Bedarfsanalyse und Konzeptentwicklung zum Aufbau und zur Weiterentwicklung der Informationssicherheit in sächsischen Kommunen

M a s t e r a r b e i t

zum Erwerb des Hochschulgrades

Master of Science (M.Sc.)

an der Hochschule Meißen (FH) und Fortbildungszentrum

Vorgelegt von

Mareen Ehret

aus Dresden

Meißen, 19.02.2020

INHALTSVERZEICHNIS

SEITE

ABKÜRZUNGSVERZEICHNIS

BfIS ..... Beauftragter für Informationssicherheit

BSI ..... Bundesamt für Sicherheit in der Informationstechnik

CIO ..... Chief Information Officer/ Beauftragter für Informationstechnologie

EU-DSGVO ..... Europäische Datenschutzgrundverordnung

ISB ..... Informationssicherheitsbeauftragter

ISMS ..... Informationssicherheitsmanagementsystem

IS ..... Informationssicherheit

IT ..... Informationstechnologie

SLKT ..... Sächsischer Landkreistag e.V.

PDF ..... Portable Document Format

SAX.CERT ..... Computer Emergency Response Team des Freistaates Sachsen

SächsEGovG ..... Sächsisches E-Government-Gesetzes

SächsISichG ..... Sächsisches Informationssicherheitsgesetzes

SSG ..... Sächsischer Städte- und Gemeindetag e.V.

SVN ..... Sächsisches Verwaltungsnetz

ABBILDUNGSVERZEICHNIS

SEITE

TABELLENVERZEICHNIS

SEITE

VORBEMERKUNG

Auf der beiliegenden CD sind neben der Masterarbeit folgende Unterlagen gespeichert:

- 32 Umfragebögen
- Übersicht Umfrageergebnisse
- Übersicht Grafiken aller Umfrageergebnisse

1 EINLEITUNG

Das Thema Informationssicherheit ist inzwischen Bestandteil des täglichen Lebens geworden. Auch durch den engen Kontakt mit Bürgerinnen und Bürgern werden in den Kommunen besonders viele schützenswerte Daten verarbeitet. Ob bei der Ausstellung einer Geburtsurkunde, der Abmeldung eines KFZ oder auch die Funktionen des neuen Personalausweises mit seiner elektronischen Identifizierungsfunktion wird deutlich, dass trotz dieser Möglichkeiten gezielt den Gefahren der Digitalisierung entgegengetreten werden muss. „Die Digitalisierung schreitet voran und verändert mehr und mehr unsere Gesellschaft. Dabei stehen sich – unter anderem – einerseits Vereinfachungen, Beschleunigung und damit einhergehend auch Optimierung, andererseits die Notwendigkeit zum Schutz der digitalen (und oftmals mit Personenbezug) versehenen Daten und Informationen gegenüber. […] Die Informationssicherheit rückt dabei in den Vordergrund und ist unabdingbarer Bestandteil der Digitalisierung.“[1] Auch die sächsischen Staats- und Kommunalverwaltungen befinden sich seit einigen Jahren im Prozess einer umfassenden Digitalisierung. Durch die Zunahme von IT-gestützten Vernetzungen gewinnt das Thema Informationssicherheit[2] immer mehr an Bedeutung.[3] Das Risiko der Beeinträchtigung eines IT-Betriebes durch Angriffe von innen und außen wie auch Nachlässigkeiten, Unkenntnis und auch fahrlässiges Handeln hat sich durch die verstärkte Abhängigkeit von moderner Kommunikationstechnik deutlich erhöht.[4]

1.1 MOTIVATION UND ZIELSETZUNG

Diese Masterarbeit entsteht in Kooperation mit der Sächsischen Staatskanzlei. Das Thema der Abschlussarbeit wurde vom Referat 44 – Informationssicherheit in der Landesverwaltung, Cybersicherheit – vergeben.

