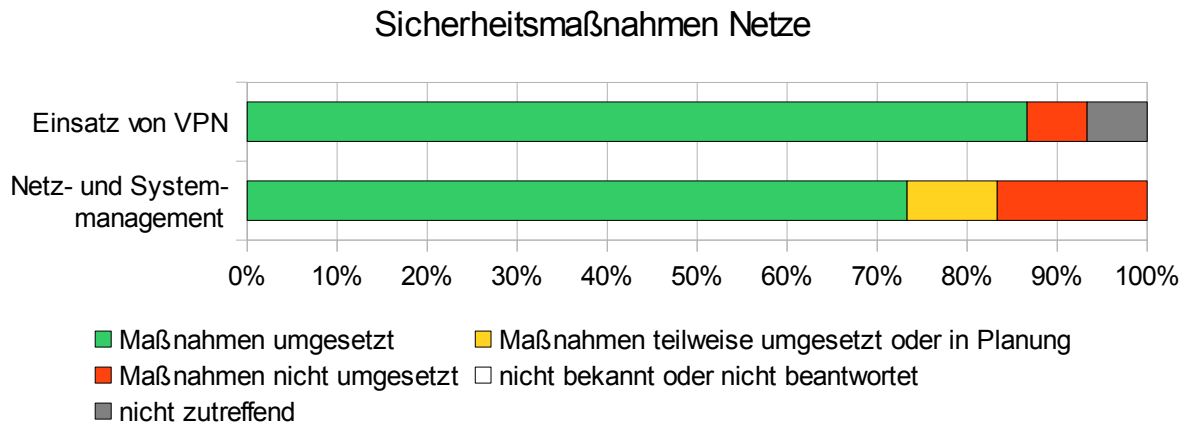


Abbildung 23: Auswertung Netze

Mehr als 80 Prozent der Unternehmen haben die abgefragten Sicherheitsmaßnahmen zum Schutz der Netze umgesetzt. In 26 der 30 befragten Unternehmen werden VPNs eingesetzt. Die übrigen Unternehmen gaben an, kein VPN zu verwenden. Dies ist jedoch nicht mit dem vollständigen Fehlen einer Schutzmaßnahme gleichzusetzen. In zwei Unternehmen wird das Internet nicht für die

Geschäftsprozesse verwendet. Des Weiteren gab ein Unternehmen an, dass ein Zugriff durch mobile Endgeräte auf das Unternehmensnetzwerk nicht vorgesehen ist. Ein Einsatz eines VPN ist daher bei diesen Unternehmen nicht notwendig. Einige der befragten Unternehmen nutzen bei der standortübergreifenden Kommunikation Multiprotocol-Label-Switching-Netzwerke (MPLS-Netzwerke)[2]. Nicht in allen Fällen wird die MPLS-Verbindung durch ein VPN geschützt. Ein Schutz der übertragenen Daten gegen unberechtigte Kenntnisnahme oder Manipulation ist in diesen Fällen nicht sichergestellt.

Drei Viertel der Unternehmen setzen automatisierte und etablierte Systeme zum Netzwerk- und Systemmanagement ein.

Insgesamt ist das Thema Netzwerksicherheit bei den Unternehmen hinreichend gut etabliert.

4.9.3 Handlungsempfehlungen

Basierend auf dem IT-Grundschutz sollten Sicherheitsmaßnahmen zum Thema Netzwerksicherheit umgesetzt werden, um den Schutz von Daten und Informationen zu gewährleisten. Der IT-Grundschutz schlägt in dem Baustein „B. 4.1 Heterogene Netze“ die folgende Vorgehensweise zur Erreichung eines sicheren Einsatzes vor:

1. **Analyse der aktuellen Netzsituation:** In dieser Analyse sollten die Erhebung der Lastfaktoren und eine Verkehrsanalyse vorgenommen werden. Weiterhin sollten Netzengpässe festgestellt und kritische Bereiche identifiziert werden. Unterstützung hierzu liefert der IT-Grundschutz in den Maßnahmen „M 2.139 Ist-Aufnahme der aktuellen Netzsituation“ und „M 2.140 Analyse der aktuellen Netzsituation“
2. **Konzeption des Netzes und des Netzmanagements:** Dabei sollten ein Netzkonzept (vgl. IT-Grundschutz Maßnahme M 2.141) und ein Netz-Realisierungsplan (vgl. IT-Grundschutz M 2.143) entwickelt werden.
3. **Sicherer Betrieb des Netzes:** Mittelfristig ist der sichere Betrieb der Netze zu gewährleisten. So sollte eine geeignete Segmentierung des Netzes auf physikalischer und logischer Ebene durchgeführt werden (vgl. IT-Grundschutz Maßnahmen „M 5.61 Geeignete physikalische Segmentierung“ und „M 5.62 Geeignete logische Segmentierung“).
4. **Notfallvorsorge:** Langfristig sollte das Thema der Notfallvorsorge in den Netzen realisiert werden. Hierbei ist es wichtig, besonders kritische Netze regelmäßig zu überprüfen und redundant auszulegen.

In dieser zeitlichen Reihenfolge sollte die Sicherung der Netze in den Unternehmen vorgenommen werden. Eine weitere Sicherungsmaßnahme zum Schutz der Daten und Informationen ist der Einsatz eines VPNs. Hierüber werden externe Zugriffe auf die Unternehmensdaten und -informationen gestattet. Dabei ist zu beachten, dass für den Aufbau des VPN ein gewisser Zeitraum geplant werden muss und keine Realisierung in kürzester Zeit möglich ist. Die zugehörigen Maßnahmen für die Realisierung eines VPNs sind im IT-Grundschutz im Baustein „B 4.4 VPN“ verankert. Voraussetzung für die richtige Auswahl und den sicheren Betrieb eines VPNs ist eine entsprechende Planung und Konzeption. Eine gute Planung vermindert die Komplexität im Betrieb und kann zusätzliche Lücken aufzeigen. Besonders wichtig ist hierbei auch die regelmäßige

2 Vermittlungsverfahren zur Übertragung von Datenpaketen entlang eines zuvor aufgebauten („signalisierten“) Pfades. MPLS wird überwiegend von Betreibern großer Transportnetze eingesetzt (Internetprovider).

Überprüfung der Konfiguration. So sollten nicht genutzte VPN-Zugänge entsprechend gesperrt werden.

Mittelfristig sollte ein Netz- und Systemmanagement realisiert werden, um den Überwachungsaufwand zu vermindern und potentielle Sicherheitsrisiken zu erkennen. Für den Aufbau eines Netz- und Systemmanagements empfiehlt der IT-Grundschutz im Baustein „B 4.2 Netz- und Systemmanagement“ folgende Maßnahmen:

1. Auf Basis der vorhandenen IT-Systeme sollte eine Strategie entwickelt werden. Hierzu werden in einem ersten Schritt die Anforderungen aufgenommen (vgl. IT-Grundschutz Maßnahme „M 2.169 Entwickeln einer Systemmanagementstrategie“ und „M 2.168 IT-System-Analyse vor Einführung eines Systemmanagementsystems“). Diese Strategie sollte in einem Managementkonzept dokumentiert werden.
2. Basierend auf dem Managementkonzept müssen die Anforderungen an das einzusetzende Produkt formuliert werden. Unterstützung hierzu bietet der IT-Grundschutz in der Maßnahme „M 2.170 Anforderungen an ein Systemmanagement“. Erst danach kann ein für das Unternehmen passendes Produkt ausgewählt werden.
3. Aufnahme des Betriebs des Produktes im Unternehmen. Der IT-Grundschutz bietet hierfür Unterstützung in den Maßnahmen „M 4.91 Sichere Installation eines Systemmanagements“ und „M 4.92 Sicherer Betrieb eines Systemmanagementsystems“.

Insgesamt sollte ein Unternehmen sich zu jeder Zeit bewusst sein, dass Netzwerke Schnittstellen in externe Netze sind, in denen Gefahren lauern. Das Risiko fehlender Schutzmaßnahmen muss einem Unternehmen bewusst sein.

4.10 Anwendungen

Im Rahmen dieser Studie wird unter dem Aspekt der Anwendungen schwerpunktmäßig die Kommunikationsanwendung E-Mail betrachtet. Mittels E-Mail können nicht nur kurze Informationen schnell, bequem und informell weitergegeben werden, sondern es können auch Geschäftsvorfälle zur Weiterbearbeitung an andere Personen weitergeleitet werden. Abhängig davon, für welchen Einsatzzweck E-Mail eingesetzt wird, unterscheiden sich auch die Ansprüche an Vertraulichkeit, Verfügbarkeit, Integrität und Verbindlichkeit der zu übertragenden Daten.

4.10.1 Themen in den Interviews

Zur Erfassung der in den Unternehmen umgesetzten Maßnahmen zur Absicherung der E-Mail-Kommunikation werden die folgenden Kriterien betrachtet:

- **Einsatz von Verschlüsselung und Signatur bei der E-Mail-Kommunikation:** Werden vertrauliche Informationen und/oder Daten mit hohem Integritätsanspruch übertragen, so sollten kryptografische Verfahren eingesetzt werden. In diesem Kriterium wird geprüft, inwieweit die Unternehmen Verschlüsselungen und Signaturen im Rahmen der E-Mail-Kommunikation[3] einsetzen.

3 Dies umfasst ebenfalls die Übertragung verschlüsselter und/oder signierter Dateien per E-Mail.

- **Einsatz von Virenscannern:** Zum Schutz vor Schadprogrammen sind auf den zentralen Übergabestellen (E-Mail-Gateway, Firewall) Virenschutzprogramme einzusetzen. Daten, die versendet werden sollen, müssen unmittelbar vor dem Versand auf Schadprogramme geprüft werden. Analog müssen empfangene Daten unmittelbar nach dem Empfang auf Schadprogramme geprüft werden. Diese Überprüfungen sind sowohl bei der Nutzung von Datenträgern als auch bei der Datenübertragung über Kommunikationsverbindungen erforderlich.
- **Archivierung von E-Mails:** Die Bedeutung von E-Mail für die interne und externe Kommunikation nimmt ständig zu. Daher ist es wichtig, dass die gesendeten bzw. empfangenen Nachrichten auch längerfristig zur Verfügung stehen. Eine E-Mail-Archivierung wird neben dem Schutz vor Datenverlust auch aus Gründen der Erfüllung rechtlicher Anforderungen und zum Schutz vor Überlastung von E-Mail-Servern eingesetzt. Hierbei kann die Archivierung Client- oder Server-gesteuert erfolgen.

4.10.2 Ergebnisse

Die Ergebnisse der Befragung sind in der Abbildung 24 dargestellt.

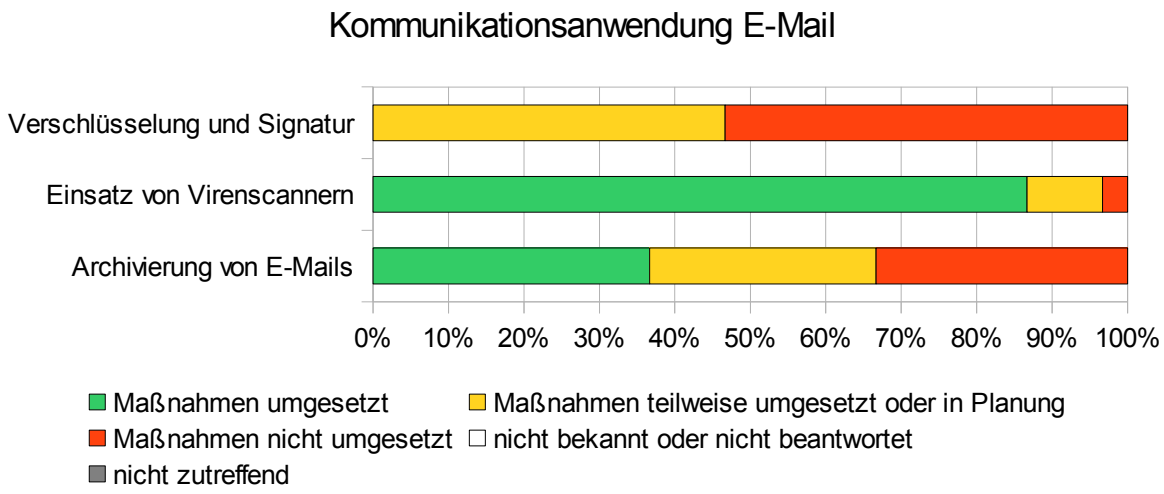


Abbildung 24: Auswertung Anwendungen

Von den befragten Unternehmen nutzen 97 Prozent das Internet in den Geschäftsprozessen. Hierbei ist die E-Mail-Kommunikation die häufigste Nutzungsart. Sie wird praktisch von allen Unternehmen verwendet (siehe Kapitel 4.15). Werden hierbei vertrauliche Informationen oder Informationen mit hohem Integritätsanspruch übertragen und besteht eine gewisse Möglichkeit, dass diese Daten Unbefugten zur Kenntnis gelangen, von diesen manipuliert oder durch technische Fehler verändert werden können, sollte ein kryptographisches Verfahren zum Schutz der Daten für den Transport oder die Übermittlung in Betracht gezogen werden. Aus der Ergebnisdarstellung in Abbildung 24 wird deutlich, dass die E-Mail-Kommunikation bei annähernd der Hälfte der befragten Unternehmen zumindest teilweise gesichert erfolgt. So werden in 14 Unternehmen ausgewählte E-Mails verschlüsselt. Die Auswahl erfolgt selektiv nach Projekt bzw. Kommunikationspartner. In zwei Fällen bieten die Kommunikationspartner keine Unterstützung für gesicherte E-Mails, so dass vorhandene technische Möglichkeiten ungenutzt bleiben. Eine

vollständige Absicherung aller externen E-Mails ist in keinem Betrieb umgesetzt. Eine digitale Signatur der E-Mail unterstützen fünf Unternehmen.

Zur Wahrung der Vertraulichkeit bzw. zur Sicherung der Integrität vertrauen 78 Prozent der Unternehmen, die den gesicherten Austausch von E-Mails unterstützen, auf den Standard GNU Privacy Guard (GPG). In 35 Prozent der Unternehmen wird der Standard S/MIME zusätzlich zu GPG unterstützt.

Die Absicherung der E-Mail scheitert häufig an fehlenden technischen Möglichkeiten bzw. der Umsetzung des Schlüsselmanagements. In der Befragung wurde häufig die Begründung angegeben, dass der Kommunikationspartner eine Absicherung der E-Mail Kommunikation aufgrund des hohen technischen Aufwandes bei der Schlüsselverteilung und -verwaltung ablehnt. In einem Fall wurde die Begründung gegeben, dass es eine Direktive gebe, keine sensitiven Daten per E-Mail zu versenden.

Die übergreifende Auswertung hat gezeigt, dass mehr Unternehmen ihre E-Mails verschlüsseln, als es in den Befragungen deutlich wurde. Dies ist noch durch die Heterogenität der Nutzung einer gesicherten E-Mail-Kommunikation verstärkt worden. Es ist allerdings festzuhalten, dass der E-Mail Versand in über 50 Prozent der Fälle generell ungesichert erfolgt.

Zum Schutz vor Schadprogrammen sind in 87 Prozent der Unternehmen geeignete Maßnahmen umgesetzt. Diese umfassen den Einsatz von Virenscannern auf den Arbeitssystemen der Mitarbeiter, der zentralen E-Mail Übergabestelle (E-Mail-Server oder Firewall) sowie dem Datei-Server. Somit sind Überprüfungen sowohl bei der Nutzung von Datenträgern, der Ablage von Daten auf dem Datei-Server als auch bei der Datenübertragung über Kommunikationsverbindungen sichergestellt. Bei drei Unternehmen werden die Maßnahmen in Teilen umgesetzt. Ein Unternehmen verzichtet aktuell vollständig auf den Einsatz von Virenscannern.

Die Hälfte der Unternehmen, die die Maßnahmen vollständig umgesetzt haben, setzen einen weiteren zentralen Virenscanner zur Prüfung der E-Mail-Kommunikationsdaten ein. Der Einsatz wurde häufig mit der im Vergleich zum Standardscanner höheren Sicherheit durch die Nutzung eines zusätzlichen Systems mit unterschiedlicher Heuristik begründet.

Die Archivierung setzen etwas mehr als zwei Drittel der Unternehmen vollständig bzw. teilweise um. Die Sicherung der E-Mails erfolgt hierbei in 75 Prozent der Unternehmen automatisiert, ansonsten selektiv durch den jeweiligen Mitarbeiter durch manuelles Zuführen zur Sicherung.

Es wird immer wieder diskutiert, ob und in wieweit dienstliche E-Mail-Zugänge für private Zwecke benutzt werden dürfen. Solange sich die private Nutzung sich in Grenzen hält, wird dies von einigen Unternehmen toleriert.

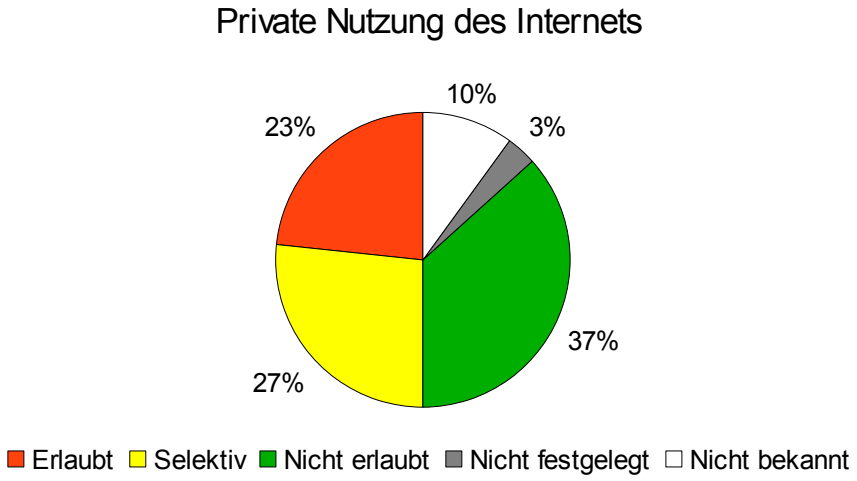


Abbildung 25: Private Nutzung des Internets

Im Rahmen der Studie (siehe Abbildung 25) gaben die Hälfte der Unternehmen an, die private Nutzung des Internets vollständig bzw. selektiv zu erlauben. Die Einschränkungen beziehen sich im Wesentlichen auf Nutzung außerhalb der Kernarbeitszeiten sowie den Einsatz Filterlisten. In 37 Prozent der Unternehmen war die private Nutzung untersagt.

4.10.3 Handlungsempfehlungen

Im Rahmen der Aufbewahrungsfristen sind verschiedene gesetzliche Vorgaben von den Unternehmen zu beachten. Neben vielen anderen Anforderungen, wie den Zugriff durch das Bundesfinanzministerium [BMF2001], sei hier auf die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) und die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) verweisen.

Die aus rechtlicher Sicht bestehenden Aufbewahrungsfristen nach §257 Abs. 4 HGB fordern für die Aufbewahrung typischerweise zehn Jahre und für Handelsbriefe sechs Jahre. Dies gilt ebenfalls für E-Mail-Nachrichten, die Handelsbriefe sind. Aus organisatorischen Gründen kann es daher erforderlich sein, alle E-Mail-Nachrichten, mit Ausnahme rein privater Nachrichten, mindestens sechs Jahre aufzubewahren.

Es sollte daher primär geprüft werden, ob den gesetzlichen und rechtlichen Anforderungen in Bezug auf die E-Mail-Kommunikation und Archivierung genüge getan wird. Sofern dies nicht der Fall ist, muss kurzfristig eine entsprechende Umsetzung der rechtlichen Vorgaben erfolgen.

Eine komplette Archivierung der E-Mail-Kommunikation ist in jedem Fall schon aus organisatorischen Gründen empfehlenswert. Hierbei sollten alle E-Mail-Nachrichten, mit Ausnahme rein privater Nachrichten, mindestens sechs Jahre aufbewahrt werden. Eine Realisierung solch einer Archivierung kann mittel- bis langfristig erfolgen.

Bei einer Planung der Umsetzung der Archivierung muss auch die private Nutzung von E-Mails geklärt sein. Auch Abstimmungen mit bestehenden Betriebsräten müssen vor der Einführung einer Archivierung – besonders im Fall der erlaubten privaten Nutzung – durchgeführt werden.

Dass die Erlaubnis bzw. die Tolerierung der privaten Nutzung des Internets bzw. des E-Mail-Dienstes nicht unproblematisch ist, zeigt die Verpflichtung des Arbeitgebers zur Wahrung des Fernmeldegeheimnisses gemäß § 88 TKG. Damit ist es dem Unternehmen untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen (§ 88 Abs. 3 TKG). In diesem Zusammenhang wurde am 16.02.2011 ein Urteil des Landesarbeitsgerichts Berlin-Brandenburg gefällt und am 28.07.2011 veröffentlicht (Az. 4 Sa 2132/10). Hiernach darf der Arbeitgeber in Abwesenheit des Mitarbeiters die dienstlichen E-Mails öffnen. Jedoch ist der Arbeitgeber zum Lesen privater E-Mails damit ebenfalls nicht berechtigt. Gegen diese Forderung kann aber bereits bei der Analyse von Protokolldaten bzw. der Durchsicht archivierter E-Mails verstoßen werden.

Eine weitergehende Vertiefung ist im Rahmen dieser Studie nicht möglich. Hierzu sei auf den Abschnitt „Private Nutzung im Unternehmen – Richtlinien und Regelungen“ im Kapitel 6: Stichwort- und Informationsverzeichnis verwiesen.

Dem entsprechend sind die vorhandenen Regelungen zur Nutzung der E-Mailsysteme zu prüfen. Hierin sollte festgelegt sein, für welchen Einsatzzweck und welche Informationen E-Mail vorgesehen ist. Abhängig davon, wofür E-Mail eingesetzt werden soll, sind die Ansprüche an Vertraulichkeit, Verfügbarkeit, Integrität und Verbindlichkeit der zu übertragenden Daten zu prüfen und ggf. neu zu definieren. Auf dieser Basis kann mittelfristig der Aufbau oder Ausbau der technischen Möglichkeiten zum sicheren Transport von E-Mail erfolgen.

4.11 Datensicherung

Durch technisches Versagen, versehentliches Löschen oder durch Manipulation können gespeicherte Daten unbrauchbar werden bzw. verloren gehen. Eine Datensicherung soll gewährleisten, dass durch einen redundanten Datenbestand der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen. Um dies zu vermeiden, müssen sich die Unternehmen dem Risiko des Verlusts von Daten bewusst sein und entsprechende Schutzmaßnahmen ergreifen.

4.11.1 Themen in den Interviews

Für die Ermittlung des Umsetzungsstandes der Datensicherung bei den befragten Unternehmen wurden die folgenden Kriterien verwendet:

- **Zeitnahe Wiederherstellung der Handlungsfähigkeit:** Der Zeitraum, bis die Handlungsfähigkeit des Unternehmens nach einem Datenverlust wiederhergestellt ist, sollte eingeschätzt werden können. Das Unternehmen wird hierbei als handlungsfähig angesehen, wenn die kritischen Geschäftsprozesse innerhalb von 72 Stunden wieder lauffähig sind.
- **Datensicherungskonzept:** Das Datensicherungskonzept dokumentiert die Vorgehensweise bei der Datensicherung. In diesem Dokument sollten die wesentlichen Punkte festgehalten sein. Das zur Sicherung verwendete IT-System, die Art der Datensicherung, die Änderungsfrequenz der Daten und die Verfügbarkeitsanforderungen sind einige dieser Faktoren.

- **Sicherungskopie eingesetzter Software:** Eine Datensicherung allein ist nicht immer ausreichend, um die Daten lesbar wieder herzustellen. So sind in einigen Fällen die Anwendungen nur bedingt oder gar nicht abwärtskompatibel. Für diese Daten müssen neben der Datensicherung auch Sicherungskopien der eingesetzten Software angefertigt werden. Dies gilt auch für die Originaldatenträger erworbener Software bzw. der Quellcodes und Binaries bei Eigenentwicklungen. Um die Handlungsfähigkeit des Unternehmens zu gewährleisten, sind Sicherungskopien zu erstellen, von denen bei Bedarf die Software wieder eingespielt werden kann.
- **Dokumentation von Datensicherungen:** Die Durchführung der Datensicherung muss dokumentiert werden. Besonders für den Fall, dass der für die Datensicherung Verantwortliche bei einer Wiederherstellung der Daten nicht verfügbar ist und dies durch andere Personen durchgeführt werden muss. Auf Basis der Dokumentation kann nachvollzogen werden, ob regelmäßig Datensicherungen vorhanden sind, wann die letzte Datensicherung erfolgt ist, welchen Stand die Daten dann haben und wo sich die Datensicherung befindet.
- **Aufbewahrung von Datenträgern:** Der Aufbewahrungsort von Datenträgern muss drei Ansprüchen genügen. Zum einem muss dieser ausreichend sicher sein. Kein Unberechtigter darf Zugriff auf die Daten erhalten. Zweitens muss der Aufbewahrungsort auch die klimatischen Bedingungen für eine längerfristige Aufbewahrung von Datenträgern gewährleisten. Schließlich muss die Verfügbarkeit der Datensicherung in Abhängigkeit von den kritischen Geschäftsprozessen gewährleistet sein. Diese kann neben einer 24-Stunden-Verfügbarkeit auch durch mehrfache Ablage verschiedener Datensicherungen gewährleistet werden.
- **Wiederherstellung von Datensicherungen:** Eine Datensicherung wird in der Regel durchgeführt, um verlorene oder beschädigte Daten wiederherstellen zu können. Dieses Wiederherstellen der Daten muss in regelmäßigen Abständen in praktischen Übungen erprobt werden. Weiterhin hat die Überprüfung der Wiederherstellung den positiven Aspekt, dass nochmal geprüft wird, ob Datensicherungen erfolgreich auf dem Datenträger gespeichert werden konnten.

4.11.2 Ergebnisse

Die Ergebnisse für die befragten Unternehmen sind in der Abbildung 26 dargestellt.

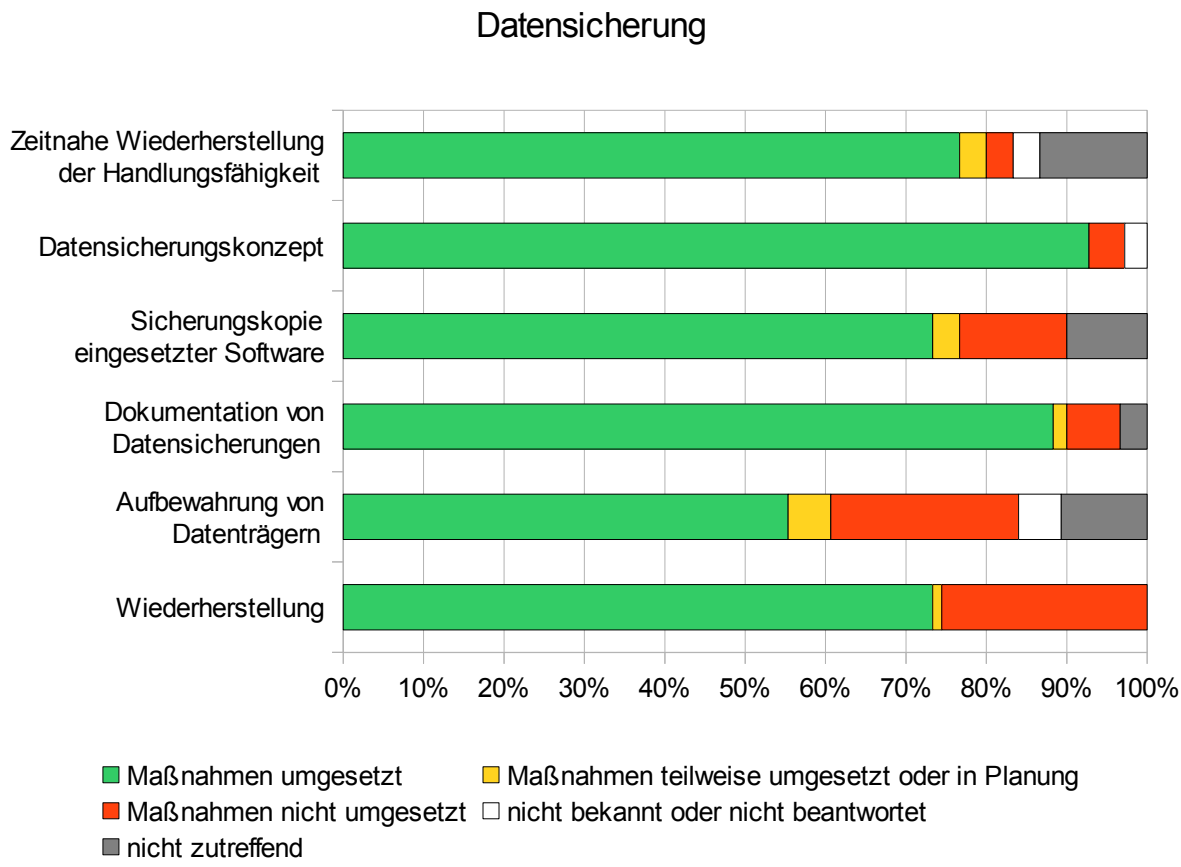


Abbildung 26: Auswertung Datensicherung

Die Ergebnisdarstellung in Abbildung 26 zeigt insgesamt einen hohen Umsetzungsgrad in Bezug auf die Sicherheitsmaßnahmen zur Datensicherung bei den Unternehmen. Die Stärken wie auch die deutlich sichtbaren Schwächen in Bezug auf die Aufbewahrung der Datenträger sowie die Wiederherstellung von Daten werden nachfolgend diskutiert.

Insgesamt haben 29 der Unternehmen angegeben, eine Sicherung der Unternehmensdaten durchzuführen. Lediglich ein Unternehmen konnte hierzu keine Angaben machen. Von diesen 29 Unternehmen können 70 Prozent die Handlungsfähigkeit innerhalb von 48 Stunden und knapp 7 Prozent innerhalb von 72 Stunden wiederherstellen (grüner Balken). Selbst bei einem Verlust von spezieller Hardware sind in den befragten Unternehmen Prozesse etabliert, die einen Wiederanlauf der kritischen Geschäftsprozesse ermöglichen.

Das Datensicherungskonzept dokumentiert bei 92 Prozent der Unternehmen die Vorgehensweise und enthält die wesentlichen Punkte zur Datensicherung. Die Verfügbarkeitsanforderungen, die organisatorischen und technischen Rahmenbedienungen zur Durchführung der Datensicherungen, die Aufstellung der zu sichernden IT-Systeme, die Häufigkeit und der Zeitpunkt der Datensicherung sowie die Anzahl der Generationen sind einige der von den Unternehmen getroffenen Festlegungen. Hier sind nur vereinzelte Ausnahmen zu finden.

Der Umsetzungsgrad bei der Dokumentation der Datensicherungen liegt auf einem vergleichbar hohen Niveau wie bei dem Datensicherungskonzept. Die Datensicherungen werden bei knapp 90 Prozent der Unternehmen dokumentiert. Die Dokumentation erfolgt auf unterschiedlichste Art und

Weise. Neben der dokumentenzentrierten Vorgehensweise finden auch die Protokolle der eingesetzten Software sowie handschriftliche Aufzeichnungen Anwendung.

Weniger bewusst, jedoch oftmals indirekt durchgeführt, erfolgt die Erstellung der Sicherungskopien der im Unternehmen eingesetzten Software. Von den Originaldatenträgern erworbener Software bzw. von der Originalsoftware bei Eigenentwicklungen erstellen knapp 75 Prozent der Unternehmen eine Sicherungskopie. Die Aufbewahrung der Sicherungskopien erfolgt hierbei grundsätzlich getrennt von den Originaldatenträgern. Hierzu zählt auch die Erstellung und Sicherung von Installationsimages für die IT-Systeme der Mitarbeiter wie auch der auf den Servern eingesetzten virtuellen Maschinen.

Der von den Unternehmen gewählte Aufbewahrungsort der Datensicherungen erfüllt in 93 Prozent der Fälle bei Inbetriebnahme die klimatischen Anforderungen an eine langfristige Aufbewahrung der Datenträger. Die Eignung wurde von 21 Unternehmen in den letzten drei Jahren zumindest einmalig geprüft. Eine regelmäßige Prüfung erfolgt dagegen lediglich in acht Unternehmen. Hiervon haben fünf Unternehmen Wertebereiche definiert, die eine qualitative und fortlaufende Überwachung sowie Bewertung des Aufbewahrungsortes erlauben. Dies entspricht knapp 17 Prozent der befragten Betriebe.

Die nachfolgende Abbildung 27 zeigt die genutzten Aufbewahrungsorte der befragten Unternehmen. Mehrfachnennungen waren bei dieser Fragestellung möglich, um den Unternehmen Rechnung tragen zu können, die mehrere Datensicherungen an getrennten Orten verfügbar halten.

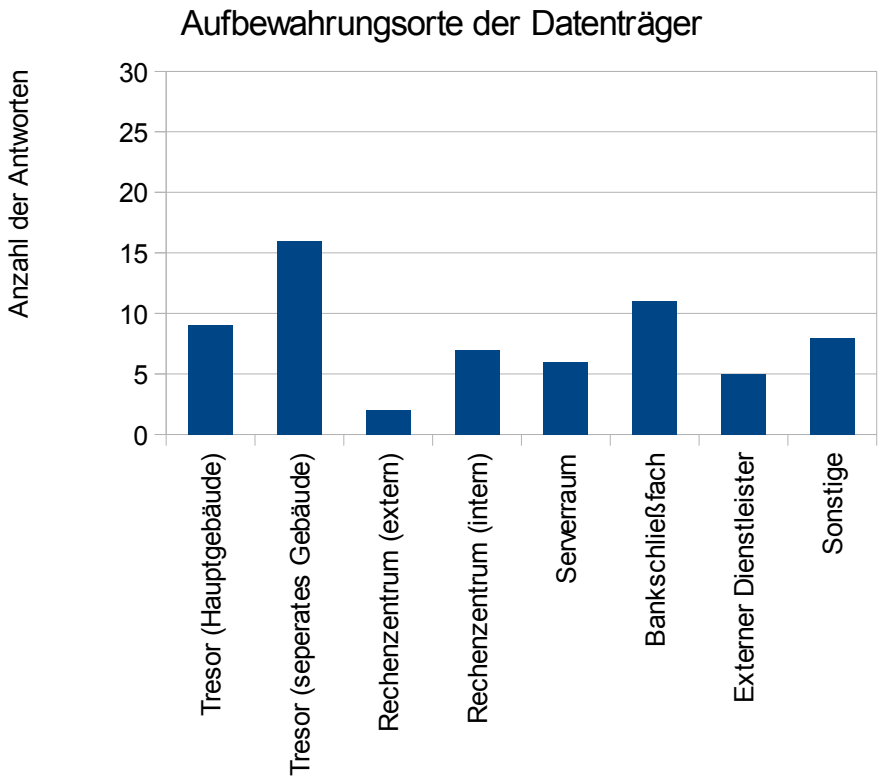


Abbildung 27: Aufbewahrungsort von Datenträgern

Die befragten Unternehmen präferieren die Aufbewahrung der Datenträger in Tresoren innerhalb des Unternehmens sowie in Bankschließfächern. Unter dem Punkt Sonstiges gaben die Unternehmen die folgenden Aufbewahrungsorte an:

- Privaträume von Geschäftsführung oder Mitarbeitern
- Externer Büroraum
- Weiteres Rechenzentrum
- Gleicher Standort, allerdings in einem anderen Gebäude als die Technik

Weiterhin wurde festgestellt, dass in der IT-Abteilung keine Datensicherungen aufbewahrt werden. Die Aufstellung der Aufbewahrungsorte zeigt, dass die IT-Leitung hinsichtlich des Zugriffsschutzes auf die Datensicherungen sensibilisiert ist und entsprechend handelt. Jedoch werden die klimatischen Bedingungen für eine längerfristige Aufbewahrung oftmals nicht fortlaufend geprüft bzw. das Bewusstsein hierfür ist nicht vorhanden. Besonders auffällig ist dies bei der Verwendung von Bankschließfächern.

Die Wiederherstellung von Datensicherungen wird nicht in jedem Unternehmen regelmäßig auf der Basis von praktischen Übungen durchgeführt. Insgesamt haben rund zwei Drittel der Unternehmen angegeben, eine regelmäßige Wiederherstellung der Datensicherungen durchzuführen. Dies beinhaltet auch die regelmäßigen Nutzeranfragen zur Wiederherstellung von Daten. Eine regelmäßige praktische Übung erfolgt bei knapp der Hälfte der Unternehmen. In Teilen werden hierzu die produktiven IT-Systeme verwendet. Der Einsatz dedizierter Testsysteme erfolgt bei knapp 30 Prozent der Unternehmen.

Zusammenfassend kann festgestellt werden, dass die Unternehmen im Bereich der Datensicherung sehr gut aufgestellt sind. Die in Bezug auf die fortlaufende Prüfung der Aufbewahrungsorte der Datensicherungen sowie die regelmäßigen praktischen Übungen zur Wiederherstellung von Daten identifizierten Schwächen können durch geeignete Maßnahmen kurzfristig adressiert werden. Dies gilt ebenfalls für die Erstellung und Aufbewahrung von Sicherungskopien der im Unternehmen eingesetzten Software.

4.11.3 Handlungsempfehlungen

Aus den Ergebnissen wird ersichtlich, dass ein hohes Sicherheitsniveau in Bezug auf die Datensicherung in den Unternehmen bereits erreicht wurde. Zur weiteren Verbesserung stellt der IT-Grundschutz entsprechende Maßnahmen zur Realisierung zur Verfügung.

Eine erste Maßnahme sollte die regelmäßige Überprüfung der Datensicherung in Bezug auf die zu sichernden kritischen Geschäftsdaten sein. Hierzu ist sicherzustellen, dass die Daten auf den in die Sicherung mit einbezogenen IT-Systemen verfügbar sind. Sofern erforderlich sollten entsprechende Verpflichtungen der Unternehmensleitung ausgesprochen werden, dass Unternehmensdaten ausschließlich auf Servern und nicht auf lokalen Systemen zu speichern sind.

Die zur Datensicherung eingesetzten Datenträger sind an einem geeigneten Ort aufzubewahren. Die folgenden Anforderungen (vgl. Maßnahmen M 6.20 „Aufbewahrung Backup-Datenträger“) sind zu beachten:

- Der Zugriff auf den Datenträger darf nur befugten Personen möglich sein, so dass eine Entwendung ausgeschlossen werden kann.

- Ein ausreichend schneller Zugriff muss im Bedarfsfall gewährleistet sein.
- Der Aufbewahrungsort muss auch die klimatischen Bedingungen für eine längerfristige Aufbewahrung von Datenträgern erfüllen.
- Für den Katastrophenfall müssen die Backup-Datenträger räumlich getrennt vom Rechner aufbewahrt werden, wenn möglich in einem anderen Brandabschnitt.

Insbesondere die gewählten Aufbewahrungsorte sollten durch die Unternehmen kurzfristig erneut auf ihre Eignung geprüft werden.

Neben den Datensicherungen ist ebenfalls kurzfristig zu prüfen, ob die Verfügbarkeit der im Unternehmen eingesetzten Softwareversionen auch bei Verlust der Originaldatenträger dauerhaft sichergestellt ist. Für den Fall, dass dies nicht gewährleistet ist, sollten kurzfristig Sicherungskopien der Software erstellt werden. Die Aufbewahrung sollte getrennt von den Originaldatenträgern erfolgen.

Um sicherzustellen, dass die Datensicherungen im Bedarfsfall zur Wiederherstellung von Daten genutzt werden können, sollte eine entsprechende Überprüfung möglichst umgehend etabliert werden. Mittelfristig ist eine regelmäßige Prüfung in praktischen Übungen unter Verwendung von Testsystemen sinnvoll. Diese Vorgehensweise gewährleistet, dass erstens eine nutzbare Datensicherung erfolgt und zweitens die Wiederherstellbarkeit der Daten gesichert ist.

Mittelfristig ist die Dokumentation der Datensicherung zur prüfen und bei Bedarf zu erweitern. Dies sollte vom Verantwortlichen für die Datensicherung durchgeführt werden. In einer Dokumentation zur Datensicherung sollten die folgenden Punkte enthalten sein (vgl. IT-Grundschutz, Maßnahme „M 6.37 Dokumentation der Datensicherung“):

- Datum der Datensicherung
- Datensicherungsumfang (Dateien- und Verzeichnisangaben)
- Datenträger, auf dem die Daten im operativen Betrieb gespeichert sind
- Datenträger, auf dem die Daten gesichert wurden
- Eingesetzte Hard- und Software (inkl. Versionsnummern) für den Einsatz der Datensicherung
- Ausgewählte Parameter der Datensicherung

Langfristig sind regelmäßige Überprüfungen zur Aktualität der etablierten Regelungen, Vorgehensweisen und Dokumentationen umzusetzen.

4.12 Behandlung von Sicherheitsvorfällen

Um die Informationssicherheit im laufenden Betrieb aufrecht zu erhalten, ist es notwendig, die Behandlung von Sicherheitsvorfällen im Vorfeld zu konzipieren und einzuüben. Als Sicherheitsvorfall wird dabei ein unerwünschtes Ereignis bezeichnet, das Auswirkungen auf die Informationssicherheit hat und in der Folge große Schäden nach sich ziehen kann. Typische Folgen von Sicherheitsvorfällen können das Ausspähen, die Manipulation oder die Zerstörung von Daten sein. Um Schäden zu vermeiden bzw. zu begrenzen, müssen Sicherheitsvorfälle schnell und effizient bearbeitet werden. Wenn hierbei auf ein vorgegebenes und erprobtes Verfahren aufgesetzt werden kann, können Reaktionszeiten minimiert werden.

4.12.1 Themen in den Interviews

Für die Einschätzung des Stands zu Sicherheitsvorfällen in den Unternehmen wurden die folgenden Kriterien in der Befragung herangezogen:

- **Definition eines Sicherheitsvorfalls:** Die Definition und die Abgrenzung eines Sicherheitsvorfalls ist die Grundlage für ein Sicherheitsvorfallmanagement. Nur wenn Sicherheitsvorfall, Störfall und Notfall klar voneinander abgegrenzt sind, können entsprechende Maßnahmen vollständig entwickelt werden.
- **Vorgehensweise zur Behandlung eines Sicherheitsvorfalls:** Die Vorgehensweise zur Behandlung von Sicherheitsvorfällen muss klaren Regeln unterliegen und entsprechend dokumentiert sein.
- **Richtlinie zur Behandlung eines Sicherheitsvorfalls:** Die schriftliche Dokumentation und das Festhalten des Vorgehens in einer Richtlinie ermöglicht den Mitarbeitern das Auffrischen ihres Kenntnisstands zu beliebigen Zeiten. Da ein Sicherheitsvorfall in der Regel spontan eintritt, sollten die Regelungen auch praktisch anwendbar und zielgruppenorientiert sein.
- **Team zur Behandlung eines Sicherheitsvorfalls etabliert:** Ein Sicherheitsvorfallteam dient zur reibungslosen Behandlung des Sicherheitsvorfalls. Wichtig bei einem Sicherheitsvorfall sind die Dokumentation der Umstände und die schnelle Behebung von Sicherheitslücken. Sofern ein Sicherheitsvorfallteam benannt ist und die Aufgaben klar strukturiert sind, kann der ggf. eintretende Schaden minimiert bis vollständig verhindert werden.
- **Maßnahmen zur Detektion von Sicherheitsvorfällen etabliert:** Um einen Sicherheitsvorfall behandeln zu können, muss dieser zuerst erkannt werden. Hierzu können zum einen technische Detektionsmaßnahmen umgesetzt werden. Diese müssen allerdings regelmäßig geprüft werden. Weiterhin gehören organisatorische Detektionsmaßnahmen hinzu, wie beispielsweise das Kontrollieren von Protokolldaten. Detektionsmaßnahmen, die einen Vorfall detektieren, müssen dann so eingerichtet sein, dass die wichtigsten Informationen zu einer Erstmeldung dokumentiert werden.
- **Zentrale Kontaktstelle zur Meldung von Sicherheitsvorfällen etabliert:** Sicherheitsvorfälle, die nicht technisch detektiert werden können, sollten trotzdem zu einer Meldung führen. Hierzu sollte eine zentrale Kontaktstelle eingerichtet werden, die allen Mitarbeitern für die Meldung von Sicherheitsvorfällen bekannt ist. Die Mitarbeiter in der zentralen Kontaktstelle sollten eine entsprechende Schulung erhalten,um alle relevanten Informationen bei einer solchen Meldung aufnehmen zu können.
- **Prozess zur Eskalation von Sicherheitsvorfällen etabliert:** Sofern ein Sicherheitsvorfall aufgetreten ist, muss der Prozess zur Eskalation klar geregelt sein. Die Eskalationsstrategie sollte dabei so ausgelegt sein, dass alle benötigten Werkzeuge auch bei einem Sicherheitsvorfall verfügbar sind. Die Verfügbarkeit sollte regelmäßig überprüft werden. Klare Erkenntnis liefert jedoch nur die Erprobung und Übung der Eskalationsstrategie. Bei Auftreten von Unstimmigkeiten sollten dann Anpassungen am Prozess der Eskalation vorgenommen werden.