Als Forschungsgegenstand der Masterarbeit soll erörtert werden, welche Vorgaben und Orientierungshilfen vom Freistaat Sachsen aus Sicht der Kommunen zu einem effektiven Aufbau bzw. zu einer Weiterentwicklung der IS benötigt werden. Eine im Rahmen dieser Masterarbeit durchgeführte Umfrage zum genannten Forschungsgegenstand wurde u.a. aufgrund der aktuellen Gesetzeslage durch das Inkrafttreten

1 Lühr, H., Jabkowski, R., Smentek, S. (2019) S. 213
2 Der Begriff „Informationssicherheit“ wird im weiteren Verlauf des Textes – insbesondere aufgrund der besseren Lesbarkeit – häufig durch die Kurzform „IS“ ersetzt.
3 Vgl. www.publikationen.sachsen.de (2017 a) S. 5
4 Vgl. www.bsi.bund.de (2012) S. 7

des Sächsischen Informationssicherheitsgesetzes (nachfolgend kurz SächsISichG) und auch der zunehmenden Gefährdungslage der IS bei den sächsischen Kommunen erforderlich. Durch die Erhebung der Ausgangssituation durch Befragungen der Kommunen zum Thema IS sowie die Entwicklung eines Konzeptes an Maßnahmen zu deren Sicherstellung können die Ergebnisse dieser Umfrage auch bei dem Ausbau der Zusammenarbeit zwischen den sächsischen Kommunen und dem Freistaat im Rahmen der IS von Nutzen sein.

1.2 Aufbau der Arbeit

Im zweiten Kapitel erfolgt eine theoretische Betrachtung der IS u.a. im Hinblick auf die Schutzziele der IS, dem Informationssicherheitsmanagement, dem IT-Grundschutz und auch der Schutzmaßnahmen bzw. Schutzbedarfe. Dabei wird gezielt auf die theoretischen Grundlagen näher eingegangen, die ebenfalls Bestandteil der durchgeführten Umfrage sind. Ebenfalls wird in diesem Kapitel auf die IS in Sachsen mit einer Darstellung der gesetzlichen Änderungen für die sächsischen Kommunen durch das Inkrafttreten des SächsISichG und auch die Gefährdungslage näher eingegangen.
Das dritte Kapitel beinhalte eine Beschreibung der Methoden der Umfrageforschung.
Das vierte Kapitel befasst sich neben der Darstellung der Umfrageteilnehmer und der Erläuterung der Herangehensweise an die durchgeführte Umfrage bei den sächsischen Kommunen auch mit der Erhebung der Ausgangssituation auf Basis der Umfrageergebnisse.
Schwerpunkt des fünften Kapitels ist die Auswertung der von den Umfrageteilnehmern gewünschten Unterstützungsmöglichkeiten zum Aufbau und Weiterentwicklung der IS. Aufbauend darauf erfolgt eine Konzeptentwicklung zum Aufbau und Weiterentwicklung der IS in den sächsischen Kommunen. Ebenfalls werden die von den sächsischen Kommunen gewünschten Unterstützungen auf deren Realisierungsmöglichkeiten überprüft.
Abschließend erfolgen im sechsten Kapitel eine Schlussbetrachtung der Ergebnisse dieser Masterarbeit und eine kritische Würdigung sowie ein Ausblick.

2 EINFÜHRUNG IN DAS THEMA INFORMATIONSSICHERHEIT

„Das Leben im 21. Jahrhundert ist ohne Informations- und Kommunikationstechnik kaum mehr vorstellbar. Der Schutz von IT-Landschaften wird deshalb immer wichtiger.“[5] Auch geänderte Gesetzeslagen tragen dazu bei, dass die Sensibilität für Informationssicherheitsthemen erhöht wird. In der Praxis gestaltet es sich oft schwierig, ein angemessenes Sicherheitsniveau zu erreichen und aufrecht zu erhalten. Dafür kann es verschiedene Gründe geben wie z. Bsp. fehlende Ressourcen, knappe Budgets und nicht zuletzt die steigende Komplexität der IT-Systeme.[6]

Nur wenige Geschäftsprozesse kommen in der heutigen Zeit ohne IT-Unterstützung aus.[7] „Sicherheit ist ein Grundbedürfnis des Menschen – und damit unserer Gesellschaft. Gerade in Zeiten von Globalisierung, steigender Mobilität und wachsender Abhängigkeit der Industrienationen von Informations- und Kommunikationstechnik nimmt das Sicherheitsbedürfnis immer mehr zu.“[8] Die Nichtverfügbarkeit von Systemen sowie z. Bsp. manipulierte oder mutwillig zerstörte Daten können auch für die Kommunen zum Problem werden.