4.12.2 Ergebnisse

Die Ergebnisse für die betrachteten Unternehmen dieser Studie sind in der Abbildung 28 zusammengefasst dargestellt.

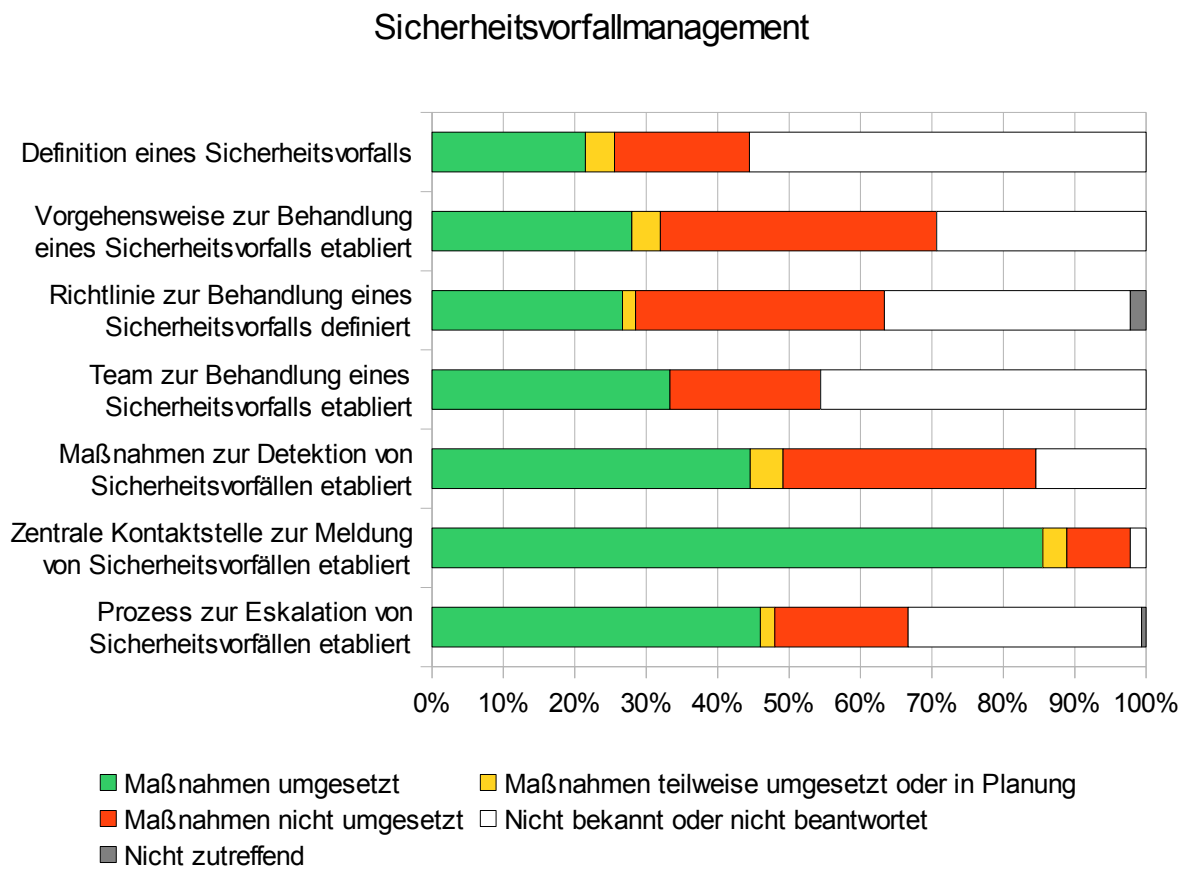


Abbildung 28: Auswertung Umgang mit Sicherheitsvorfällen

In den Ergebnissen wird deutlich sichtbar, dass das Management von Sicherheitsvorfällen ein noch zu erschließendes Themengebiet für die Mehrzahl der Unternehmen darstellt. Die weißen und roten Bereiche verdeutlichen, dass viele Unternehmen keine geeigneten Prozesse und Mechanismen zur Behandlung von Sicherheitsvorfällen etabliert haben.

Grundlegend hat rund ein Viertel der Unternehmen definiert, was einen Sicherheitsvorfall für das Unternehmen darstellt, und diesen von Störfällen abgegrenzt. Knapp ein weiteres Viertel der befragten Unternehmen gaben an, dass sie Kenntnis über die Definition eines Sicherheitsvorfalls haben, diesen jedoch im Unternehmen nicht deutlich abgrenzt haben. Somit hat auch nur ein geringer Teil der Unternehmen entsprechende Vorgehensweisen und Richtlinien entwickelt und prüft diese regelmäßig.

In den Interviews konnte, abweichend von der Definition eines Sicherheitsvorfalls, ermittelt werden, dass die Mehrheit der Unternehmen eine zentrale Kontaktstelle für die Meldung von Sicherheitsvorfällen etabliert hat. Bei zwei Dritteln der Unternehmen sind die zuständigen Mitarbeiter speziell geschult worden. Auch haben viele Unternehmen, die keine Abgrenzungen

eines Sicherheitsvorfalls vorgenommen haben, dennoch eine Art des Sicherheitsvorfallteams benannt. Jedoch konnte bei der Befragung auch ermittelt werden, dass zentrale Kontaktstelle und Sicherheitsvorfallteam aufgrund der teilweise geringen Unternehmensgröße häufig bei der IT-Leitung und deren Mitarbeitern angesiedelt sind.

Bei der Ermittlung der Ergebnisse zur Detektion von Sicherheitsvorfällen wurde deutlich, dass fast alle Unternehmen Sicherheitsvorfälle erkennen würden. Hier sind entsprechende und ausreichende Detektionsmaßnahmen verfügbar. Die nachfolgende Abbildung 29 zeigt die in den befragten Unternehmen verwendeten Detektionsmaßnahmen.

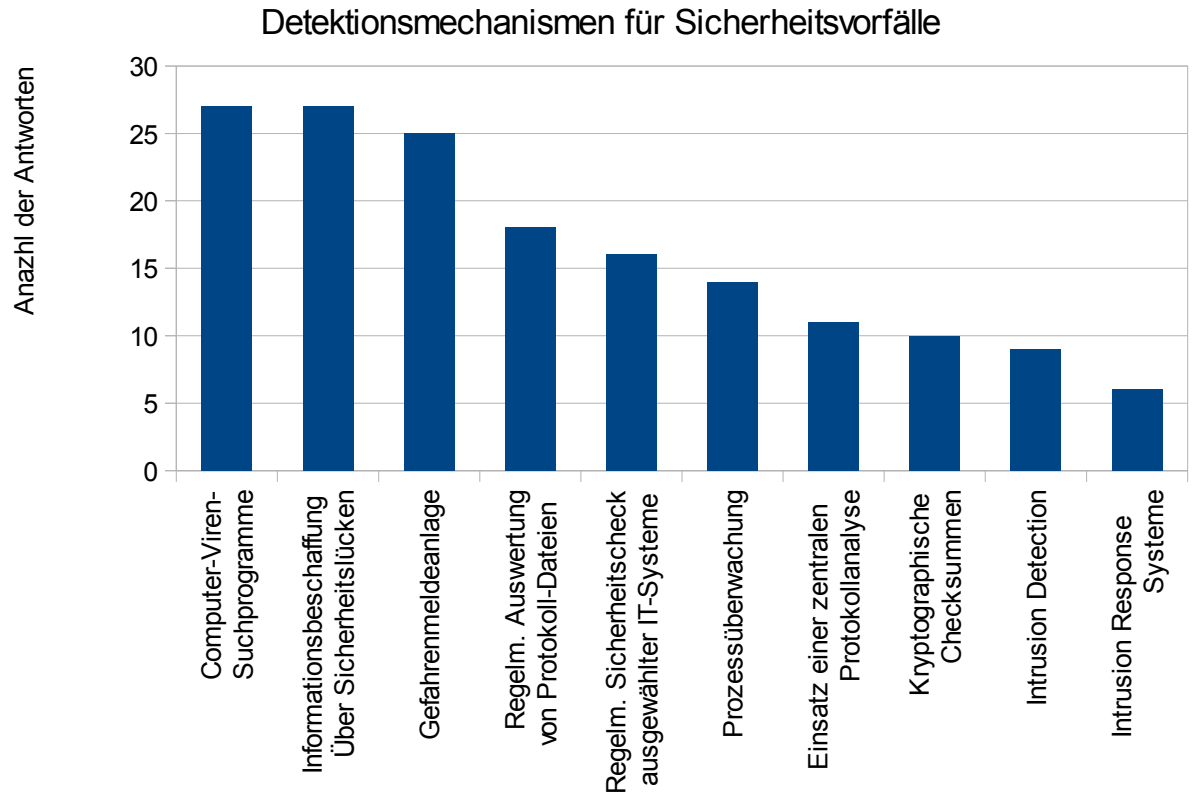


Abbildung 29: Detektionsmaßnahmen zu Sicherheitsvorfällen

Aus Rückfragen konnte ermittelt werden, dass aufgrund der oftmals fehlenden Definition eines Sicherheitsvorfalls diese im Unternehmen selbst jedoch nicht als Sicherheitsvorfall bezeichnet würden. Auch ist in der Regel keine Übersicht über die einzelnen Detektionsmaßnahmen verfügbar. Aufgrund der fehlenden Übersicht über die Maßnahmen erfolgt auch keine regelmäßige Überprüfung und Überwachung. Die zu registrierenden Informationen bei einer Erstmeldung sind ebenfalls nur in einem geringen Teil der Unternehmen bekannt.

Die Eskalation bei einem Sicherheitsvorfall ist in mehreren Unternehmen durch allgemeingültige Regeln abgedeckt. So gehört zur Eskalationsstrategie sehr häufig, die Geschäftsführung zu informieren. Die IT-Leitung gab sehr häufig an, dass bei der Behandlung von Sicherheitsvorfällen auf Handlungsanweisungen der Geschäftsführung gewartet wird. Dieses wird auch dadurch bestätigt, dass Eskalationsstrategien zumeist nicht dokumentiert sind. Eine regelmäßige Überprüfung, strukturierte Erprobungen und Übungen sind so nicht möglich. Auch hat nur rund ein

Viertel der Unternehmen über die Verfügbarkeit benötigter Werkzeuge während eines Sicherheitsvorfalls nachgedacht und entsprechende Maßnahmen getroffen.

Insgesamt ist das Sicherheitsvorfallmanagement in den befragten Unternehmen noch ausbaufähig. Hierbei kann eine Klärung und Abgrenzung von Sicherheitsvorfall zu Störfall und Notfall zu einer Verbesserung der Ergebnisse beitragen.

4.12.3 Handlungsempfehlungen

Für die Verbesserung der Ergebnisse sollte kurzfristig eine Definition eines Sicherheitsvorfalls im Unternehmen gefunden werden. So muss sehr deutlich der Sicherheitsvorfall vom Notfall und vom Störfall (vgl. Kapitel 6 „Definition Sicherheitsvorfall, Notfall und Störfall“) abgegrenzt sein. Der IT-Grundschutz liefert in der Maßnahme „M 6.122 Definition eines Sicherheitsvorfalls“ folgende beispielhafte Definition:

> *„Als Sicherheitsvorfall wird in unserem Unternehmen ein Ereignis bezeichnet, das die Vertraulichkeit, Verfügbarkeit und Integrität unserer Informationen, Geschäftsprozesse, IT-Dienste, IT-Systeme oder IT-Anwendungen mit hohem oder sehr hohem Schutzbedarf derart beeinträchtigt, dass ein großer Schaden für unser Unternehmen/Kunden/Geschäftspartner entstehen kann."*

Um mit Sicherheitsfällen umzugehen, müssen diese in einem ersten Schritt erkannt und erfasst werden. Da Sicherheitsvorfälle verschiedenste Ausprägungen haben können, ist die Erfassung nicht unmittelbar oder direkt möglich. So kann ein Teil der Sicherheitsvorfälle durch technische Maßnahmen erkannt werden. Kurzfristig sollten alle Detektionsmaßnahmen für Sicherheitsvorfälle geprüft und zusammengefasst dokumentiert werden. Fehlende Detektionsmaßnahmen sollten mittelfristig ergänzt werden, um möglichst viele Sicherheitsvorfälle zu erkennen. Der Teil der Sicherheitsvorfälle, der nicht über technische Maßnahmen erkannt wird, kann durch organisatorische Maßnahmen ermittelt werden.

Für diese Erkennung muss eine zentrale Kontaktstelle eingerichtet sein, die die Meldung von Sicherheitsvorfällen entgegennimmt und entsprechende Maßnahmen einleitet. Die Maßnahmen und die Verantwortlichkeiten müssen sowohl für technisch als auch für organisatorisch erkannte Sicherheitsvorfälle geklärt sein. Zu den Maßnahmen gehört die Festlegung der Meldewege und die Benachrichtigung betroffener Stellen, aber auch die Dokumentation und Beweissicherung bei Sicherheitsvorfällen. Kurzfristig sollten daher die Verantwortlichkeiten und die Festlegung der Meldewege erfolgen. Zusätzlich sollten Checklisten für die Identifizierung von Sicherheitsvorfällen (in Abhängigkeit von der unternehmensspezifischen Definition) und zur Erhebung der Erstinformation aufgestellt und an die zentrale Kontaktstelle übergeben werden.

Welche Erstinformationen zu erfassen sind, kann exemplarisch dem Meldeverfahren des Bundes bei IT-Sicherheitsvorfällen (siehe Kapitel 6) entnommen werden.

Um einen Sicherheitsvorfall beheben zu können, muss dieser in einem ersten Schritt untersucht und bewertet werden. Der IT-Grundschutz empfiehlt in der Maßnahme „M 6.130 Erkennen und Erfassen von Sicherheitsvorfällen“ die Erfassung der Einflussfaktoren, um eine Bewertung durchführen zu können. Um einen Sicherheitsvorfall zu beheben, muss hierfür eine Strategie festgelegt werden. In Anlehnung an den IT-Grundschutz (Maßnahme „M 6.64 Behebung von Sicherheitsvorfällen“ und Maßnahme „M 6.61 Eskalation von Sicherheitsvorfällen“) sollte eine entsprechende Strategie kurzfristig entwickelt werden.

Mittelfristig muss die Vorgehensweise zur Behandlung von Sicherheitsvorfällen etabliert und entsprechend dokumentiert werden. Hierzu gehört auch die Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen. Der IT-Grundschutz listet in der Maßnahme „M 6.121 Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen“ die in einer Richtlinie zu berücksichtigenden Punkte auf. Basierend auf der Art des Sicherheitsvorfalls verweist die Maßnahme auf weitere benötigte Maßnahmen.

Mittelfristig ist zu empfehlen, ein entsprechendes Expertenteam im Unternehmen zu etablieren, welches mit der Behandlung von Sicherheitsvorfällen betraut ist. So müssen sowohl die Mitarbeiter des Expertenteams als auch die der zentralen Kontaktstelle, entsprechend geschult werden. Auch sollten Beweissicherungsmaßnahmen etabliert und die Experten entsprechend geschult sein.

Mittelfristig sollte das Unternehmen auch in der Lage sein, die Wiederherstellung der Betriebsumgebung zu gewährleisten. Diese Maßnahme muss konzeptionell erarbeitet, etabliert und entsprechend mit den Verantwortlichen geübt werden.

Langfristige Maßnahmen, wie die Einführung von Computer-Forensik[4], Nachbereitung von Sicherheitsvorfällen und Effizienzprüfung des Managementsystems zur Behandlung von Sicherheitsvorfällen, wie sie im IT-Grundschutz empfohlen werden, sollten erst nach der Aufstellung einer entsprechenden Vorgehensweise umgesetzt werden.

4.13 Notfallmanagement

Ein Notfall ist ein Schadensereignis, bei dem wesentliche Prozesse oder Ressourcen eines Unternehmens nicht wie vorgesehen funktionieren. Hier tritt, abweichend vom Sicherheitsvorfall und Störfall, das Schadensereignis tatsächlich ein. Um Notfällen vorzubeugen, ist der Aufbau und Betrieb eines Notfallmanagement-Prozesses notwendig. Nur ein geplantes und organisiertes Vorgehen garantiert eine optimale Notfallvorsorge und Notfallbewältigung. Dies verringert die Wahrscheinlichkeit des Auftretens eines Notfalls sowie dessen Auswirkungen und sichert somit das Überleben des Unternehmens. Es sind geeignete Präventivmaßnahmen zu treffen, die zum einen die Robustheit und Ausfallsicherheit der Geschäftsprozesse erhöhen und zum anderen ein schnelles und zielgerichtetes Reagieren in einem Notfall oder einer Krise ermöglichen.

4.13.1 Themen in den Interviews

Für die Beurteilung der Umsetzung des Notfallmanagements in den befragten Unternehmen wurden folgenden Kriterien betrachtet:

- **Notfallmanagement:** Zum Notfallmanagement gehören die Überprüfung der Organisationsstruktur und die Etablierung sowie Besetzung der Rollen im Notfallmanagement.
- **Notfallkonzept:** Das Notfallkonzept dokumentiert die identifizierten Risiken der Geschäftsprozesse und deren Bewertung. Weiterhin enthält das Notfallkonzept die Notfallpläne für Maßnahmen zum schnellen Wiederanlauf der kritischen Geschäftsprozesse unter der Berücksichtigung der Informationssicherheit.

4 Weitergehende Informationen zur Computer-Forensik können dem "Leitfaden IT-Forensik" [BSI_ITF] des BSI entnommen werden.

- **Einbindung der Mitarbeiter:** Die Einbindung der Mitarbeiter des Unternehmens in das Notfallmanagement erfolgt durch Verteilung der Informationen. Hierfür müssen die Mitarbeiter regelmäßig sensibilisiert werden. Weiterhin müssen die Mitarbeiter des Notfallteams speziell und regelmäßig geschult werden. Hierzu sollte ein gesondertes Schulungs- und Sensibilisierungskonzept zur Verfügung stehen.
- **Tests und Notfallübungen:** Der Notfall tritt immer unerwartet ein. Daher müssen regelmäßig Tests und Notfallübungen durchgeführt werden. Hierzu muss in erster Linie eine Grobplanung zur Abdeckung der wesentlichen Maßnahmen vorhanden sein, die bei Auftreten von Unstimmigkeiten aktualisiert wird. Zusätzlich sollte die Prüfung der USV und der Notstromversorgung im Rahmen solcher Übungen stattfinden. Diese bilden die Grundlage der IT-Systeme und sollten im Eintritt eines Notfalls verfügbar und funktionsfähig sein.

4.13.2 Ergebnisse

Die Ergebnisse für die befragten Unternehmen sind in der Abbildung 30 zusammenfassend dargestellt.

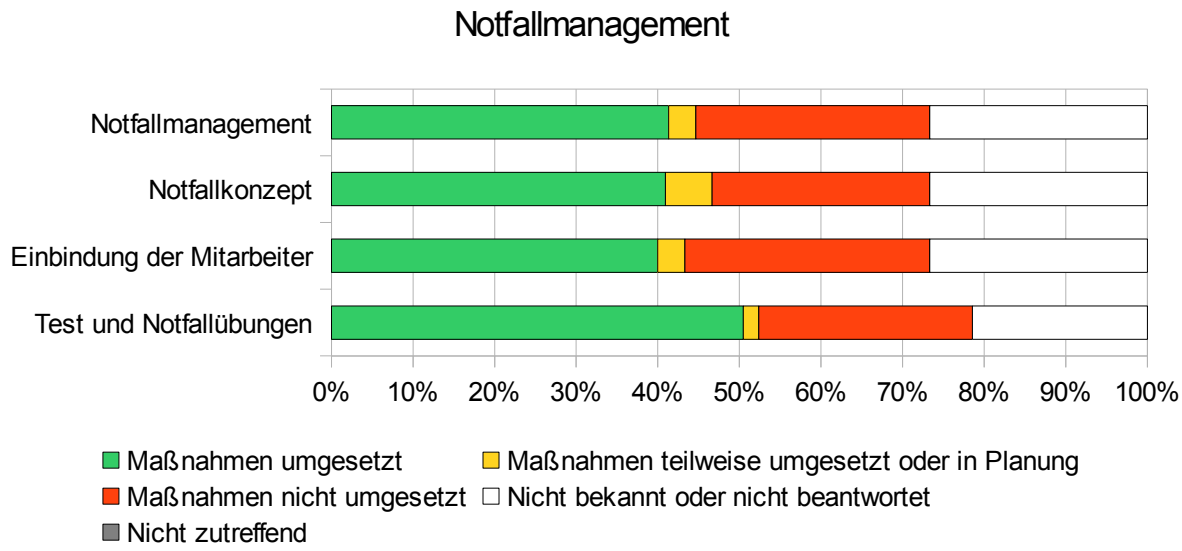


Abbildung 30: Auswertung Notfallmanagement

Insgesamt ist das Notfallmanagement bei weniger als der Hälfte der Unternehmen umgesetzt. Dies ist i.d.R. jedoch nicht durch Unwissenheit bedingt, sondern vielmehr durch die Einsparung von Kosten und die mangelhafte Einschätzung des zu tragenden Risikos. Dies wird auch dadurch deutlich, dass weit mehr als drei Viertel der Unternehmen angeben, mit einem Notfallkonzept vertraut zu sein. Hingegen haben nur die Hälfte der Unternehmen ein Notfallkonzept verfügbar. Somit kann davon ausgegangen werden, dass die Hälfte der Unternehmen ein Notfallmanagement teilweise oder vollständig aufgesetzt haben.

In der Befragung wurde zusätzlich deutlich, dass das Notfallmanagement als eine Einzelkomponente im Unternehmen betrachtet wird. So wird die Informationssicherheit im Rahmen

des Notfallmanagements bzw. des Notfallkonzepts nur noch bei knapp einem Drittel der Unternehmen berücksichtigt.

Die Einbindung der Mitarbeiter in das Notfallmanagement erfolgt bei knapp der Hälfte der befragten Unternehmen. Hier gaben die Unternehmen an, dass teilweise nur ein ausgewählter Mitarbeiterkreis über das Thema Notfall informiert wird. Die Verfügbarkeit eines Notfallteams und die regelmäßige Schulung und Sensibilisierung dieser Mitarbeiter anhand eines Konzepts erfolgt bei knapp einem Drittel der Unternehmen.

Auf spezifische Nachfrage hin führen mehr als die Hälfte der Unternehmen an, dass sie Tests und Notfallübungen durchführen. Diese finden jedoch unkoordiniert und voneinander losgelöst statt. Eine umfassende Planung aller durchzuführenden Tests und Übungen kann die Gewissheit über die Wirksamkeit der Maßnahmen erhöhen.

Insgesamt besteht dringender Handlungsbedarf bei der Realisierung eines Notfallmanagements in den befragten Unternehmen.

4.13.3 Handlungsempfehlungen

Als Basis für die Realisierung eines Notfallmanagements kann der Notfallmanagement-Prozess nach BSI Standard 100-4 initiiert werden. Hierfür muss in einem ersten Schritt die Leitungsebene die Verantwortung für ein Notfallmanagement übernehmen und den Geltungsbereich für das Notfallmanagement sowie die Notfallstrategie festlegen. Zur Festlegung des Geltungsbereichs und der Notfallstrategie gibt der IT-Grundschutz mit der Maßnahme „M 6.110 – Festlegung des Geltungsbereichs und der Notfallstrategie“ Hinweise. Für eine weitere Unterstützung der Unternehmensleitung kann auch bereits ein Notfallbeauftragter benannt werden, welcher nach der Initiierung des Notfallmanagements Mitglied des Notfallteams wird. So wie das Notfallteam durch die Unternehmensleitung benannt werden muss, wird auch die weitere Organisationsstruktur mit Rollen in der Notfallbewältigung benannt (vgl. IT-Grundschutz Maßnahme „M 6.112 – Aufbau einer geeigneten Organisationsstruktur für das Notfallmanagement“).

Erst nachdem alle Verantwortlichkeiten benannt sind und ihnen ausreichend Ressourcen zur Verfügung stehen, kann ein Notfallkonzept erstellt werden. Das Notfallkonzept dient der Umsetzung der Notfallstrategie und beschreibt die geplante Vorgehensweise. Dabei umfasst das Notfallkonzept sowohl das Notfallvorsorgekonzept als auch das Notfallhandbuch. Die detaillierte Umsetzung ist im IT-Grundschutz in der Maßnahme „M 6.114 Erstellung eines Notfallkonzepts“ und die Vorgehensweise zur Erstellung im BSI-Standard 100-4, Kapitel 5, beschrieben.

Mittelfristig sind die Notfallmanagement-Prozesse in das Unternehmen einzubinden. Um dies zu ermöglichen, müssen alle Mitarbeiter eines Unternehmens in die Notfallmanagement-Prozesse integriert werden. Dieses kann durch Schulungs- und Sensibilisierungsmaßnahmen erfolgen.

Sofern die Notfallmanagement-Prozesse umgesetzt sind, müssen langfristig regelmäßige Übungen eingeplant werden. Denn ein Notfall tritt zu einem unerwarteten Zeitpunkt auf, der kurzfristig oder aber auch erst nach langer Zeit eintreten kann. Die Übungen haben den Zweck der Wiederauffrischung des Wissens bei allen Beteiligten und die Prüfung der Praxistauglichkeit der Notfallmanagement-Prozesse. Sich hieraus ergebende Schwierigkeiten sollten eine Aktualisierung der Notfallmanagement-Prozesse zur Folge haben (vgl. IT-Grundschutz Maßnahmen „M 6.117 Tests und Notfallübungen“ und „M 6.118 Überprüfung und Aufrechterhaltung der Notfallmaßnahmen“).

Langfristig sollte eine Überprüfung und Steuerung des Notfallmanagement-Systems durch die Unternehmensleitung durchgeführt werden. Hierzu gehören regelmäßige und anlassbezogene Management-Berichte, damit eine Steuerung möglich ist. Eine detaillierte Beschreibung erfolgt im IT-Grundschutz in der Maßnahme „M 6.120 Überprüfung und Steuerung des Notfallmanagement-Systems“.

4.14 Aktualität der Informationen

Die einmalige Umsetzung von IT-Sicherheit bildet nur einen kurzfristigen Schutz des Unternehmens. So schnell, wie sich IT-Systeme ändern, so schnell ändern sich auch die Bedrohungen für ein Unternehmen. Nur durch regelmäßige Aktualisierung der Informationen und durch die regelmäßige Anpassung der Schutzmaßnahmen können diese einen längerfristigen Schutz des Unternehmens bieten. Hierfür müssen entsprechende Prozesse zur Aktualisierung der Informationen, aber auch zur Anpassung der Maßnahmen bestehen.

4.14.1 Themen in den Interviews

Um die Aktualität der Informationen in den verschiedenen Unternehmen bewerten zu können, wurden die folgenden Kriterien betrachtet:

- **Informationen zu Sicherheitsgefährdungen:** Informationen zu Sicherheitsgefährdungen können aus unterschiedlichen Stellen bezogen werden. Das Kriterium zeigt, inwieweit sich die befragten Unternehmen über Sicherheitsgefährdungen informieren.
- **IT-Sicherheitsleitfäden und -kriterien:** IT-Sicherheit ist mittlerweile ein internationales Thema. So sind verschiedene IT-Sicherheitsleitfäden und -kriterien entwickelt worden, die bei einer Realisierung von IT-Sicherheit in einer Institution unterstützen sollen. In diesen Ergebnissen wird die Verwendung von IT-Sicherheitsleitfäden und -kriterien im KMU-Bereich gezeigt.
- **Sicherheitsmanagement:** Sofern sich Informationen ändern, müssen entsprechende Änderungen in den Schutzmaßnahmen und Prozessen durchgeführt werden. Ein Sicherheitsmanagement dient als regelmäßiger Prozess zur Aktualisierung von Prozessen und Informationen. Da diese individuell für jedes Unternehmen erstellt werden, ist auch das Sicherheitsmanagement individuell. Übergreifend werden die Ergebnisse für die Aktualisierung von Sicherheitskonzepten, Sicherheitszielen und -strategien sowie die Durchführung von Sicherheitsrevisionen und -audits dargestellt.

4.14.2 Ergebnisse

Die Abbildung 31 zeigt die zusammengefassten Ergebnisse zu den genannten Kriterien.

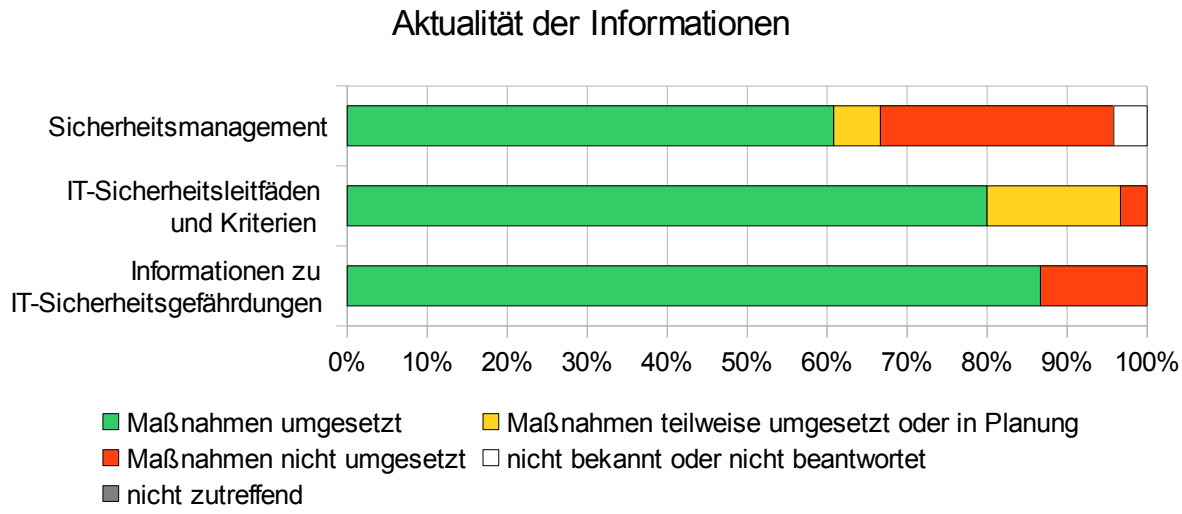


Abbildung 31: Auswertung Aktualität der Informationen

Das Sicherheitsmanagement wird von zwei Dritteln der Unternehmen umgesetzt. So sind bei der Mehrheit der Unternehmen die IT-Konzepte auf dem aktuellen Stand und werden regelmäßig aktualisiert. Die Aktualisierung der Sicherheitsziele und -strategien hingegen wird von weniger als der Hälfte der Unternehmen zeitnah und von weiteren zehn Prozent mit einem Zeitabstand von mehr als zwei Jahren vorgenommen. Die zugehörigen Sicherheitsrevisionen und -audits werden ebenfalls von zwei Dritteln der Unternehmen realisiert.

Die Orientierung an Sicherheitsleitfäden und Kriterien führen 80 Prozent der Unternehmen bereits heute durch. Weitere Unternehmen planen die Orientierung an bekannten Sicherheitsleitfäden. Die befragten Unternehmen orientierten sich am häufigsten an IT-Grundschutz, ISO 2700x und ISO 900x. Weitere Sicherheitsleitfäden und -kriterien werden in Abhängigkeit von Geschäftsprozessen eingesetzt.

Alle befragten Unternehmen informieren sich regelmäßig über den Stand von möglichen Sicherheitslücken und Vorfällen. Als Quellen werden hierfür verschiedenste Internetseiten verwendet. Das Informationsangebot des BSI nutzen rund 70 Prozent der befragten Unternehmen.

4.14.3 Handlungsempfehlungen

Ziel der Unternehmen sollte ein stets aktueller Stand der Informationen zu IT-Sicherheitsthemen sein. Durch die Nutzung des Internets werden Informationen zeitnah verteilt. Hier können verschiedenste Webseiten genutzt werden. Allerdings muss der Leser dieser Webseiten die Informationen korrekt einschätzen können. Als Alternative kann das CERT des BSI genutzt werden. Hier werden die Informationen vor der Veröffentlichung geprüft. Sofern die Vorfälle behoben werden können, werden passende Informationen zusätzlich veröffentlicht. Durch die Abonnement-Funktion werden die Informationen automatisiert per E-Mail an die zu informierende Person zugestellt. Somit entfällt das aktive Suchen auf der Webseite.

Langfristig sollten entsprechende Prozesse für die Optimierung des Sicherheitsmanagements umgesetzt werden. Hilfestellung bieten die Sicherheitsleitfäden wie IT-Grundschutz und ISO

2700x. Viele Sicherheitsleitfäden gehen nach dem PDCA-Zyklus vor. Hier wird eine regelmäßige Prüfung und Verbesserung vorgeschlagen.

4.15 Geschäftsprozesse

Funktionierende Geschäftsprozesse sind die Basis für den Erhalt eines Unternehmens. So werden über Geschäftsprozesse die individuellen Leistungen eines Unternehmens abgebildet. Jedes Unternehmen sollte in der Lage sein, die eigenen Geschäftsprozesse zu benennen, sowie deren Kritikalität einzustufen. Besonders kritische Geschäftsprozesse sind zu schützen. Entfällt ein kritischer Geschäftsprozess, so kann die Existenz eines Unternehmens gefährdet sein.

4.15.1 Themen in den Interviews

Die folgenden Kriterien werden für die Einschätzung der Geschäftsprozesse der befragten Unternehmen herangezogen:

- **Kritische Geschäftsprozesse benennen:** Die IT-Leitung muss über kritische Geschäftsprozesse informiert sein und deren Kritikalität sollte bekannt sein.
- **Risiko kritischer Geschäftsprozesse:** Für die Geschäftsprozesse wurde eine Risikobewertung durchgeführt, die nicht älter als zwei Jahre ist.
- **Schutz kritischer Geschäftsprozesse:** Für den Schutz der kritischen Geschäftsprozesse muss der Bedarf ermittelt werden und entsprechende Schutzmaßnahmen umgesetzt sein.
- **Kritische Ressourcen (Personal):** Kritische Ressourcen in Form von Personal im Unternehmen können Geschäftsprozesse beeinflussen. Sofern kritisches Personal im Unternehmen vorhanden ist, müssen Maßnahmen ergriffen werden, um das Risiko zu minimieren.

4.15.2 Ergebnisse

Die Unternehmen wurden hinsichtlich ihrer Geschäftsprozesse im Rahmen der Studie befragt. Die Ergebnisse werden in der Abbildung 32 zusammenfassend dargestellt.

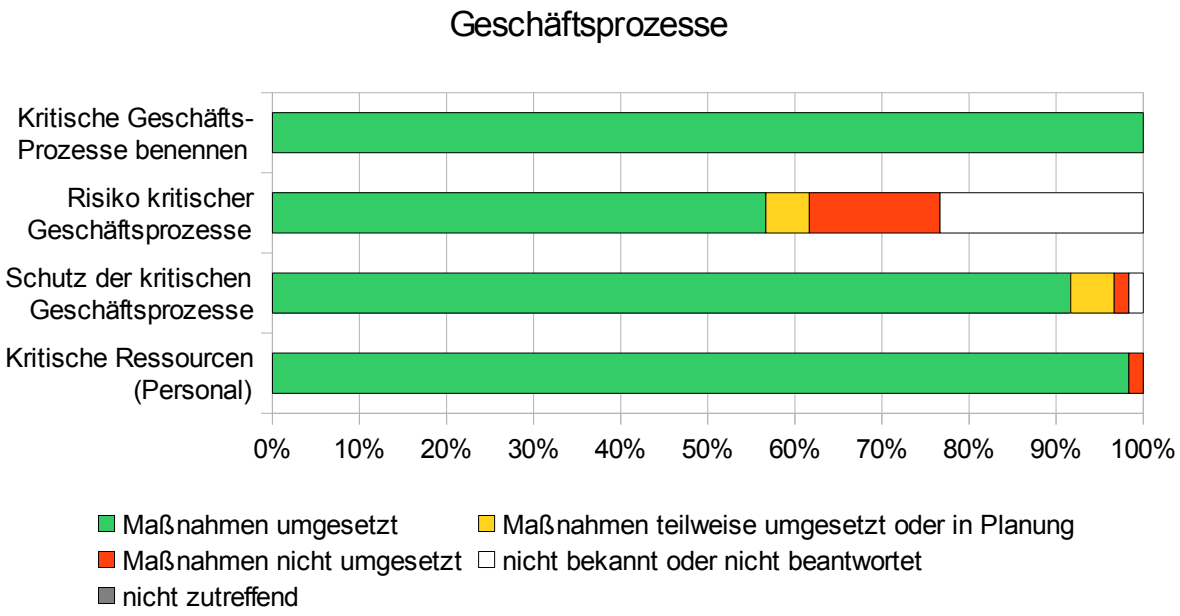


Abbildung 32: Auswertung Geschäftsprozesse

Insgesamt kann die IT-Leitung sehr gut über Geschäftsprozesse und kritische Geschäftsprozesse Auskunft geben. So sind alle IT-Leiter der befragten Unternehmen über die kritischen Geschäftsprozesse informiert. Jedoch kann das Risiko häufig nicht eingeschätzt werden. Hier fehlen in vielen Unternehmen die Risikobetrachtungen zu kritischen Geschäftsprozessen. Auch wissen einige IT-Leiter nicht, ob seitens des Managements eine Risikobetrachtung durchgeführt wurde.

Die Umsetzung von Maßnahmen, um den Schutz der kritischen Geschäftsprozesse zu gewährleisten, wird als gut bis sehr gut eingeschätzt. Bei den Gesprächen konnte ermittelt werden, dass die Motivation sehr hoch ist, die kritischen Geschäftsprozesse noch stärker zu schützen. Kleinere Defizite bei den Schutzmaßnahmen werden eingeräumt und deren zeitnahe Behebung in Aussicht gestellt.

Kritische Ressourcen konnten ebenfalls fast alle IT-Leiter einschätzen. Hierbei wurde mehrheitlich die IT-Leitung selbst als die kritische Ressource identifiziert. Sowohl Management als auch IT-Leitung ergreifen Maßnahmen wie qualifizierte Vertreterregelung, Dokumentation von Prozessen und Kennwörtern und Einbindung externer Dienstleister, um das Risiko zu minimieren.

4.15.3 Handlungsempfehlungen

Für einen zeitnahen Schutz müssen die kritischen Geschäftsprozesse vollständig identifiziert und deren Schutzbedarf kurzfristig festgelegt werden. Dies ist die Grundlage um das Risiko eines Ausfalls von kritischen Geschäftsprozessen zu minimieren. Sofern Schutzmaßnahmen bestehen, sind diese zusätzlich zu kontrollieren und bei Bedarf zu aktualisieren.

Mittelfristig sollten Prozesse für regelmäßige Kontrollen und Neubewertungen im Unternehmen etabliert werden. Somit wird erreicht, dass der Schutzbedarf der kritischen Geschäftsprozesse angepasst wird. Folglich müssen die Sicherheitsmaßnahmen aktualisiert werden.

4.16 Bewertung der Gefahrenbereiche

Gefahren drohen einem Unternehmen jederzeit. Dabei kann sich das Unternehmen nicht komplett gegen alle Gefahren absichern. Ein mögliches Restrisiko bleibt immer bestehen. Um das Risiko einschätzen zu können, müssen die Gefahren bewertet werden. Bei Gefahren werden dabei vier Klassen unterschieden – menschliches Fehlverhalten, technische Mängel, organisatorische Mängel und höhere Gewalt.

4.16.1 Themen in den Interviews

Die folgenden Kriterien werden für die Einschätzung in Bezug auf die Bewertung der Gefahrenbereiche der befragten Unternehmen herangezogen:

- **Regelmäßige Bewertung der Gefahrenbereiche:** Das Kriterium zeigt, ob die Unternehmen regelmäßig eine Bewertung der Gefahrenbereiche vornehmen, wobei die Bewertung nicht älter als 3 Jahre ist.
- **Bedeutung der Gefahrenbereiche:** Die Bedeutung für das Unternehmen kann durch die Geschäftsleitung wie auch die IT-Leitung für jeden der vier Gefahrenbereiche benannt werden.
- **Vorfälle in den Gefahrenbereichen:** Die Unternehmen können angegeben, ob und welche Gefahren zu Vorfällen geführt haben.

4.16.2 Ergebnisse

Die Bedeutung der Gefahrenbereiche für das Unternehmen wurde durch direkte Fragestellungen sowohl bei der IT-Leitung wie auch der Geschäftsführung ermittelt. Das Ergebnis zur Bewertung der Gefahrenbereiche für die befragten Unternehmen ist in der Abbildung 33 dargestellt.

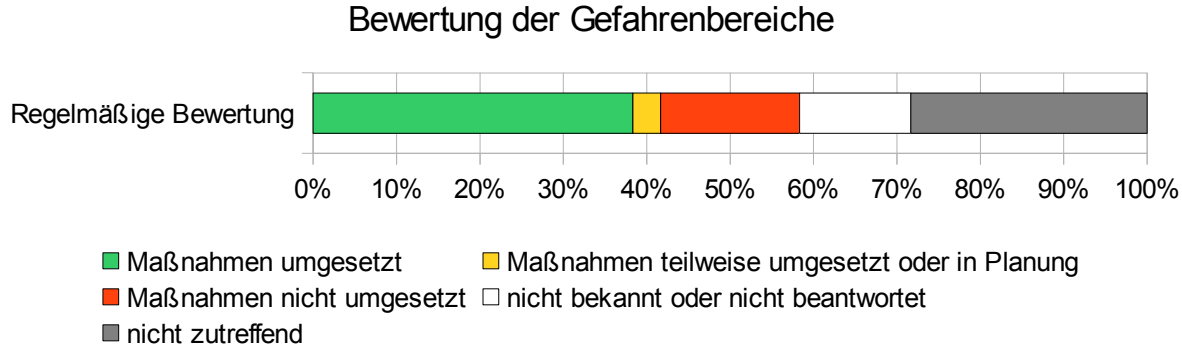


Abbildung 33: Auswertung Gefahrenbereiche

Die Auswertung ergibt, dass lediglich 40 Prozent der Unternehmen die Gefahrenbereiche regelmäßig bewerten. Die Bedeutung der Gefahrenbereiche wird hierbei von IT-Leitung und Management in nahezu identischer Form eingeschätzt. Die Abbildung 34 zeigt die Einschätzung von Management (blau) und IT-Leitung (rot) zu den vier Gefahrenbereichen.

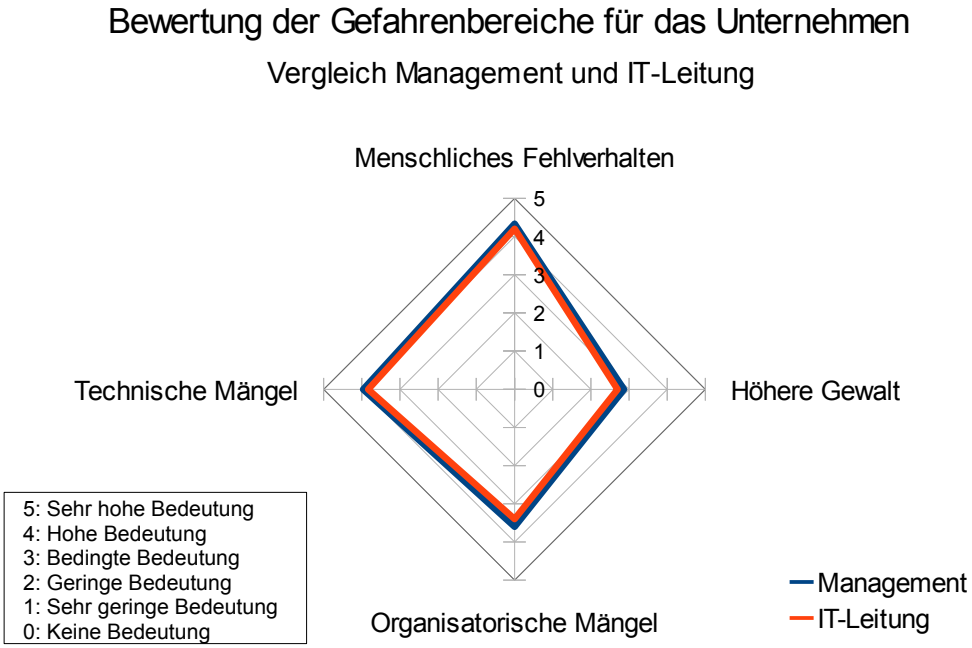


Abbildung 34: Bewertung der Gefahrenbereiche im Vergleich IT-Leitung und Management

Insgesamt schätzen sowohl IT-Leitung als auch Management das menschliche Fehlverhalten als die höchstmögliche Gefahr für das Unternehmen ein. Das Risiko in Bezug auf technische und organisatorische Mängel wird um jeweils 0,4 Punkte geringer eingestuft. Der Gefahrenbereich höhere Gewalt wird mit dem geringsten Risiko für das Unternehmen bewertet.