In diesem Kapitel wird im ersten Abschnitt das Thema IS allgemein betrachtet, wobei im ersten Abschnitt auf die Grundlagen wie Grundbegriffe, Management der IS oder das Informationssicherheitsmanagementsystem (nachfolgend kurz ISMS) näher eingegangen wird.

Im darauf folgenden zweiten Abschnitt wird das Thema IS in Sachsen näher erläutert.

2.1 GRUNDLAGEN

Zunächst soll zu Beginn dieses Kapitels zum besseren Verständnis eine Abgrenzung der Begrifflichkeiten Informationssicherheit, IT-Sicherheit und Datenschutz erfolgen.

„Die Informationssicherheit zielt auf den angemessenen Schutz von Informationen und IT-Systemen insbesondere in Bezug auf alle festgelegten Schutzziele, wie Vertraulichkeit, Integrität und Verfügbarkeit, ab. So soll insbesondere ein unbefugter Zugriff oder Manipulation von Daten verhindert und soweit möglich vorgebeugt wer-

5 www.bsi.bund.de (2012) S. 7
6 Vgl. ebd.
7 Vgl. Hanschke, I. (2019) S. 1
8 www.bsi.bund.de (2012) S. 10

den, um daraus resultierende Schäden zu verhindern. Bei den Daten ist es unerheblich, ob diese einen Personenbezug haben oder nicht. Informationen können sowohl auf Papier oder in IT-Systemen vorliegen.“[9]

„IT-Sicherheit adressiert als Teilbereich der Informationssicherheit den Schutz elektronisch gespeicherter Informationen und deren Verarbeitung inklusive Funktionssicherheit, also das fehlerfreie Funktionieren und die Zuverlässigkeit der IT-Systeme. […] Die IT-Sicherheit ist also Bestandteil der Informationssicherheit.“[10]

„Unter Datenschutz wird primär der Schutz personenbezogener Daten vor missbräuchlicher Verwendung und Datenverarbeitung verstanden, um das Recht des Einzelnen auf informationelle Selbstbestimmung zu stärken.“[11]

2.1.1 Grundwerte/ Schutzziele der Informationssicherheit

„Aufgabe der Informationssicherheit ist der angemessene Schutz der Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowie erweiterter Grundwerte, wie der Authentizität und Nichtabstreitbarkeit als Spezialfälle der Integrität.“[12]

Vertraulichkeit: „Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden.“[13] Es soll nur der Personenkreis Informationen erreichen, für die sie bestimmt sind. Informationen sollen nur von autorisierten Personen gelesen und auch verändert werden. Dazu zählt der Zugriff auf gespeicherte Daten, Dokumente und auch die Datenübertragung. Der Zugriff muss durch ein Berechtigungsmanagement geregelt werden.[14]

Verfügbarkeit: „Dem Benutzer stehen Dienstleistungen, Funktionen eines IT-Systems oder auch Informationen zum geforderten Zeitpunkt zur Verfügung.“[15] Die Verfügbarkeit beschreibt somit den Grad der unterbrechungsfreien Funktionserfüllung von IT-Systemen. Es beschreibt das Verhältnis der Zeit, in dem das System zur Verfügung stand und der vereinbarten Zeit (Service Level Agreement, SLA), in der das System hätte zur Verfügung stehen sollen. Ausprägungen für den Schutzbedarf