Dieses Ergebnis resultiert aus den Gefahren, die in der Vergangenheit und nach Erfahrung der Befragten bereits zu Vorfällen geführt haben. Von den befragten Unternehmen hat bereits bei 77 Prozent eine Gefahr zu einem Vorfall geführt (vgl. Abbildung 35).

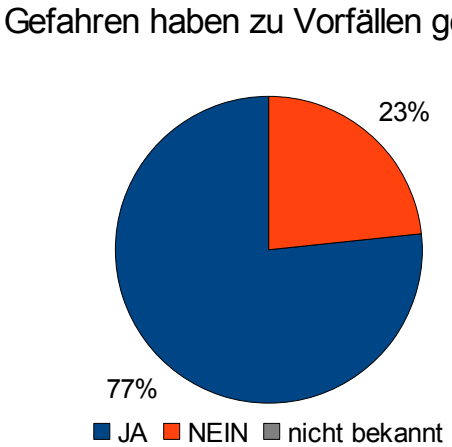


Abbildung 35: Gefahren haben zu Vorfällen geführt

Die Frage nach dem Auftreten von Vorfällen war dabei nicht zeitlich eingeschränkt; die Antworten reflektieren den Kenntnisstand der Befragten über die Unternehmenshistorie.

Für die Ermittlung der Schwere des Vorfalls wurden die Umstände, die zu einem Vorfall geführt haben, erläutert. Das allgemeine Ergebnis ist in der Abbildung 36 dargestellt.

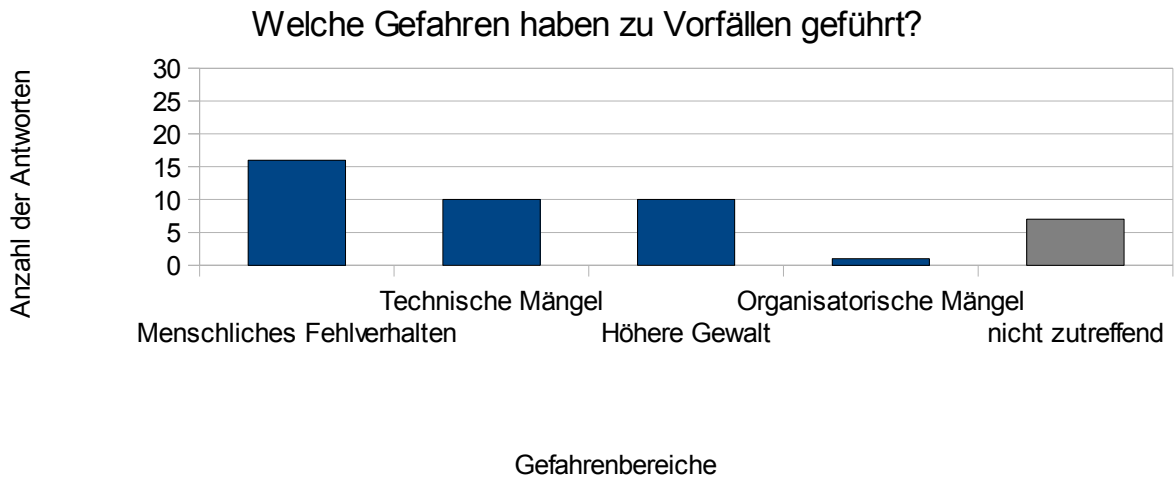


Abbildung 36: Gefahren die zu Vorfällen geführt haben

Die häufigste Gefahr, die zu einem Vorfall geführt hat, ist menschliches Fehlverhalten. So berichteten verschiedene Unternehmen von Verlust oder Diebstahl von Daten.

Allerdings haben auch technische Mängel und höhere Gewalt in gleicher Anzahl zu Vorfällen geführt. Gemäß der Erläuterung der Befragten wurden in diesen Fällen sofort Sicherheitsmaßnahmen etabliert, um einen erneuten Vorfall aufgrund dieser Gefahrenbereiche zu vermeiden.

Lediglich ein Unternehmen gab an, dass es aufgrund organisatorischer Mängel zu einem Vorfall im Unternehmen gekommen ist.

4.16.3 Handlungsempfehlungen

Für die Vermeidung möglicher Vorfälle aufgrund der vier Gefahrenbereiche wird empfohlen, im Unternehmen eine entsprechende Bewertung des Gefährdungspotentials vorzunehmen. Hierbei ist das Risiko eines jeden Gefahrenbereichs zu ermitteln und dem entsprechend Gegenmaßnahmen zu ergreifen. Dabei sind die Maßnahmen in der Reihenfolge des Eintrittsrisikos zu priorisieren und umzusetzen.

Langfristig sollte ein Prozess zur regelmäßigen Bewertung der Gefahrenbereiche entwickelt werden. Somit können bei Veränderung der Risikobewertung vorbeugend Maßnahmen zum Schutz des Unternehmens ergriffen werden.

4.17 Reifegrade

IT-Sicherheitsmanagement muss sich auf zyklische Prozesse stützen, um effektiv zu sein. Die Prozesse sind jedoch nur dann dauerhaft nutzbar, wenn deren Qualität (Erfolg) gemessen und die zukünftige Entwicklung gesteuert wird. Prozesse, deren Abläufe nicht festgelegt oder deren Veränderungen das Ergebnis von „trial-and-error“ sind, werden über kurz oder lang zu Fehlern in den Abläufen und damit zu Lücken im IT-Sicherheitsmanagement führen.

Dagegen bilden Prozesse, die auf der Basis strukturierter und dokumentierter Beschreibungen gelebt werden, die aufeinander abgestimmt und deren Rollen und Verantwortlichkeiten geregelt sind, die Grundlage für ein belastbares IT-Sicherheitsmanagement. Nur eine fortlaufende Bewertung der Qualität sowie ggf. Nachjustierung der Prozesse kann mittel- bis langfristig deren erfolgreiche Anwendung sicherstellen.

4.17.1 Ergebnisse

Die im Rahmen der Reifegrade nachfolgend betrachteten Bereiche sind gemäß der in Kapitel 3.3.1 definierten Struktur gruppiert. Die jeweilige Zuordnung ist den untenstehenden Bereichsdefinitionen zu entnehmen. Von den insgesamt sechzehn Themenkomplexen werden bis auf Sicherheitsprozesse und Zukunftsthemen alle Themen nach ihren Reifegraden bewertet. Die Sicherheitsprozesse als Querschnittsthema werden bereits in der Bewertung der Einzelthemen betrachtet und die Zukunftsthemen sind als solche nicht über Reifegrade auszuwerten. In den einzelnen Bereichen werden die den Themenkomplexen (siehe Kapitel 4.3 bis 4.16) zugeordneten Teilgebiete über alle Unternehmen ausgewertet.

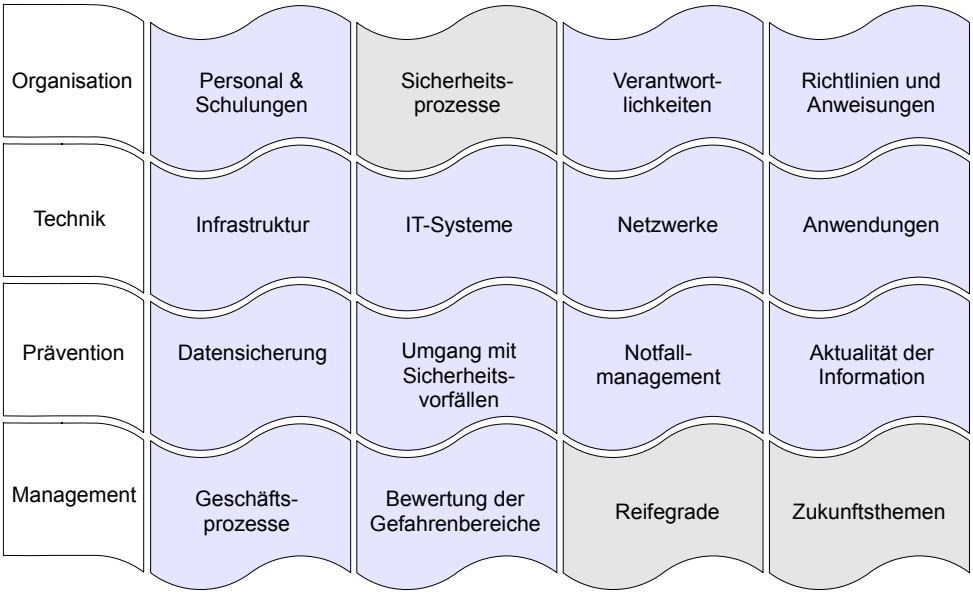


Abbildung 37: Gruppierung der Themenkomplexe

Zur Einschätzung der Reifegrade der IT-Sicherheitsprozesse in den befragten Unternehmen werden die folgenden Bereiche betrachtet:

- **Management und Organisation:** Neben dem Bereich Personal und Schulungen werden die Reifegrade der übergeordneten Management- und Organisationsprozesse in Bezug auf die Verantwortlichkeiten sowie die Richtlinien und Anweisungen betrachtet. Zusätzlich werden die Aspekte der Risikobewertung in Verbindung mit der Bewertung der für die Unternehmen relevanten Gefahrenbereiche als Aufgaben für Management und Organisation ausgewertet.
- **Technik (Infrastruktur, IT-Systeme, Netze und Anwendungen):** Es werden die Prozessreifegrade in Bezug auf die baulich-technischen Gegebenheiten am Hauptstandort des Unternehmens, den IT-Systemen, der Vernetzung der IT-Systeme sowie der Kommunikationsanwendung E-Mail ausgewertet.
- **Prävention:** Untersucht werden die, den übergeordneten Management- und Organisationsthemen zuzuordnenden, präventiven Sicherheitsmaßnahmen zum Datenerhalt durch Datensicherung, das Sicherheitsvorfall- und Notfallmanagement sowie die Aktualität der Informationen in Bezug auf gegenwärtige und zukünftige Bedrohungsszenarien.

Die strukturierte Analyse erfolgte im Rahmen der Interviews mit den IT-Verantwortlichen und gibt somit die IT-interne Sichtweise wieder. Die Bewertung erfolgte anhand der in Tabelle 1 aufgeführten Kriterien. Hierbei ergibt das arithmetische Mittel der Einzelbewertungen den Gesamtreifegrad pro Thema.

4.17.1.1 Management und Organisation

Das Ergebnis[5] der Bewertung der Prozessreifegrade im Bereich Management und Organisation ist dem nachfolgenden Diagramm zu entnehmen.

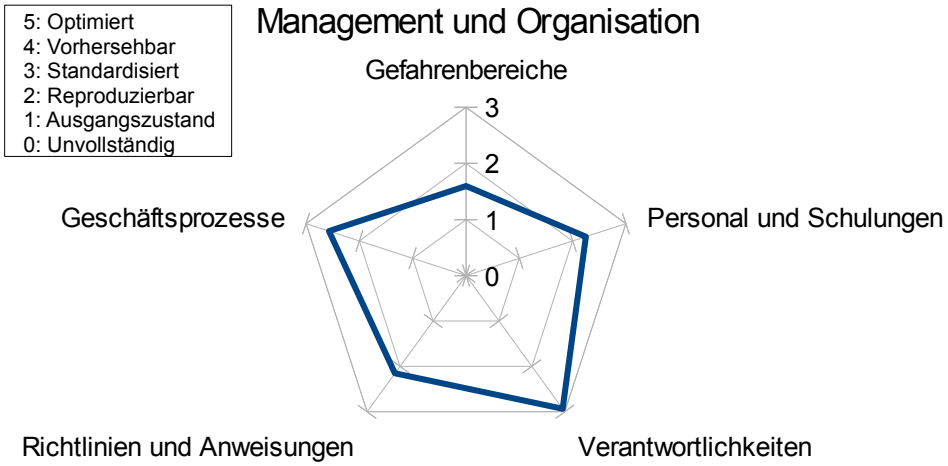


Abbildung 38: Reifegradbetrachtung der Management- und Organisationsprozesse

Wie aus Abbildung 38 ersichtlich, wurde in keinem Teilgebiet ein Gesamtreifegrad der Ebenen 4 (vorhersehbar) oder 5 (optimiert) erreicht.

5 Es werden zur besseren Lesbarkeit nur die Wertebereiche 0 bis 3 aus der bis 5 reichenden Skala dargestellt.

Bei der Festlegung der Verantwortlichkeiten haben die Unternehmen einen insgesamt standardisierten Prozess erreicht. Veränderungen bei den Rollen und Verantwortlichkeiten werden in einem geregelten Prozess vorgenommen. Eine Standardisierung des Prozesses haben knapp drei Viertel der befragten Unternehmen vorgenommen.

Es zeigen sich deutliche Schwächen bei den Prozessen zur Prüfung auf Einhaltung von Richtlinien und Anweisungen. Dies gilt ebenfalls für die Prozesse zur Definition, Aktualisierung und Bekanntmachung der IT-Sicherheitsziele und -strategie der Unternehmen. Hier sind im Mittel bei zwei Drittel der Unternehmen keine bzw. unzureichend geregelte Prozesse umgesetzt. Die Aktualität des Kenntnisstandes der Mitarbeiter in Bezug auf IT-Sicherheitsziele und -strategien kann nicht dauerhaft sichergestellt werden. Obwohl die Hälfte der Unternehmen die vorhandenen Richtlinien und Anweisungen fortlaufend auf Eignung prüft und ggf. ergänzt, ist nur bei knapp 25 Prozent der Betriebe ein Prozess zur Prüfung auf Einhaltung etabliert. Bei knapp der Hälfte der Unternehmen ist dieser Prozess noch nicht initiiert worden.

Der Prozess zur fortlaufenden Risikobewertung der Geschäftsprozesse ist in etwas mehr als der Hälfte der Unternehmen etabliert. Bei knapp 26 Prozent wird dieser Prozesse sogar fortlaufend optimiert. Dagegen haben knapp ein Drittel der Unternehmen keinen Prozess zur Risikobewertung aufgesetzt.

Ein standardisierter Prozess zur fortlaufenden Bewertung der Gefahrenbereiche (menschliches Fehlverhalten, technische oder organisatorische Fehler sowie höhere Gewalt) ist in knapp 40 Prozent der Unternehmen etabliert. Dieser wird jedoch nur in 13 Prozent der Betriebe fortlaufend optimiert. Bei etwas mehr als der Hälfte der Unternehmen ist kein Prozess zur Bewertung der Gefahrenbereiche vorhanden.

Im Bereich Personal und Schulungen zeigen sich Schwächen insbesondere bei den Prozessen rund um die Schulungen zu IT-Sicherheitsmaßnahmen. Sind die Prozesse im Bereich der Betreuung der Mitarbeiter noch von 60 Prozent der Unternehmen als standardisiert anzusehen, haben nur ein Drittel der Betriebe diesen Reifegrad bei den IT-Sicherheitsschulungen erreicht. Bei 56 Prozent der Unternehmen ist eine Wiederholbarkeit der Prozesse nicht sichergestellt bzw. kein Prozess initiiert.

Insgesamt ist festzustellen, dass die Prozesse im Bereich Management und Organisation nur partiell standardisiert sind. Eine Optimierung findet nur in wenigen Unternehmen statt. Insbesondere die Prozesse zur Bewertung der Gefahrenbereiche sind in der Mehrzahl der Unternehmen nicht aufgesetzt.

4.17.1.2 Infrastruktur, IT-Systeme, Netze und Anwendungen

Das Ergebnis[6] der Bewertung der Prozessreifegrade im Bereich Infrastruktur, IT-Systeme, Netze und Anwendungen ist der Abbildung 39 zu entnehmen.

6 Es werden zur besseren Lesbarkeit nur die Wertebereiche 0 bis 3 aus der bis 5 reichenden Skala dargestellt.

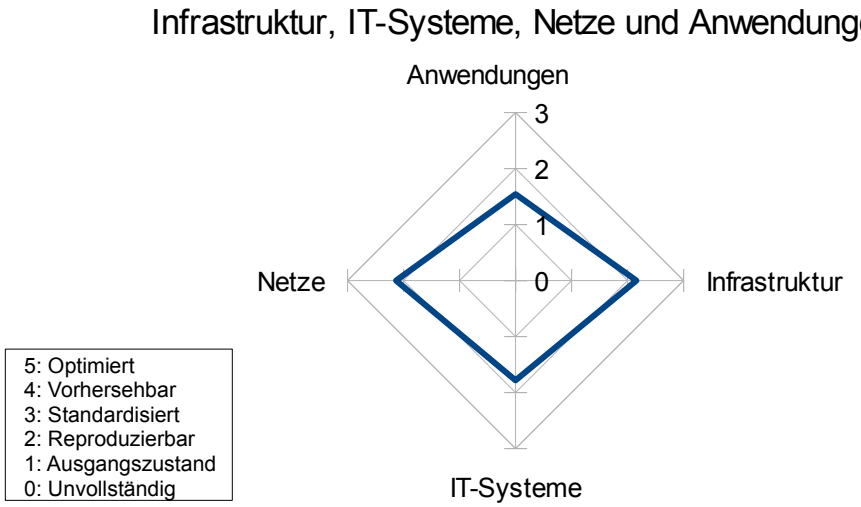


Abbildung 39: Reifegradbetrachtung der Infrastruktur, IT-Systeme, Netze und Anwendungen

Im Bereich der Infrastruktur haben zwei Drittel der Unternehmen die Prozesse zur Absicherung der Serverräume und etwas mehr als die Hälfte der Betriebe die Prozesse zur Handhabung der Besucher-, Veranstaltungs- und Schulungsräume standardisiert. Dagegen ist bei der Hälfte der Unternehmen die Absicherung der Gebäude gegen unbefugten Zutritt nicht dokumentiert bzw. die Dokumente sind nicht aktuell. Ein langfristiger Schutz der Betriebsräume kann somit nicht gewährleistet werden.

Die Prozesse zum Schutz der auf den mobilen Endgeräte gespeicherten Daten sowie die Absicherung gegen unkontrollierte Datentransfers haben rund ein Drittel der Unternehmen geeignet umgesetzt, also standardisiert. Die verbleibenden zwei Drittel haben die erforderlichen Prozesse nicht initiiert – mindestens ein Drittel der Unternehmen – bzw. nicht ausreichend standardisiert.

Im Rahmen der fortlaufenden Bewertung der Redundanz der kritischen Systeme haben 40 Prozent der Unternehmen die erforderlichen Prozesse zur Strukturierung und Dokumentation definiert. Bei der Hälfte der Unternehmen ist die Wiederholbarkeit nicht gewährleistet, das heißt, die notwendigen Beschreibungen sind nicht vorhanden bzw. nicht aktuell. Von diesen 50 Prozent haben 20 Prozent überhaupt keinen Prozess initiiert.

Die VPN-Nutzung ist bei knapp über 50 Prozent der Unternehmen ausreichend dokumentiert. Die Prozesse sind etabliert.

Während im Bereich der Virenscanner (Content-Sicherheit) die Prozesse zur langfristigen Absicherung der Schutzmechanismen bei knapp der Hälfte der Unternehmen standardisiert sind, gilt dies im Bereich der E-Mail-Archivierung nur für ein Drittel der Unternehmen. Von 20 Unternehmen, die angaben, eine E-Mail-Archivierung durchzuführen, sind bei zehn Unternehmen – also der Hälfte – keine Prozesse hierzu vorhanden. Eine gesicherte E-Mail-Kommunikation nutzen knapp die Hälfte der Unternehmen. Einen standardisierten und belastbaren Prozess hierzu haben nur 20 Prozent der Betriebe umgesetzt.

Insgesamt zeigt sich ein deutlicher Handlungsbedarf in allen betrachteten Bereichen. Insbesondere die Schwächen in Bezug auf die mobilen Endgeräte, die Sicherstellung der Wirksamkeit einer Zutrittskontrolle sowie im Bereich der E-Mail-Kommunikation können die Bedrohungslage für das Unternehmen mittel- bis langfristig verschärfen.

4.17.1.3 Präventionsmaßnahmen

Die nachfolgende Abbildung stellt das Ergebnis[7] der Prozessreifegrade in Bezug auf die Präventionsmaßnahmen dar.

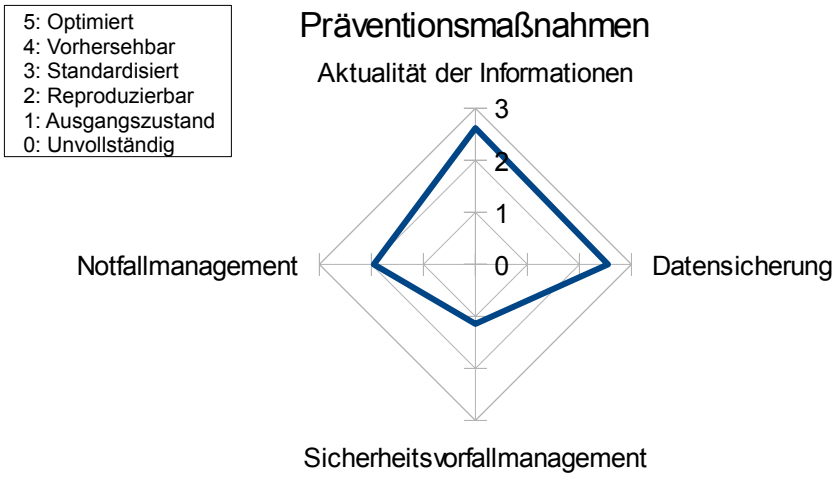


Abbildung 40: Reifegradbetrachtung der Präventionsprozesse

Nahezu alle Unternehmen haben Prozesse etabliert um die Aktualität der Informationen zur Bedrohungslage, zu Schwachstellen und Sicherheitsupdates gewährleisten zu können. Es können jedoch nur zwei Drittel der Unternehmen bei der Umsetzung neuer Erkenntnisse auf standardisierte Prozesse in der Adaption der Sicherheitskonzepte zurückgreifen. Prozesse zur Verifizierung der IT-Sicherheitskonzepte durch qualifizierte externe Personen in Form von Revisionen oder Audits sind bei der Hälfte der Unternehmen etabliert. Bei lediglich 20 Prozent der Unternehmen wird die Prozessqualität fortlaufend gemessen und die Prozesse im Bedarfsfall nachjustiert.