[9] Hanschke, I. (2019) S. 1
[10] Hanschke, I. (2019) S. 2
[11] ebd.
[12] Hanschke, I. (2019) S. 51
[13] www.bsi.bund.de (2012) S. 14
[14] Vgl. Hanschke, I. (2019) S. 52
[15] www.bsi.bund.de (2012) S. 14

in Bezug auf die Verfügbarkeit sind „sehr hoch“ (Verfügbarkeit von 99,9 % oder mehr), „hoch“ (Verfügbarkeit von 99 % oder mehr), „mittel“ (Verfügbarkeit von 95 % oder mehr) und „gering“ (Verfügbarkeit von weniger als 90 %).[16]

Integrität: „Die Daten sind vollständig und unverändert. Der Begriff „Information“ wird in der Informationstechnik für „Daten“ verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert wurden oder Angaben zum Autor verfälscht wurden oder der Zeitpunkt der Erstellung manipuliert wurde.“[17] „Integrität adressiert Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.“[18] Daten können wertlos sein, wenn die Integrität der Daten verletzt worden ist. Ausprägungen für den Schutzbedarf in Bezug auf die Integrität sind „gering“ (Datenänderungen, ob unbefugte oder fehlerhafte, stellen kein Risiko dar), „mittel“ (Maßnahmen zum Schutz der Datenintegrität sind erforderlich wie z. Bsp. Leserechte), „hoch“ (zusätzliche erweiterte technische Maßnahmen zum Schutz der Datenintegrität erforderlich) und „sehr hoch“ (über die Sicherheitsmaßnahmen für die Einstufung „hoch“ noch weitere Maßnahmen notwendig).[19]

Authentizität: „Echtheit und Glaubwürdigkeit einer Person oder eines Dienstes müssen überprüfbar sein. Unter Authentizität versteht man, sowohl einen Identitätsnachweis (der Kommunikationspartner ist der, für den er sich ausgibt) als auch die Authentizität der eigentlichen Daten (erhaltene Daten stammen auch tatsächlich von der authentisierten Instanz).“[20]

Nichtabstreitbarkeit: „Hier geht es darum, dass einen Kommunikation im Nachhinein nicht von einer der beteiligten Instanzen gegenüber Dritten abgestritten werden kann.“[21]

Als Beispiele für die Verletzung von den vorhergehend beschriebenen Schutzzielen können folgende potenzielle Gefährdungen genannt werden:

16 Vgl. Hanschke, I. (2019) S. 57
17 www.bsi.bund.de (2012) S. 14
18 Hanschke, I. (2019) S. 56
19 Vgl. ebd.
20 Hanschke, I. (2019) S. 58
21 ebd.

Vertraulichkeit	Verfügbarkeit	Integrität
– unverschlüsselte Übertragung von Informationen im Internet, die dadurch abgehört werden können – ein verlorengegangener USB-Stick mit unverschlüsselt abgespeicherten personenbezogenen Daten	– Datenträger und/ oder IT-Systeme werden durch eine Schadsoftware verschlüsselt – wichtige Anwendungen funktionieren nach einem Software-Update nicht mehr korrekt – Verzögerung der Weiterleitung von wichtigen Informationen innerhalb eines Geschäftsprozesses	– Mitarbeiter manipuliert (wichtige) Produktionsdaten, durch die beispielsweise ein wirtschaftlicher Schaden entsteht – mehrere Benutzer nutzen gleiches Benutzerkonto (z. Bsp. aus Lizenzgründen)

Tab. 1: Beispiele Verletzung Schutzziele
[Quelle: Eigene Darstellung in Anlehnung an Wegener, C.; Milde, T.; Dolle, W. (2016) S. 4]

Zur Sicherstellung der Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität gibt es Kontrollmöglichkeiten wie beispielsweise Zutritt, Zugang und Zugriff. Durch den Zutritt wird z. Bsp. die Möglichkeit des Betretens eines Serverraums bezeichnet. Es wird somit jemand in die Lage versetzt, Gegenstände in einem Raum anzufassen. Ein Beispiel für eine Zutrittskontrolle ist ein Schloss an der Tür zu einem Serverraum. Der Zugang bezeichnet die Möglichkeit, sich an einem System (Betriebssysteme o.a.) eines Rechners anzumelden oder anmelden zu können. Ein Beispiel für eine Zugangskontrolle ist die Passworteingabe bei der Anmeldung an einem Betriebssystem. Der Zugriff bezeichnet die Möglichkeit, Zugriff auf Daten eines Systems nehmen zu können oder eine entsprechende Ressource wie einen Drucker o.a. zu nutzen. Zugriffskontrollen können beispielsweise die Abbildung von Dateirechten und deren Kontrolle durch die Sicherheitsfunktionen des Betriebssystems sein.[22]

Die nachfolgende Abbildung stellt die vorhergehend beschriebenen unterschiedlichen Kontrollmöglichkeiten zur Sicherstellung der Schutzziele dar.