Im Bereich der Datensicherung sind im Mittel bei zwei Drittel der Unternehmen die Prozesse zur Prüfung des Aufbewahrungsortes sowie zur regelmäßigen Prüfung der Wiederherstellbarkeit der Datensicherungen standardisiert. Dagegen ist bei knapp 27 Prozent der Unternehmen die Wiederholbarkeit dieser Prozesse nicht sichergestellt bzw. sind diese noch nicht initiiert worden.

Das Notfallmanagement ist bei weniger als der Hälfte der Unternehmen umgesetzt worden (siehe Kapitel 4.13). Die Unternehmen, welche das Notfallmanagement aufgebaut haben, haben auch die notwendigen Prozesse aufgesetzt. So sind die Prozesse zur Erstellung und Aktualisierung des Notfallkonzepts in knapp über einem Drittel der Betriebe etabliert. Die erforderlichen Notfalltests und -übungen sind in etwas mehr als 40 Prozent der Fälle standardisiert. In 13 Prozent der Unternehmen wird die Qualität der Notfalltests und -übungen fortlaufend gemessen und der Prozess ggf. optimiert.

Die Prozesse im Bereich des Sicherheitsvorfallmanagements unterstreichen die bereits bei der Bewertung der Sicherheitsmaßnahmen (siehe Kapitel 4.12) identifizierten Schwächen der Unternehmen. So ist nur bei einem Drittel der Betriebe ein standardisierter Prozess im Bereich der Detektion von Sicherheitsvorfällen etabliert. Hier erfolgt eine regelmäßige Überprüfung und Überwachung der eingesetzten Detektionsmaßnahmen. Dagegen ist in mindestens zwei Drittel der Unternehmen eine Wiederholbarkeit der Vorgehensweise bei einem Sicherheitsvorfall nicht

7 Es werden zur besseren Lesbarkeit nur die Wertebereiche 0 bis 3 aus der bis 5 reichenden Skala dargestellt.

gegeben. Dies begründet sich dadurch, dass zwei Drittel der Betriebe keine Definition eines Sicherheitsvorfalls sowie keine Richtlinien zur Behandlung eines Sicherheitsvorfalls vorweisen können.

Insgesamt ist festzustellen, dass im Bereich des Notfall- und Sicherheitsvorfallmanagements die größten Defizite aus Prozesssicht liegen. In großen Teilen sind hier die Prozesse noch nicht initiiert bzw. eine Wiederholbarkeit nicht gegeben.

4.17.1.4 Vergleich der Einschätzungen

Im Rahmen der Datenerhebung wurden getrennte Interviews mit der Geschäftsführung sowie den IT-Verantwortlichen der Unternehmen unter Verwendung angepasster Interviewbögen durchgeführt. Beide Interviewbögen enthielten teils identische Fragestellungen, um Vergleichswerte in Bezug auf die in der nachfolgenden Abbildung aufgezeigten Themen zur erhalten.

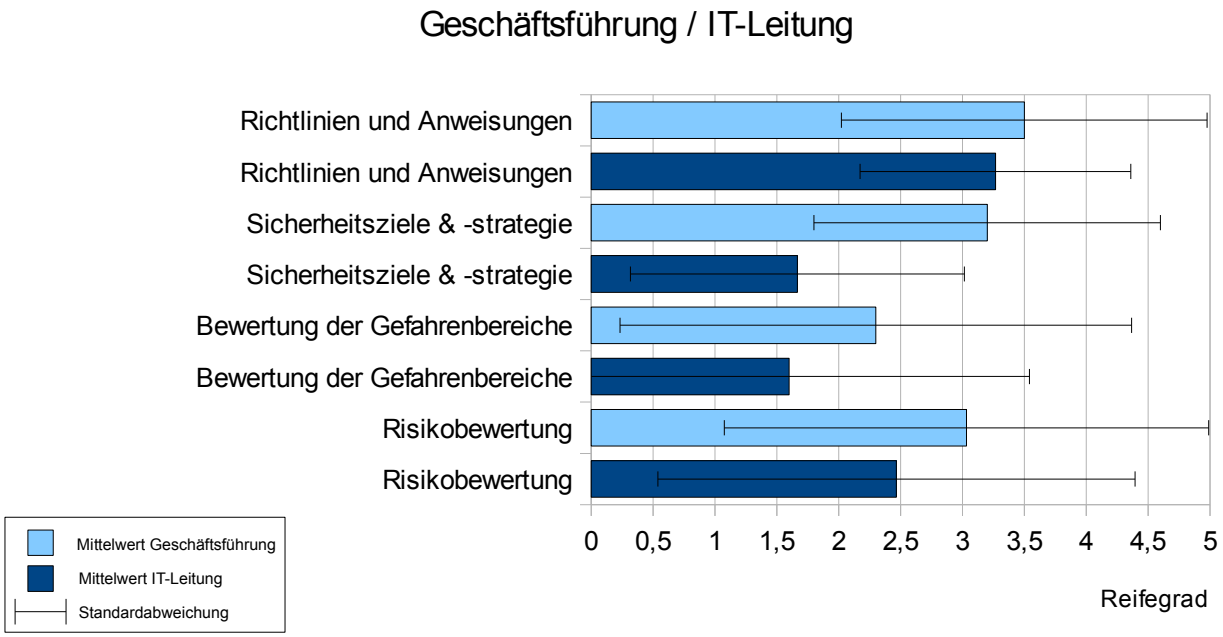


Abbildung 41: Vergleich der Einschätzungen von Geschäftsführung und IT-Leitung

Die in Abbildung 41 dargestellten Prozessreifegrade wurden als arithmetischer Mittelwert über alle zum Themengebiet gestellten prozessualen Fragen ermittelt. Zusätzlich wurde die Standardabweichung gemäß der deskriptiven Statistik berechnet.

Deutlich sichtbar sind die Unterschiede bei der Einschätzung in Bezug auf die Aktualität und Gültigkeit der unternehmensweiten Sicherheitsziele und -strategien. Aus Sicht der Geschäftsführung handelt es sich hier um einen etablierten und standardisierten Prozess, während die IT-Leitung diesen als nicht reproduzierbar ansieht. Ähnlich, wenn auch nicht mit gleich großem Unterschied ist die Einschätzung der Prozesse zur Bewertung der Gefahrenbereiche gelagert. Während die Geschäftsführung diese als wiederholbar ansieht, kommen die IT-Verantwortlichen zu einer gegenteiligen Einschätzung.

Eine deutlich höhere Übereinstimmung wird im Bereich der Risikobewertung der Geschäftsprozesse und bei den Richtlinien und Anweisungen erreicht. Gehen beide Parteien bei den

Richtlinien und Anweisungen von standardisierten Prozessen aus, gilt dies bei der Risikobewertung der Geschäftsprozesse nur für die Geschäftsführung. Hier sehen die IT-Verantwortlichen die Wiederholbarkeit noch nicht als gegeben an.

Insgesamt ist festzustellen, dass es bei den eher auf die Geschäftsführung bezogenen Themen, wie der Definition der IT-Sicherheitsziele und -strategien, der Risikobewertung der Geschäftsprozesse und der Bewertung der Gefahrenbereiche, einen erhöhten Abstimmungsbedarf zwischen der Geschäftsführung und den IT-Verantwortlichen gibt.

Des Weiteren ist die Bandbreite der Einschätzungen, dargestellt über die Standardabweichung, auffällig. Diese ist in den Bereichen mit dem erhöhten Abstimmungsbedarf am stärksten ausgeprägt. Die Einschätzungen lagen hier bei mindestens einem Drittel der Unternehmen um drei Ebenen auseinander. Während z.B. die Geschäftsführung einen Prozess insgesamt als standardisiert (Ebene 3) ansieht, bewerten die IT-Verantwortlichen diesen als nicht initiiert (Ebene 0).

4.17.2 Handlungsempfehlungen

Aus den Ergebnissen der Kapitel 4.17.1.1 bis 4.17.1.4 wird deutlich, dass dringender Handlungsbedarf zur langfristigen Sicherstellung der Funktionsfähigkeit sowie der Eignung der umgesetzten Sicherheitsmaßnahmen besteht.

Die Bewertung hat klar aufgezeigt, dass das IT-Sicherheitsmanagement in weiten Teilen nicht auf zyklischen Prozessen beruht, die Qualität der Prozesse nur in Einzelsituationen beziehungsweise einzelnen Unternehmen gemessen oder deren zukünftige Entwicklung gesteuert wird.

Bei der Mehrzahl der Prozesse sind die Abläufe nicht festgelegt oder die Veränderungen das Ergebnis von „trial-and-error“. Dies wird über kurz oder lang zu Fehlern in den Abläufen und damit zu Lücken im IT-Sicherheitsmanagement führen.

Ein erster, kurzfristiger Schritt zur Verbesserung der Prozesse ist, die vorhandenen Beschreibungen auf Vollständigkeit und Aktualität zu prüfen und diese bei Bedarf zu ergänzen. Dies kann durch eine Verbesserung des gemeinsamen Verständnisses von Geschäftsführung und IT-Verantwortlichen in Bezug auf die IT-Sicherheitsziele und -strategien, die Gefahrenbereiche für das Unternehmen sowie die Risikobewertung der Geschäftsprozesse unterstützt werden. Nur ein gemeinsames Verständnis der IT-Sicherheitsziele, der Bedrohungen sowie der Risiken IT-gestützter Geschäftsprozesse ermöglicht eine abgestimmte Vorgehensweise.

Auf Basis dieser abgestimmten Vorgehensweise sind mittelfristig alle Prozesse mindestens auf den Reifegrad „Standardisiert“ (Ebene 3) zu bringen.

Als langfristiges Ziel ist eine fortlaufende Bewertung der Qualität sowie ggf. ein Nachjustieren der Prozesse anzustreben. So kann mittel- bis langfristig deren effektive Anwendbarkeit sichergestellt werden.

Nur Prozesse, die auf der Basis strukturierter und dokumentierter Beschreibungen gelebt werden, die aufeinander abgestimmt und deren Rollen und Verantwortlichkeiten geregelt sind, können die Grundlage für ein dauerhaft belastbares IT-Sicherheitsmanagement bilden.

4.18 Zukunftsthemen

Zukunftsthemen sind neue Technologien oder Maßnahmen zur Unterstützung der Geschäftsprozesse in den Unternehmen. Die folgenden drei neuen Technologien sind in den Medien derzeit sehr präsent:

- **Cloud Computing:** Cloud Computing ist die zentrale Bereitstellung von technischen IT-Dienstleistungen. Derzeit bieten unterschiedlichste Dienstleister Clouds für Unternehmen an. Hierzu wurde ein Eckpunktepapier mit Sicherheitsempfehlungen für Cloud Computing Anbieter (vgl. [BSI_2011n]) vom BSI in Zusammenarbeit mit der Wirtschaft erstellt.
- **De-Mail/E-Postbrief:** De-Mail zielt auf die Einrichtung einer sicheren Kommunikationsinfrastruktur für Bürger, Unternehmen und Verwaltung. De-Mail ist Bestandteil des Modernisierungsprogramms "Vernetzte und transparente Verwaltung" der Bundesregierung. Es steht in Übereinstimmung mit der Nationalen E-Government-Strategie. Weiterführende Informationen zu De-Mail sind dem Kapitel 6 zu entnehmen. Der E-Postbrief ist ein Produkt der Deutschen Post und bietet Grundfunktionen in Anlehnung an das De-Mail-Gesetz.
- **Neuer elektronischer Personalausweis (nPA):** Der neue elektronische Personalausweis wird seit dem 1. November 2010 ausgegeben. Durch die eID-Funktionen können auch Unternehmen den neuen elektronischen Personalausweis sowohl für Dienstleistungen als auch für unternehmenseigene Geschäftsprozesse verwenden. Weitere Informationen stellt die Webseite zum neuen elektronischen Personalausweis (www.personalausweisportal.de) bereit.

4.18.1 Ergebnisse

Cloud Computing ist ein IT-Angebot, das es ermöglicht, eine oder mehrere IT-Dienstleistungen wie Rechenleistung, Hintergrundspeicher, Entwicklungsumgebungen, Anwendungssoftware oder sogar komplette Arbeitsumgebungen

- jederzeit,
- netzbasiert,
- schnell und dem tatsächlichen Bedarf angepasst
- sowie nach tatsächlicher Nutzung abrechenbar

zu beziehen.

Demzufolge beschäftigt Cloud Computing sich im weitesten Sinne mit Outsourcing. Die Unternehmen wurden daher zuerst nach dem Einsatz von Outsourcing befragt. Anschließend wurde um eine Zukunftseinschätzung in Bezug auf die Bedeutung von Cloud Computing gebeten.

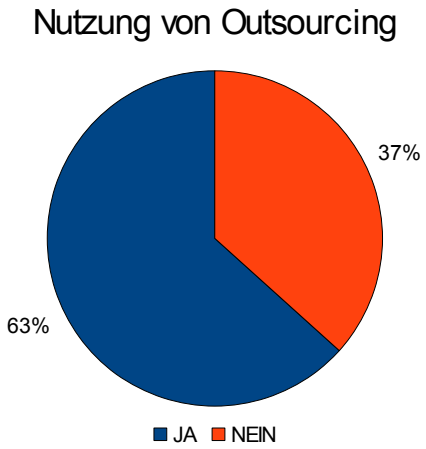


Abbildung 42: Nutzung von Outsourcing

Outsourcing wird bereits heute von mehr als 60 Prozent der befragten Unternehmen genutzt. Hinsichtlich des Themas Cloud Computing sind die Unternehmen jedoch zurückhaltender. Insgesamt 26 Prozent der IT-Verantwortlichen sehen Cloud Computing aktuell als wichtig bis sehr wichtig an, während dies nur für 20 Prozent der Vertreter der Geschäftsführung zutrifft. Danach befragt, wie die zukünftige Bedeutung von Cloud Computing eingeschätzt wird, sprachen sich insgesamt 23 Prozent der Personen für eine steigende Bedeutung aus. Als Hinderungsgrund für eine Nutzung der Cloud wurden besondere Bedenken hinsichtlich der IT-Sicherheit geäußert, da sich die Kontrolle über Risiken und Schutzmaßnahmen dem direkten Einfluss der Unternehmen entzieht.

Hinsichtlich der zukünftigen Verwendung der De-Mail bzw. des E-Postbriefs sind die Unternehmen ähnlich zurückhaltend wie bei dem Thema Cloud Computing.

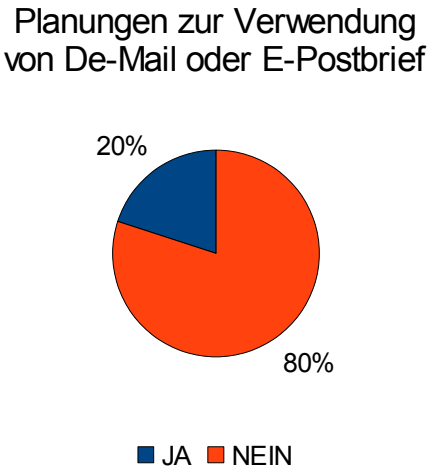


Abbildung 43: Planung der Verwendung von De-Mail bzw. E-Postbrief

Den Einsatz von De-Mail oder E-Postbrief in seinen Geschäftsprozessen planen 20 Prozent der Unternehmen. Jeweils zwei Unternehmen würden sich für De-Mail respektive E-Postbrief entscheiden. Zwei weitere Unternehmen haben noch keine bestimmte Wahl getroffen. Die Gründe für den Einsatz sind unterschiedlich – die Mehrheit der Unternehmen gibt den rechtsverbindlichen

Zustellnachweis und die Transportverschlüsselung der E-Mail-Kommunikation als Kriterien für die Auswahl an.

Den Einsatz des neuen elektronischen Personalausweises planen nur zwei der 30 befragten Unternehmen. Die Unternehmen planen dabei den Einsatz der eID-Funktion im Rahmen einer Zutrittskontrolle und als Servicedienstleistung für die Kunden in den eigenen Geschäftsprozessen.

Da es sich demzufolge um noch umzusetzende Technologien in der Mehrheit der Unternehmen handelt, wurde auf eine Bewertung verzichtet.

4.18.2 Handlungsempfehlungen

Neue Technologien können positiven Einfluss auf die Geschäftsprozesse haben. Daher sollten Prozesse zur Informationsgewinnung über neue Technologien etabliert sein. Ein möglicher Einsatz der neuen Technologien im Unternehmen sollte in regelmäßigen Abständen geprüft werden.

5 Fazit und Ausblick

Erstmalig ist mit der vorliegenden Studie eine Untersuchung des IT-Sicherheitsniveaus von KMU in Deutschland durchgeführt worden, bei der die Daten in einem dreistufigen Interview-Prozess ermittelt wurden und somit als hochgradig gesichert anzusehen sind. Die getrennte Befragung von Geschäftsführung und IT-Bereich mit nachfolgender moderierter Rückmeldung der Ergebnisse führt über Vermutungen oder Einschätzungen hinaus zu gesichertem Wissen über den Stand der IT-Sicherheit im Unternehmen. Die Darstellung des Sachstands enthält auch unstrittige Sicherheitsdefizite, die in nahezu allen Unternehmen priorisiert und deren Beseitigung unmittelbar vereinbart wurde. Durch die gesamtheitliche und gleichzeitig qualitätsgesicherte Analyse konnte ein umfassender Eindruck über den Stand der IT-Sicherheit in kleinen und mittleren Unternehmen gewonnen werden.

Die Ergebnisse machen deutlich, dass die KMU bei Wertung der umgesetzten IT-Sicherheitsmaßnahmen grundsätzlich geeignet aufgestellt sind. Im Durchschnitt werden rund zwei Drittel der in Anlehnung an den IT-Grundschutz abgefragten IT-Sicherheitsmaßnahmen in den Unternehmen umgesetzt. Die in der Studie betrachteten Themenkomplexe sind als Gesamtergebnis in Abbildung 44 dargestellt. Die angegebenen Bewertungen beziehen sich auf den Umsetzungsgrad der abgefragten IT-Sicherheitsmaßnahmen. Die Kapitel sind dabei in Anlehnung an die Bausteine des IT-Grundschutzes benannt.

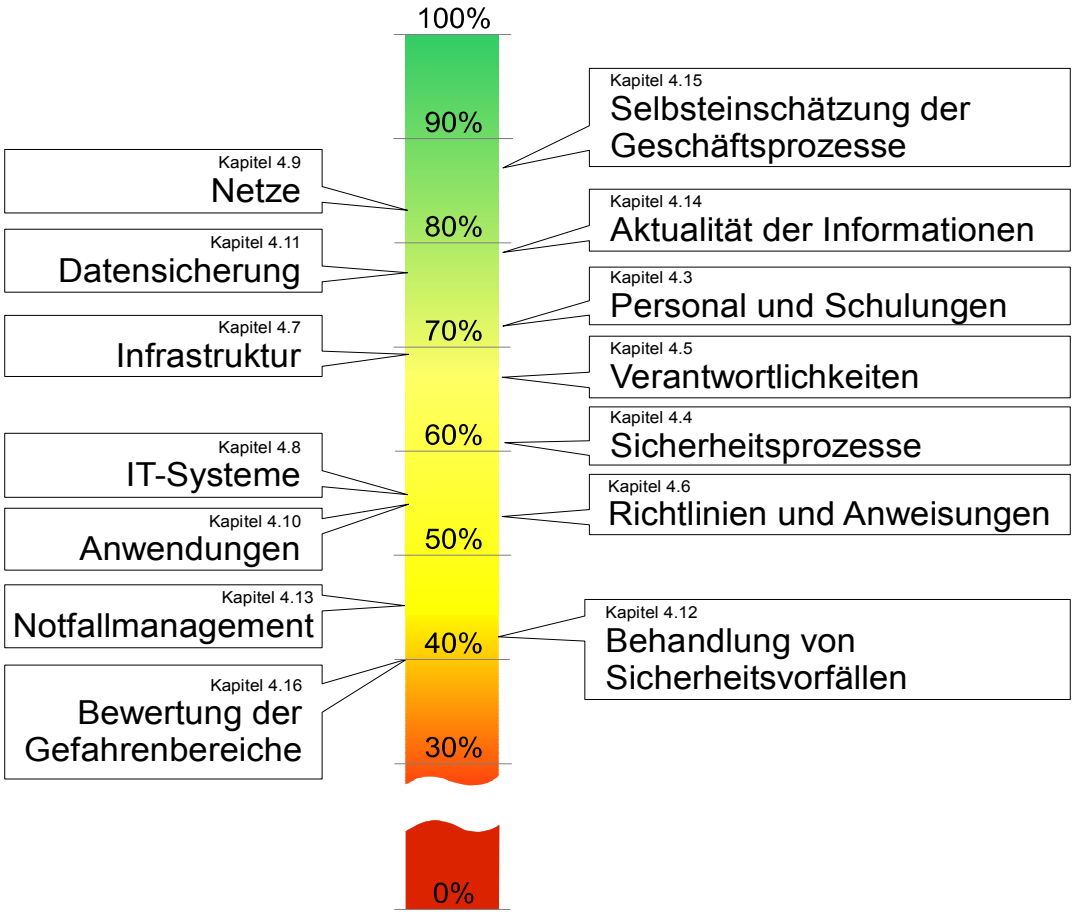


Abbildung 44: Themenbezogene Gesamtdarstellung des Umsetzungsgrades der abgefragten IT-Sicherheitsmaßnahmen

Deutliche Schwächen liegen vor allem noch im Bereich der *geschäftskritischen IT-Sicherheitsprozesse*, das heißt, dem Umgang mit *Sicherheitsvorfällen*, dem *Notfallmanagement* und der B*ewertung der Gefahrenbereiche*. Ursächlich für diese Situation scheint ein verbreiteter „Funktionaler Optimismus“ zu sein, der die eigenen Handlungsmöglichkeiten bei Sicherheitsvorfällen überschätzt (Illusorische Kontrolle) und daher weitestgehend auf Dokumente verzichtet.