[22] Vgl. Wegener, C.; Milde, T.; Dolle, W. (2016) S. 4

Aus dieser wird erkennbar, dass ein Zugriff auf Informationen von der Außenwelt aus nur durch eine Überwindung der dargestellten Kontrollschichten möglich ist. Dabei tragen an jeder dieser Schichten eingerichtete Schutzmechanismen dazu bei, die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität zu erreichen. Somit können die schützenswerten Informationen angemessen abgesichert werden.[23]

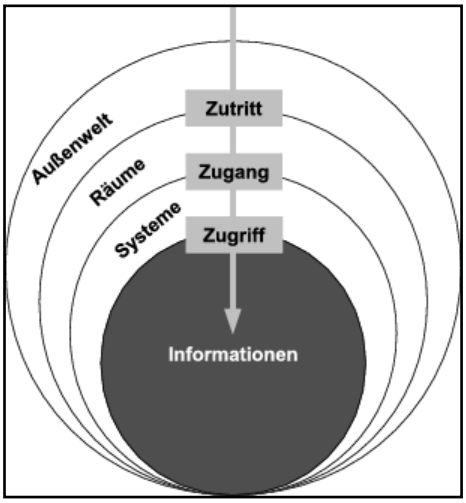


Abb. 1: Darstellung des Zwiebelschalenmodells der Zutritts-, Zugangs-, und Zugriffskontrolle
[Quelle: Wegener, C.; Milde, T.; Dolle, W. (2016) S. 5]

Die Schutzziele können dabei durch vorsätzliche Handlungen wie beispielsweise gezieltes Abhören oder Abfangen von Informationen als auch durch höhere Gewalt beeinträchtigt werden. Wie zu Beginn dieses Kapitels bereits beschrieben, erfolgt heutzutage die Verarbeitung von Informationen zum Großteil elektronisch und hat nahezu alle Lebensbereiche durchdrungen. Daher ist eine Unterscheidung, ob die Verarbeitung von Informationen elektronisch (durch IT-Systeme) oder auf Papier erfolgt, nicht erforderlich. Man geht vom Begriff der IT-Sicherheit zum Begriff der IS über. Dieser bezieht sich auf alle Informationen in allen Phasen des Geschäftsprozesses. Das nachfolgend in der ABBILDUNG 2 dargestellte Säulenmodell zur IS verdeutlicht, dass die IS von den drei Säulen Personen, Prozesse und Technik getragen wird.[24]

[23] Vgl. Wegener, C.; Milde, T.; Dolle, W. (2016) S. 5
[24] Vgl. ebd.

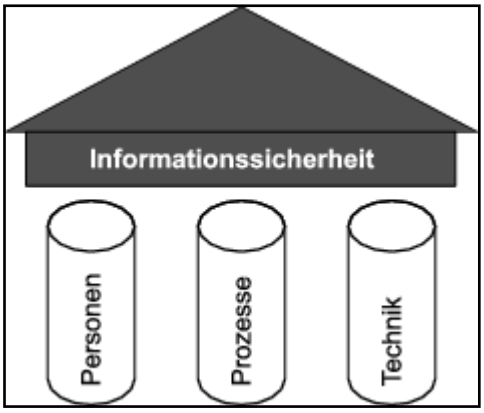


Abb. 2: Säulenmodell zur Informationssicherheit
[Quelle: Wegener, C.; Milde, T.; Dolle, W. (2016) S. 5]