Nach Analyse der Organisation der IT-Sicherheit in Unternehmen lässt sich feststellen, dass diese sich überwiegend durch eine Folge von nicht aufeinander abgestimmten Einzelaktionen darstellt und ein Bewusstsein für einen Prozess als Arbeitsgrundlage der IT-Sicherheit nicht durchgängig präsent ist. Anpassungen der Prozesse sind oft das Ergebnis von Versuch und Irrtum, folgen aber nicht einem idealerweise vorher festgelegten Konzept.

Dieses Ergebnis ist sehr erstaunlich, weil dem Thema IT-Sicherheit an sich sowohl von den Geschäftsführungen als auch von den Technikern der Unternehmen eine sehr hohe Bedeutung beigemessen wurde. Das Bewusstsein für das Thema ist in den Unternehmen sehr ausgeprägt, dennoch lässt der Umsetzungsgrad der IT-Sicherheitsmaßnahmen wie auch die Etablierung eines IT-Sicherheitsmanagements zu wünschen übrig.

Insbesondere langjährige IT-Mitarbeiter verfügen durchaus über Erfahrung bezüglich der betriebsinternen Abläufe in der IT und werden somit als Garanten für IT-Sicherheit angesehen. Produktions- und Termindruck, personell knappe Besetzung der IT-Abteilung und sich einschleichende Routine verhindern jedoch häufig eine zeitlich angemessene Auseinandersetzung mit der IT-Sicherheit und neuen Risiken. Für den Blick über das eigene Unternehmen hinaus auf neue, ausgeklügelte Angriffstechniken auf die IT bleibt keine Zeit. Die mit Raffinesse vorgetragenen Angriffe können jedoch oft nur noch von speziell und regelmäßig geschultem IT-Personal eindeutig erkannt und abgewehrt werden. Ein wesentlicher Sicherheitsbeitrag für Unternehmen besteht darin, den „Ausguck“, einen höher gelegenen Beobachtungspunkt, fachkompetent und dauerhaft mit einem „Lotsen“ zu besetzen. Diese Maßnahme stellt sicher, dass das Unternehmen im Informationsfluss neuer Risiken bleibt – Prävention ist effizienter und kostengünstiger als auf Sicherheitsvorfälle zu reagieren.

Die in Kapitel 4 aufgezeigten Handlungsempfehlungen sind als erster Schritt zur Stabilisierung des IT-Sicherheitsniveaus zu sehen. Um ein dauerhaft hohes Niveau an IT-Sicherheit zu erreichen, müssen die erforderlichen Schutzmaßnahmen umgesetzt, aber vor allem auch die zugehörigen IT-Sicherheitsmanagementprozesse in den KMU etabliert und standardisiert werden.

Die im Laufe der Studie durchgeführten Interviews zeigten, dass durch die Diskussion mit IT-Sicherheitsexperten und der transparenten Ergebnisrückmeldung eine Sensibilisierung für IT-Sicherheitsthemen bei den beteiligten KMU erreicht werden konnte. Nach Auskunft der Unternehmen würde ein einführendes und kostenfreies Audit bereits dazu beitragen, ein Grundverständnis für IT-Sicherheit zu erhalten. Zusätzlich könnten bei solchen Sensibilisierungsmaßnahmen Problemstellungen von IT-Sicherheitsexperten besprochen und Lösungsansätze entwickelt werden. Abhängig vom Erfolg dieses Angebots könnten langfristig weitere erläuternde Module – beispielsweise zu Themen des IT-Grundschutzes – kostenpflichtig angeboten werden.

Aller Anfang ist schwer – zur Annäherung an das Thema IT-Sicherheit bedarf es in vielen Fällen offensichtlich eines Schadensereignisses im Unternehmen. Auch ohne Sicherheitsvorfall ist für Unternehmen der Einstieg in die Themen der IT-Sicherheit möglich. Dann aber, so die

Rückmeldungen aus der Studie, ist für die Unternehmen für den Start eine externe Moderation eine nahezu unverzichtbare Hilfestellung.

Die Aussagen unterstreichen zudem die anfängliche Vermutung, dass die IT von den Verantwortlichen in KMU oftmals primär als Kostenfaktor und nicht als „Business Enabler“ angesehen wird. Investitionen werden nur bei erkannten akuten Bedrohungen und nur im unbedingt erforderlichen Kostenrahmen getätigt. Die Zurückhaltung bei den finanziellen Mitteln spiegelt sich auch auf der personellen Ebene wider – Arbeitszeit ist sehr knapp und teuer. Selbst wenn sämtliche für ein externes Audit erforderlichen Dokumentationen verfügbar wären – eine Schwäche im Mittelstand – sind für ein derartiges Audit mehrere Arbeitstage einzuplanen. Selbst eine IS-Kurzrevision benötigt rund einen Arbeitstag. Hilfe zur Selbsthilfe durch regionale Aktionsbündnisse stärkerer Wirtschaftsunternehmen, die in geringem Umfang die ersten Gehversuche zur IT-Sicherheit in kleinen Unternehmen begleiten und fördern könnten eine Lösung werden. Diese Unterstützung wäre insbesondere in Zulieferbetrieben ein Beitrag zum eigenen Nutzen der Förderer.

Als ergänzende Lösung sollten im Rahmen der künftigen Cyber-Strategie für Deutschland Behörden verstärkt mit Verbänden und Kammern vor Ort zusammenarbeiten und diese zu Kompetenzzentren für IT-Sicherheit entwickeln. Die Auskünfte der Befragten ließen erkennen, dass die verfügbaren IT-Angebote regional unterschiedlich stark ausgeprägt sind, aber durchaus von Teilnehmern bereits genutzt wurden beziehungsweise Interesse an derartigen Angeboten besteht. Als Multiplikatoren könnten diese Einrichtungen selbst IT-Sicherheitsveranstaltungen durchführen und eine lokale Wissensaustauschplattform etablieren. So wäre beispielsweise ein von den Unternehmensleitungen selbst organisierter, partnerschaftlicher Wissensaustausch mit gegenseitiger Beratung zu IT-Sicherheitsaspekten durch die IT-Mitarbeiter zweier nicht im Wettbewerb stehender Unternehmen denkbar, um den Risikofaktor Betriebsblindheit zu umgehen. Die Kammern und Verbände könnten zudem die Marketingmaßnahmen der IT-Sicherheitsdienstleister unterstützen und somit Bedarf und Bedarfsdecker in Kontakt bringen. Die Aufgabe könnte sein, Unternehmen durch regionale „Gelbe Seiten der IT-Sicherheit“ zu vernetzen.

Die teilweise Auslagerung der IT-Sicherheit mit Komplettlösungen von IT-Sicherheitsdienstleistern wäre ein weiterer Weg, dem schnellen Wandel der Bedrohungen auf diesem Gebiet zu begegnen. Da diese Dienstleister in der Regel einen sehr tiefen Einblick in die Unternehmensinterna erhalten, ist die Auswahl eines zuverlässigen und vertrauenswürdigen Partners wichtig. Mit der Vergabe des ISO 27001-Zertifikats auf der Basis von IT-Grundschutz bietet das BSI einen Anhaltspunkt zur selbstständigen objektiven Auswahl eines fachkompetenten IT-Sicherheitsdienstleisters. Das BSI bildet „Auditoren“ aus, die ohne Einschränkung in der freien Wirtschaft ihre Dienstleistungen anbieten können.

Als besonders hilfreich nannten die befragten IT-Leiter eine Kontaktstelle zur Beantwortung einzelner IT-Sicherheitsfragen. Vorhandene Angebote und Kontaktmöglichkeiten, wie beispielsweise die Beratungsleistungen der Landesämter für Verfassungsschutz gegen Wirtschaftsspionage, die auch IT-Sicherheitsaspekte einschließen, waren nur wenigen Teilnehmern bekannt oder wurden von diesen bereits genutzt. Die Diskussionsgruppe IT-Grundschutz im Sozialen Netzwerk „XING“ kannte vor der Befragung kein Teilnehmer. Auch der Warn- und Informationsdienst sowie die Newsletter von IT-Grundschutz und Bürger-CERT des BSI waren weitestgehend unbekannt. Insgesamt scheinen in den Unternehmen die seriösen und kostenfreien Informationsangebote zur IT-Sicherheit in der Fläche nicht bekannt zu sein. Ursache hierfür könnte die „Reizüberflutung“ und die Vielfalt der unaufgefordert zugestellten Sicherheitswarnungen sein – mit dem Ergebnis, dass auch die Annäherung zu anerkannt guten Warn- und Informationsdiensten verhindert wird. Eine Lösung könnte in der zielgruppenspezifischen und am Bedarf des

Unternehmens orientierten Zusammenstellung von Informationsdiensten, wahlweise Push oder Pull, liegen.

Die KMU, die sich noch nicht mit dem Thema der IT-Sicherheit beschäftigt haben müssen in erster Linie über den Sicherheitsstatus des Unternehmens aufgeklärt werden. Um eine erste Einschätzung des Status der Umsetzung von Sicherheitsmaßnahmen im Unternehmen vornehmen zu können, sollte ein Kurzinterview oder eine Checkliste bereitgestellt werden. Diese Materialien hinterfragen den Status Quo und können gleichzeitig die Funktion eines Ratgebers übernehmen, der auf die Vielfalt der Aspekte der IT-Sicherheit verweist. Gefahren werden dadurch auf verständliche Weise nahe gebracht und der Einstieg in den IT-Grundschutz erleichtert. Nach Aussage der Unternehmen ist der IT-Grundschutz in seiner Gesamtheit für die Betriebe aus dem KMU-Bereich ohne Anwendung von Hilfsmitteln zu komplex, diese Einschätzung verhindert auch weitestgehend die Annäherung und die Anwendung.

Die KMU sehen einen zentralen Dienstleister des Bundes als Hilfestellung an, um die Komplexität und die Informationsflut zu vermindern. Besonders wichtig ist dort die Bereitstellung von technischen Umsetzungen zu beschlossenen Gesetzgebungen – wie es bereits mit technischen Richtlinien seitens des BSI teilweise erfolgt.

Nicht selten wurde in Interviews eine Überbordung der Unternehmen mit Rechtsvorschriften und gesetzlichen Regelungen beklagt, deren Nichtbeachtung strafbewährt ist. Die Einhaltung der Vorschriftenlage wird in Unternehmen mit Priorität befolgt. In diesem Kontext wurde das Thema IT-Sicherheit von der Geschäftsführung nicht selten als „Kür“ oder nahezu „esoterisches“ Thema eingeordnet. Der *verpflichtende* Respekt vor Recht und Gesetz dominiert offensichtlich und nachvollziehbar die *freiwillige* Bereitschaft, sich den Anforderungen der IT-Sicherheit zu stellen. Eine Lösung könnte sich dadurch ergeben, dass die Unternehmen bei der Umsetzung rechtlicher Anforderungen eine deutliche Unterstützung und Arbeitserleichterung erfahren und somit Raum für eine intensivere Auseinandersetzung mit den Belangen der IT-Sicherheit geschaffen wird.

Das BSI hat deshalb IT-Grundschutz-Profile [BSI_ITGSP] mit Anwendungsbeispielen für unterschiedliche Zielgruppen als Hilfsmittel veröffentlicht, mit der die IT-Sicherheit in den Unternehmen vollständig abgebildet werden kann. Die Anwendungsbeispiele wurden bereits für das produzierende Gewerbe, kleine Institutionen (beispielsweise Kleinbetrieb), den Mittelstand und große Institutionen veröffentlicht. Die ISi-Reihe (Internet-Sicherheit) ist zur einfacheren Umsetzbarkeit jeweils in eine Leitlinie für das Management, eine Studie für IT-Fachkräfte und eine Checkliste für Administratoren und IT-Revisoren unterteilt.

Das BSI leistet mit zielgruppenspezifischen Informationen, Lageberichten zur IT-Sicherheit, zertifizierten Sicherheitsprodukten und ganzheitlichen Sicherheitslösungen „best practice“ Beiträge zum Schutz der Wirtschaft in Deutschland. Das Surfen im Internet wird durch die massive Zunahme von Websites, die mit Schadsoftware infiziert wurden, zunehmend von den Interviewpartnern als Risiko für das eigene Unternehmen angesehen, von nahezu allen Unternehmen wurde diese Sorge geäußert. Vom BSI wurde mit „Browser in the Box (BitBox)“ für die Behörden eine Sicherheitslösung entwickelt, die auch für Unternehmen verfügbar ist. Die BitBox ist eine gekapselte Surfumgebung, die abgeschottet auf dem PC des Anwenders läuft. Ein Schädling, dem es gelingen würde, den gehärteten BitBox zu befallen, ist nach Beenden der Surf-Sitzung beseitigt. Ein Durchgriff auf das eigentliche Arbeitsplatzsystem des Nutzers und interne Netze mit all seinen schützenswerten Daten ist nicht möglich. Derartige Sicherheitslösungen wurden von den Unternehmen mit großem Interesse aufgenommen.

Es gibt ausnahmslos gute Gründe, dass kleine und mittlere Unternehmen zumindest das kostenlose Informationsspektrum des BSI kennen. Der Bekanntheitsgrad der Beratungsangebote des BSI ist im Mittelstand jedoch noch optimierungsfähig. Die für den KMU-Bereich zur Verfügung gestellten Dienstleistungen sollten zukünftig an einer Stelle gebündelt werden, um die öffentliche Wahrnehmung und die Nutzung vorhandener Wissensquellen beim Mittelstand zu verbessern. Auf der anderen Seite benötigt das BSI kontinuierlich Rückmeldung aus dem Mittelstand über die praktische Anwendbarkeit der Angebote, zum Beispiel des GS-TOOLs, um die Leistungen entsprechend anpassen zu können.

Durch eine solche vertrauensvolle Zusammenarbeit können IT-Risiken gemindert und Schadensfälle verhindert werden. Denn IT-Sicherheit ist eine gemeinsame Herausforderung für Wirtschaft, Staat und Bürger.

6 Stichwort- und Informationsverzeichnis

Thema	*Erläuterung und weiterführende Literatur*
Archivierung: Vorgaben und Umsetzung	Archivierung unterteilt sich in E-Mailarchivierung und Datenarchivierung. Für die E-Mailarchivierung gerade für den Geschäftsverkehr gelten verschiedenste rechtliche Vorschriften (vgl. HGB, GoBS, BetrVerfG). In der BSI-Studie „IT-Sicherheit und Recht“ (vgl. [BSI_2011d]) sind weiterführende Hinweise aufgelistet. Datenarchivierung wird seitens BSI-IT-Grundschutz (vgl. [BSI_2011]) in der Maßnahme M 2.246 behandelt. Weiterhin enthält die technische Richtlinie TR 03125 (vgl. [BSI_2009]) Hinweise auf die Beweiswerterhaltung kryptografischer Systeme und die Vertraulichkeit.
Auslandsreisen	Das Bundesamt für Verfassungsschutz (www.verfassungsschutz.de) ruft derzeit zur erhöhten Vorsicht bei Reisen auf. Das BSI (www.bsi.bund.de) und das Auswärtige Amt (www.auswaertiges-amt.de) veröffentlichen Hinweise zu Auslandsreisen.
Awareness-Steigerung für IT-Sicherheit	Mitarbeiter sollten für den Bereich IT-Sicherheit sensibilisiert sein, um die IT-Sicherheit im Unternehmen auf einem hohen Niveau zu etablieren. In einem ersten Schritt ist es erforderlich, den Stand der Awareness zu ermitteln. Dazu werden Kriterien festgelegt und deren Erreichungsgrad beispielsweise durch einen Fragebogen abgeprüft. Somit kann der Bedarf ermittelt und regelmäßige Maßnahmen festgelegt werden. Einen geeigneten Rahmen zur Ansprache der Mitarbeiter bilden interne Vorträge, Schulungen (vgl. IT-Grundschutz M3.5, M3.45), Rundschreiben, Plakate und Videos. Literatur: • Sicher gewinnt! - Sensibilisierungsleitfaden [BA-KOEV] • Security Awareness Training "open beware!" [OB2011] • Awareness-Steigerung in KMUs [ENISA_2011]

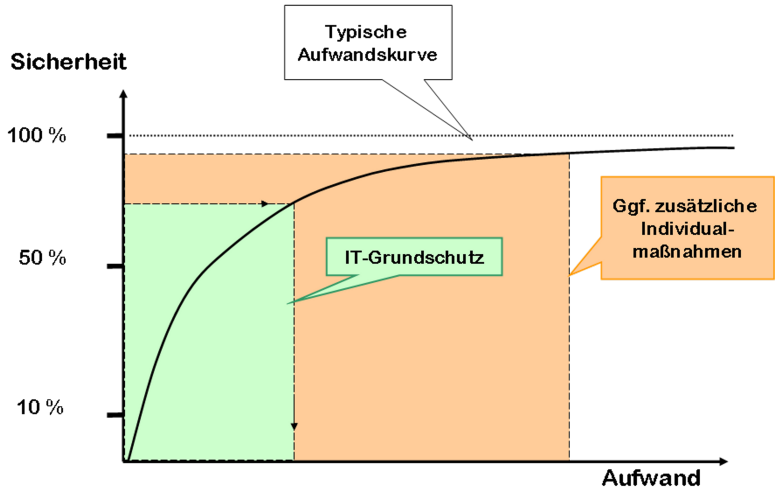
Thema	*Erläuterung und weiterführende Literatur*
Browser in the Box (BitBox)	Durch einen Browser kann unter Ausnutzung von eventuell vorhandenen Schwachstellen Schadsoftware von infizierten Websites unbemerkt heruntergeladen werden (sogenannte Drive-by-Downloads). Um das System nicht durch einfaches Websurfen zu gefährden, wurde vom BSI eine gekapselte Surf-Umgebung entwickelt. Das BSI realisierte einen Browser in the Box (BitBox), der innerhalb einer virtuellen Systemumgebung mit einem gehärteten Linux läuft. Durchgriffe auf das eigentliche System sind nur über definierte Wege (z.B. Drucken, Dateidownloads) möglich. Weitere Informationen hierzu sind auf der Webseite des BSI zu finden (vgl. [BSI_2011o]).
Cloud Computing	Cloud Computing ist die zentrale Bereitstellung von technischen IT-Dienstleistungen. Derzeit bieten unterschiedlichste Anbieter Clouds für Unternehmen an. Das BSI erstellte in Zusammenarbeit mit der Wirtschaft ein Eckpunktepapier mit Sicherheitsempfehlungen für Cloud Computing Anbieter (vgl. [BSI_2011n]).
Data Loss Prevention und Data Leakage Prevention	Data Loss Prevention ist der Schutz vor unerwünschten Abfluss von Daten. Data Leakage Prevention ist der Schutz gegen vermutete, aber nicht messbaren, Abfluss von Daten. Weitere Hinweise finden sich im IT-Grundschutz-Katalog [BSI_2011] Maßnahme M 4.345 Schutz vor unerwünschten Informationsabflüssen.
Strategien zur Realisierung des Datenschutzes in KMU	Zuständig für die Überprüfung des Datenschutzes in KMU ist der jeweilige Landesbeauftragte für Datenschutz (www.datenschutz.de oder www.datenschutz.bund.de). Die IT-Grundschutzkataloge sind durch die Beauftragten für Datenschutz (Bund und Länder) erweitert worden (vgl. [BSI_2011] Baustein B 1.5 Datenschutz). Hier stehen auch als Ergänzung Checklisten zum Grundschutzkatalog zur Verfügung.

Thema	*Erläuterung und weiterführende Literatur*
Datensicherung	Datensicherungen sind, sofern die Daten für die Geschäftsprozesse benötigt werden, eine elementare Geschäftsgrundlage des Unternehmens. Der IT-Grundschutz-Katalog empfiehlt jedem Unternehmen Datensicherungen durchzuführen (vgl. [BSI_2011]). Hier sind die folgenden Maßnahmen benannt: • M 6.33 Entwicklung eines Datenschutzkonzepts • M 6.34 Einflussfaktoren bei der Datensicherung • M 6.35 Festlegungen der Verfahrensweise für die Datensicherung Ausgehend vom festgelegten Schutzbedarf kann es notwendig sein, die Beweiskraft signierter Dokumente in der Datensicherung langfristig zu sichern. Hierfür hat das BSI die technische Richtlinie TR 03125 (vgl. [BSI_2009]) entwickelt.
Definition Sicherheitsvorfall, Notfall und Störfall	Als Störfall definiert man einen Vorfall, der den bestimmungsgemäßen Betrieb stört, jedoch nicht unterbricht. Als Notfall wird ein Vorfall mit Schadereignis benannt, bei dem wesentliche Prozesse oder Ressourcen eines Unternehmens nicht wie vorgesehen funktionieren. Ein Sicherheitsvorfall muss von jedem Unternehmen selbstständig definiert werden. Hierbei können Hinweise aus den IT-Grundschutz-Katalog [BSI_2011] Maßnahme „M 6.122 Definition eines Sicherheitsvorfalls“ genommen werden. Weiterhin kann eine Orientierung zur Definition eines Sicherheitsvorfalls anhand der Verwaltungsvorschriften für Bundesbehörden [Bund_2011] erfolgen.

Thema	*Erläuterung und weiterführende Literatur*
De-Mail	De-Mail zielt auf die Einrichtung einer sicheren Kommunikationsinfrastruktur für Bürger, Unternehmen und Verwaltung. De-Mail ist Bestandteil des Modernisierungsprogramms "Vernetzte und transparente Verwaltung" der Bundesregierung. Es steht in Übereinstimmung mit der Nationalen E-Government-Strategie. Am 3. Mai 2011 ist das De-Mail-Gesetz in Kraft getreten. Interessierte Anbieter können damit beim BSI die Akkreditierung als De-Mail-Diensteanbieter ("De-Mail-Provider") beantragen. Im Rahmen der Akkreditierung müssen alle künftigen De-Mail-Diensteanbieter nachweisen, dass sie die durch das De-Mail-Gesetz geforderten hohen Anforderungen an die organisatorische und technische Sicherheit der angebotenen De-Mail-Dienste erfüllen. Jeder Anbieter, der diese Anforderungen erfüllt, kann sich als De-Mail-Diensteanbieter akkreditieren lassen. Das BSI hat hierzu das Informationsmaterial auf der Webseite veröffentlicht (vgl. [BSI_2011k]).
Device-Sicherheit	Über mobile Datenträger können zusätzliche Sicherheitslücken entstehen. Hier gilt es, genauso wie in Netzwerken, ein Schutz zu installieren. Das BSI-Projekt Wechseldatenträgerschleuse Janus beschäftigt mit dem sicheren Austausch von Daten auf mobilen Medien. Neben der Behördenversion „Janus“ existiert unter dem Namen Provaia ein privatwirtschaftlich vertriebenes Produkt für die Wirtschaft, das direkt aus der Software des Entwicklungsprojekts hervor ging.
Richtlinie zur sicheren Nutzung und Abruf von E-Mail	Die sichere Nutzung von E-Mail wurde in der ISi-Reihe des BSI (vgl. [BSI_2011h]) betrachtet. Hierzu gehören verschiedene Studien und Checklisten für verschiedene Produkte.

Thema	*Erläuterung und weiterführende Literatur*
Sichere E-Mail Kommunikation	Mit einer sicheren Kommunikation sollen die Ziele Authentizität, Integrität, Vertraulichkeit und Verbindlichkeit erreicht werden. Hierzu gibt der IT-Grundschutz [BSI_2011] die folgenden Maßnahmen an: • M 2.118 Konzeption der sicheren E-Mail-Nutzung • M 5.108 Kryptografische Absicherung von E-Mail • M 2.46 Geeignetes Schlüsselmanagement Hierüber hinaus kann die Kommunikation auf verschiedenen Ebenen abgesichert werden: • Netz zu Netz • Client zu Web-/Mailserver • Client zu Netz • Client zu Client Mögliche Unterstützungen zur sicheren Kommunikation sind beispielsweise De-Mail, E-Postbrief, GPG-Verschlüsselung oder Julia MailOffice.
Festplattenverschlüsselung	Festplattenverschlüsselung ist in unterschiedlichen Formen realisierbar: • Partielle Festplatten- oder Datenverschlüsselung • Vollständige Festplattenverschlüsselung • Integrierte Hardwarefestplattenverschlüsselung Die Auswahl der richtigen Festplattenverschlüsselung hängt von den Einsatzszenarien im Unternehmen ab. Eine teilweise Festplattenverschlüsselung oder Verschlüsselung einzelner Dateien birgt grundsätzlich das Risiko, dass z.B. bei der Anzeige und Verarbeitung von Dateien unverschlüsselte Zwischenversionen auf dem System erhalten bleiben.
Aussehen und Anwendung von IT-Grundschutz	Das Konzept von IT-Grundschutz besteht darin einen Katalog für übliche Abläufe und IT-Komponenten bereitzustellen, die überall gleich sind. Somit ist die Wiederverwendbarkeit gegeben, jedoch mit dem Aspekt der Anpassbarkeit und Erweiterbarkeit. Literatur zur Einführung von IT-Grundschutz: • BSI-IT-Grundschutz-Standards [BSI_2011a] • IT-Grundschutz-Kataloge [BSI_2011] • Webkurs IT-Grundschutz [BSI_2011b]

Thema	*Erläuterung und weiterführende Literatur*
Bedrohungsanalyse nach IT-Grundschutz	Die Bedrohungsanalyse ist im IT-Grundschutz-Standards 100-3 beschrieben (vgl. [BSI_2011a]).
Anforderungen an Dokumentation nach IT-Grundschutz	Der IT-Grundschutz-Katalog (vgl. [BSI_2011]) bietet in den Maßnahmen M 6.134 Dokumentation von Sicherheitsvorfällen, M 6.37 Dokumentation der Datensicherung und in M 2.25 Dokumentation der Systemkonfiguration Hinweise zur Dokumentation. Weitere Empfehlungen sind in den BSI-IT-Standards enthalten (vgl. [BSI_2011a]).
Zertifizierung nach BSI-IT-Grundschutz	Weiterführende Informationen finden sich auf der BSI-Webseite unter: [BSI_2011c]
Anforderungen nach ISO 2700x	Eine Auflistung der zugehörigen Standards zu ISO 2700x findet sich auf der Webseite von ISO (vgl.[ISO_2011]). Ziel der ISO 2700x ist die Verminderung, Verlagerung und Vermeidung von Schaden. Hierbei stützt sich der Informationssicherheitsprozess auf das PDCA-Modell.
Einsatz von IT-Sicherheit	IT-Sicherheit im Unternehmen einzusetzen hat das Ziel geschäftskritische Daten zu schützen. Weiterhin kann IT-Sicherheit Schutz vor Haftung und Schutz vor Imageschäden bieten. Hervorzuheben ist auch der Schutz vor finanziellen Auswirkungen (siehe auch [BSI 2008] 100-2 Kapitel 4.3.1). Literatur: • Leitfaden Informationssicherheit – IT-Grundschutz kompakt [BSI_03] • Schutzprofil für KMU
IT-Sicherheit bei der Entsorgung von Hardwaresystemen	Der BfDI stellt Informationen zur Entsorgung von Hardwaresystemen bereit [BfDI_2008]. Weiterhin werden Methoden im IT-Grundschutz-Katalog (vgl. [BSI_2011] Maßnahme M 2.167 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten) benannt.
Meldeverfahren des Bundes bei IT-Sicherheitsvorfällen	Die Beschreibung erfolgt in den Verwaltungsvorschriften (vgl. [Bund_2011]).

Thema	*Erläuterung und weiterführende Literatur*
Risiko und Kosten von IT-Sicherheit	 *Abbildung 45: Aufwandskurve für IT-Grundschutz* Mit der Umsetzung des IT-Grundschutzes wird bereits ein Sicherheitsniveau von 80 Prozent erreicht. Zusätzliche Maßnahmen verursachen im Verhältnis zum Sicherheitsgewinn überproportionale Mehrkosten. Hundertprozentige Sicherheit ist nicht möglich.
Erstellung eines IT-Sicherheitskonzepts	Das IT-Sicherheitskonzept wird grundsätzlich nach den BSI-IT-Grundschutz-Standards 100-2 und 100-3 erstellt (vgl. [BSI_2011a]). Weitere Hinweise finden sich im IT-Grundschutz-Katalog [BSI_2011] in der Maßnahme M 2.195 Erstellung eines IT-Sicherheitskonzepts.
Strategien zur Realisierung von IT-Sicherheitsmaßnahmen	Für die Realisierung von IT-Sicherheitsmaßnahmen muss als erster Schritt das Maß der IT-Sicherheit festgelegt werden. Das Ermitteln des Maßes erfolgt durch Messen an relevanten Kriterien und Bewerten von Schwachstellen. Die gefundenen Schwachstellen sollten dann nach Eintrittswahrscheinlichkeit und nach Schaden klassifiziert werden. Das Schließen der Schwachstellen mit dem größten Schadenspotential und mit der höchsten Eintrittswahrscheinlichkeit sollte schnellst möglich erfolgen. Hierzu bietet sich die Vorgehensweise nach IT-Grundschutz an. [BSI_2011]
Klassifizierung von Unternehmensdaten	Daten sollten grundsätzlich im Unternehmen klassifiziert werden. Der IT-Grundschutz (vgl. [BSI_2011a] 100-2 Kapitel 4.3) gibt Hinweise zur Einstufung in Schutzbedarfskategorien.

Thema	*Erläuterung und weiterführende Literatur*
Kriterien und Kennzahlen	Kriterien und Kennzahlen werden benötigt, um Prozesse zu beurteilen und zielorientiert zu steuern. Dazu muss eine Definition von Kriterien und Kennzahlen erfolgen. Hierbei kann eine Orientierung an bekannten Best Practice Methoden wie ITIL [ITIL_2011] oder COBIT erfolgen.
OWASP	OWASP – Open Web Application Security Project (www.owasp.org) beschreibt die Maßnahmen für Webserver in Bezug auf IT-Sicherheit. Hierbei handelt es sich nicht um einen Standard, sondern um eine fortlaufende Ermittlung der Top 10 Sicherheitsrisiken in Webanwendungen mit Hinweisen zur Vorsorge. Somit ist OWASP praxisnah und permanent Änderungen unterzogen.
Neuer elektronischer Personalausweis	Der neue elektronische Personalausweis wird seit dem 1. November 2010 ausgegeben. Durch die eID-Funktionen können auch Unternehmen den neuen elektronischen Personalausweis sowohl für Dienstleistungen als auch für unternehmenseigene Geschäftsprozesse verwenden. Weitere Informationen stellt die Webseite zum neuen elektronischen Personalausweis (www.personalausweisportal.de) bereit.
Private Nutzung im Unternehmen – Richtlinien und Regelungen	Die Regelungen zur privaten Nutzung von betrieblichen IT-Systemen sind im IT-Grundschutz-Katalog (vgl. [BSI_2011] beschrieben. So definiert die Maßnahme M 2.9 das Nutzungsverbot nicht freigegebener Hard- und Software, die Maßnahme M 2.216 beschreibt das Genehmigungsverfahren für IT-Komponenten, M 2.62 Software-Abnahme- und Freigabeverfahren und M 4.4 den geeigneten Umgang mit Laufwerken für Wechselmedien und externe Datenspeicher. Weiterhin sind Teile im Baustein B 1.10 Standardsoftware beschrieben. Jedoch muss jede private Nutzung individuell für jedes Unternehmen geprüft werden, sodass keine allgemeine Aussage zur Vorgehensweise getroffen werden kann. Rechtliche Hinweise finden sich in der BSI-Studie: IT-Sicherheit und Recht (vgl. [BSI_2011d]) wieder.

Thema	*Erläuterung und weiterführende Literatur*
Publikationen des BSI	Publikationen des BSI stehen auf der nachfolgenden Webseite bereit: www.bsi.bund.de/DE/Publikationen/publikationen_node.html Für die IT-Sicherheit sind die folgenden Publikationen veröffentlicht worden: • BSI-Standards 100-1 bis 100-4 [BSI 2008] • ISi-Reihe [BSI_2011h] • IT-Grundschutz-Kataloge mit IT-GS-Profil für den Mittelstand • IT-Grundschutz kompakt • Leitfaden IT-Sicherheit [BSI_01] • Recht der IT-Sicherheit (juristische Studie im Auftrag des BSI) • Studie zu IT-Sicherheitsthemen • BSI-akkreditierte Auditoren • Zertifizierte IT-Produkte • Softwareangebote des BSI • Technische Richtlinien zur Aneignung von Spezialwissen • CERT-Bund • Bürger-CERT • Lageberichte des BSI
Risikomanagement	Das Risikomanagement wird technisch durch den BSI-Standard 100-3 (vgl. [BSI_2011a]) und organisatorisch durch den ISO-Standard 27005 (vgl. [ISO_2011]) erläutert. Weiterhin hat das BMI Konzepte und Leitfäden für Behörden und Unternehmen zum Thema „Kritische Infrastrukturen“ (vgl. [BMI_KRITIS]) veröffentlicht, welche ergänzende Informationen und Checklisten enthalten.

Thema	*Erläuterung und weiterführende Literatur*
Sichere Anbindung lokaler Netzwerke im Internet	Das BSI entwickelte die Schriftenreihe Internet-Sicherheit (vgl. [BSI_2011i]). Die ISi-Reihe enthält Informationen zur Anbindung lokaler Netzwerke an das Internet (ISi-S) für IT-Fachleute sowie Checklisten (ISi-Check) für Administratoren, Programmierer, Webentwickler und eine Leitlinie (ISi-L) für Führungskräfte und IT-Koordinatoren. Weiterführend sollte der BSI-Standard 100-2 (vgl. [BSI 2008]) umgesetzt sein. Für eine Beschreibung von lokalen IT-Netzen können die Bausteine „B 4.1 heterogene Netze“ und „B 4.2 Netz- und Systemmanagement“ aus dem IT-Grundschutz-Katalog (vgl. [BSI_2011]) verwendet werden.
Sichere Anbindung über das Internet	Informationen für eine sichere Anbindung über das Internet stellt das BSI in der Schriftenreihe Internet-Sicherheit (ISi-Reihe) (vgl. [BSI_2011i]) bereit. Besonders für das Thema sichere Anbindung über das Internet steht der Abschnitt ISi-VPN bereit. Darüber hinaus finden sich Hinweise in dem IT-Grundschutz-Katalog des BSI (vgl. [BSI_2011]). Hierfür sind folgende Maßnahmen relevant: • M 2.226 – Regelungen für den Einsatz von Fremdpersonal • M 2.418 – Erstellung einer Sicherheitsrichtlinie zur VPN-Nutzung • M 3.65 – Einführung in die VPN-Grundbegriffe • M 4.319 – Sichere Installation von VPN-Endgeräten • M 4.320 – Sichere Konfiguration eines VPNs

Thema	*Erläuterung und weiterführende Literatur*
Smartphone Apps	Generell ist die Verwendung und Bearbeitung von Unternehmensdaten auf Smartphones einer Sicherheits- und Nutzenabwägung zu unterziehen (z.B. bei Auslandsreisen ggf. einfaches Reise-Handy verwenden). Für Aspekte der Vertraulichkeit sind Geräte/Plattform, Betriebssystem, Serveranbindungen (VPN) und installierte Apps in Gesamtheit zu betrachten. Sicherheitskonfiguration und Auswahl der Geräte sind dem Unternehmenssicherheitskonzept entsprechend vorzunehmen. Das BSI hat zur Verwendung von Smartphones und Apps derzeit diese Empfehlungen für Privatnutzer herausgegeben (vgl. [BSI_2011e] und [BSI_2011f]). Weiterhin gibt das BSI in einer Publikation „Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen“ (vgl. [BSI_2011g]) allgemeine Hinweise zum mobilen Arbeiten.
Web 2.0	Web 2.0 wird mit den sozialen Netzen wie beispielsweise Facebook, Xing oder StudiVZ immer interessanter. Das BSI veröffentlichte die Publikation „Web 2.0 – Sicherheitsaspekte neuer Anwendungen und Nutzungsformen des Mediums World Wide Web und ihre Implementierung.“ (vgl. [BSI_2011l]) Weiterhin klärt BSI-für-Bürger (www.bsi-fuer-buerger.de) über aktuelle Themen des Web 2.0 auf. So beispielsweise „Soziale Netzwerke – Sicher unterwegs in studiVZ, Xing, Facebook & Co.“ (vgl. [BSI_2011m])
Zutrittskontrolle	Zutrittskontrollanlagen sind technische Umsetzungen von Zugangsbeschränkungen, um unerwünschte Personen von der unternehmenseigenen Infrastruktur abzuwehren. Der IT-Grundschutz-Katalog (vgl. [BSI_2011]) beschreibt in der Maßnahme M 2.17 die wesentlichen Anforderungen an eine Zutrittskontrolle.

7 Abkürzungsverzeichnis

BitBox	Browser in the Box
BSI	Bundesamt für Sicherheit in der Informationstechnik
BfV	Bundesamt für Verfassungsschutz
CERT	Computer Emergency Response Team
CMMI	Capability Maturity Model Integration
E-Mail	Electronic Mail
EU	Europäische Union
GS	Grundschutz
IfM	Institut für Mittelstandsforschung
IHK	Industrie- und Handelskammer
ISi	ISi-Reihe: BSI-Standard zur Internet-Sicherheit
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
ISMS	Informationssicherheitsmanagementsystem
IT	Informationstechnik
KMU	Kleine und mittlere Unternehmen
KPI	Key Performance Indicator
LfV	Landesämter für Verfassungsschutz
MPLS	Multiprotocol Label Switching
NAC	Network Access Control
nPA	Neuer elektronischer Personalausweis
OWASP	Open Web Application Security Project
PDCA	Plan-Do-Check-Act
PMM	Process-Maturity-Model
SLA	Service Level Agreement
SOA	Service-orientierte-Architekturen
TL	Technische Leitlinie
TR	Technische Richtlinie
VPN	Virtuelle private Netze

8 Literaturverzeichnis

[Stat 2010]: Statistisches Bundesamt, Ergebnisse aus dem Unternehmensregister, 2008, http://www.ifm-bonn.org/index.php?id=580

[BSI_2011g]: Bundesamt für Sicherheit in der Informationstechnik, Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen, 2011, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/MobilEndgeraete/mobile_endgeraete_pdf.pdf

[BSI_mE11]: Bundesamt für Sicherheit in der Informationstechnik, Neue Schwachstellen im Apple Betriebssystem iOS, 2011, https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2011/Schwachstelle-im-Apple-Betriebssystem-iOS-06072011.html

[BSI 2008]: BSI, BSI-Standards, 2008, https://www.bsi.bund.de/cln_156/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

[PBS 2005]: Sönke Peters, Rolf Brühl, Johannes Stelling, Betriebswirtschaftslehre,2005,Oldenburger Wissenschaftsverlag GmbH,3-486-57685-2

[BIP2010]: Statistisches Bundesamt, Bruttoinlands-Produkt 2010für Deutschland, 2011, http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Presse/pk/2011/BIP2010/Pressebroschuere__BIP2010,property=file.pdf

[ArM_2010]: Statistisches Bundesamt, Arbeitsmarkt, 2011, http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Content/Statistiken/Zeitreihen/LangeReihen/Arbeitsmarkt/Content75/lrerw13a,templateId=renderPrint.psml

[BDSG_4f]: Bundesministerium der Justiz, Bundesdatenschutzgesetz (BDSG), 2009, http://www.gesetze.juris.de/bdsg_1990/__4f.html

[BSI_2011]: Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kataloge, 2011, https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

[BMF2001]: Bundesfinanzministerium, Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU), 2001, http://www.bundesfinanzministerium.de/nn_53848/DE/Wirtschaft__und__Verwaltung/Steuern/Veroeffentlichungen__zu__Steuerarten/Abgabenordnung/Datenzugriff__GDPdU/002,property=publicationFile.pdf

[BSI_2011n]: Bundesamt für Sicherheit in der Informationstechnik, Sicherheitsempfehlung für Cloud Computing Anbieter - Mindestsicherheitsanforderungen in der Informationssicherheit, 2011, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf

[BSI_ITGSP]: Bundesamt für Sicherheit in der Informationstechnik, Beispiel-Profile für den IT-Grundschutz, 2008/2010, https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzKataloge/Hilfsmittel/ITGrundschutzProfile/itgrundschutzprofile_node.html

[BSI_2011d]: Bundesamt für Sicherheit in der Informationstechnik, IT-Sicherheit und Recht, 2011, https://www.bsi.bund.de/ContentBSI/Publikationen/Studien/recht/index_htm.html

[BSI_2009]: Bundesamt für Sicherheit in der Informationstechnik, BSI Technische Richtlinie 03125 - Vertrauenswürdige elektronische Langzeitspeicherung, 2009, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125.pdf

[BAKOEV]: BAKÖV, Sicher gewinnt! - Sensibilisierungsleitfaden, 2010, http://www.bakoev.bund.de/nn_7728/SharedDocs/Publikationen/LG__5/Sicher__gewinnt,templateId=raw,property=publicationFile.pdf/Sicher_gewinnt.pdf

[OB2011]: open beware, Security Awareness Training , 2011, http://www.bdg.de/beware/open-beware/index.html

[ENISA_2011]: European Network and Information Security Agency, Awareness Raising, 2011, http://www.enisa.europa.eu/act/ar

[BSI_2011o]: Bundesamt für Sicherheit in der Informationstechnik, Browser in the Box (BitBox), 2011, https://www.bsi.bund.de/DE/Themen/ProdukteTools/BitBox/BitBox_node.html

[Bund_2011]: Die Bundesregierung, Allgemeine Verwaltungsvorschriften über das Meldeverfahren gemäß §4 Abs. 6 BSIG, 2011, http://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_08122009_IT5606000111.htm

[BSI_2011k]: Bundesamt für Sicherheit in der Informationstechnik, DE-Mail, 2011, https://www.bsi.bund.de/DE/Themen/EGovernment/DeMail/DeMail_node.html

[BSI_2011h]: Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard zur Internet-Sicherheit (ISi-Reihe), 2011, https://www.bsi.bund.de/DE/Themen/InternetSicherheit/ISiReihe/isireihe_node.html

[BSI_2011a]: Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Standards, 2011, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

[BSI_2011b]: Bundesamt für Sicherheit in der Informationstechnik, Webkurs IT-Grundschutz, 2011, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Webkurs/gskurs_pdf.pdf

[BSI_2011c]: Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Zertifikat - Allgemeine Informationen, 2011,

https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzZertifikat/itgrundschutzzertifikat_node.html

[ISO_2011]: International Organization for Standardization, JTC1/SC27 - IT Security techniques, 2011, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306

[BSI_03]: Bundesamt für Sicherheit in der Informationstechnik, Leitfaden Informationssicherheit - IT-Grundschutz kompakt, 2011, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf

[BfDI_2008]: Der Bundesbeauftragte für den Datenschutz und die Informationssicherheit, Keine persönlichen Daten auf ausrangierten PCs vergessen!, 2008, http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2008/PM_37_08_KeinePersoenlichenDatenAufAusrangiertenPCsVergessen.html

[ITIL_2011]: Information Technology Infrastructure Libary, ITIL Knowlege - Overview, 2011, http://www.itil.org/en/vomkennen/itil/index.php

[BSI_01]: Bundesamt für Sicherheit in der Informationstechnik, Leitfaden Informationssicherheit – IT-Grundschutz kompakt, 2010, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf

[BMI_KRITIS]: Bundesministerium des Innern, Veröffentlichungen zum Thema "Kritische Infrastrukturen", 2009, https://www.bsi.bund.de/ContentBSI/Themen/Kritis/VeroeffentlLinks/veroeffentlichungen.html

[BSI_2011i]: Bundesamt für Sicherheit in der Informationstechnik, Struktur der BSI-Schriftenreihe zur Internet-Sicherheit (ISi-Reihe), 2011, https://www.bsi.bund.de/ContentBSI/Themen/Internet_Sicherheit/ISiReihe/ModulederISiReihe/isi-module.html

[BSI_2011e]: Bundesamt für Sicherheit in der Informationstechnik, Basisschutz für das Handy, 2011, https://www.bsi-fuer-buerger.de/cln_031/ContentBSIFB/MobileSicherheit/BasisschutzHandy/handy_tipps.html

[BSI_2011f]: Bundesamt für Sicherheit in der Informationstechnik, Wie sicher sind Smartphones?, 2011, https://www.bsi-fuer-buerger.de/cln_031/ContentBSIFB/WissenswertesHilfreiches/Service/Brennpunkt/Smartphones.html

[BSI_2011l]: Bundesamt für Sicherheit in der Informationstechnik, Web 2.0 - Sicherheitsaspekte neuer Anwendungen und Nutzungsformen des Mediums World Wide Web und ihre Implementierung", 2011, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Web20/web20_pdf.pdf

[BSI_2011m]: Bundesamt für Sicherheit in der Informationstechnik, Soziale Netzwerke - Sicher unterwegs in studiVZ, Xing, Facebook & Co., 2011, https://www.bsi-fuer-

buerger.de/BSIFB/DE/SicherheitImNetz/KommunikationUeberInternet/SozialeNetzwerke/sozialenetzwerke_node.html