IS berücksichtigt Aspekte der drei Säulen. Neben der technischen Sichtweise sind dies auch Fragestellungen bzgl. der Geschäftsprozesse und der Mitarbeiter. Die Basis für die IS bilden die in der ABBILDUNG 2 dargestellten drei Säulen.[25]

2.1.2 INFORMATIONSSICHERHEITSMANAGEMENT

„Um zu einem bedarfsgerechten, die Gefährdungslage angemessen würdigenden Sicherheitsniveau zu gelangen, ist mehr als Anschaffen von Antiviren-Software (AV-Software), Firewalls oder Datensicherungssystemen notwendig. Ein ganzheitliches Konzept ist wichtig: ein Sicherheitskonzept.“ [26]

Ein funktionierendes und in die Organisation integriertes ISMS gehört dazu. Auch die wachsende Verwundbarkeit und die Gefahr von wirtschaftlichen Schäden durch Risiken bei der Informationsverarbeitung erhöhen den Druck zu handeln. Dabei müssen durch aktives Informationssicherheitsmanagement Schäden verhindert, Gefahren begegnet und das Restrisiko minimiert werden.[27] „Entscheidend ist – und genau dies ist das Wesen des Informationssicherheitsmanagements –, sich der im jeweiligen Kontext bestehenden Risiken und Gefährdung bewusst zu sein, Schwachstellen aufzudecken und die notwendigen Strategien, Prozesse und relevanten Sicherheitsmaßnahmen zu bestimmen, umzusetzen und letztlich auch kon-

[25] Vgl. Wegener, C.; Milde, T.; Dolle, W. (2016) S. 5
[26] Sowa, A. (2017) S. 12
[27] Vgl. ebd.

sequent nachzuhalten bzw. zu kontrollieren.“ [28] „Das Managementsystem für Informationssicherheit (ISMS, Information Security Management System) legt fest, mit welchen Instrumenten und Methoden die Leitungsebene einer Organisation die auf IS ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt.“[29]

KOMPONENTEN EINES MANAGEMENTSYSTEMS FÜR INFORMATIONSSICHERHEIT

„Als Management wird einerseits die Leitungsebene, also die Gesamtheit der Führungskräfte einer Institution, und anderseits im allgemeinen Sprachgebrauch die Aufgabe der Führung der Institution bezeichnet.“[30] Die ABBILDUNG 3 verdeutlicht, dass ein Managementsystem alle Regelungen, die für die Steuerung und Lenkung einer Institution sorgen, umfasst, und zur Zielerreichung führen soll. Als ISMS wird der Teil des Managementsystems bezeichnet, der sich mit der IS beschäftigt. Dabei legt das ISMS fest, mit welchen Instrumenten und Methoden die Leitungsebene die auf IS ausgerichteten Aufgaben und Aktivitäten lenkt (plant, einsetzt, durchführt, überwacht und verbessert). Zu einem ISMS gehören grundlegende Komponenten wie Managementprinzipien, Ressourcen, Mitarbeiter und der Sicherheitsprozess. Der Sicherheitsprozess besteht dabei aus der Leitlinie zur IS, in der die Sicherheitsziele und die Strategie zu ihrer Umsetzung dokumentiert sind, dem Sicherheitskonzept und der Sicherheitsorganisation.[31]

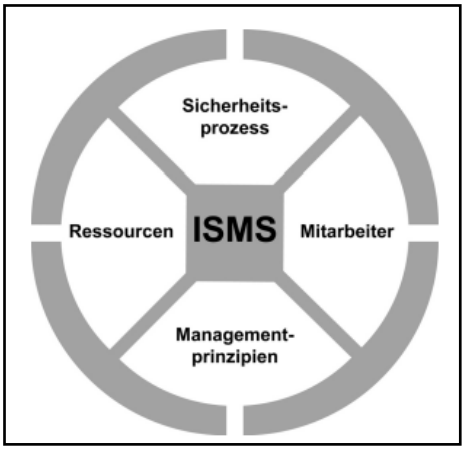


Abb. 3: Bestandteile des Managementsystems für Informationssicherheit [Quelle: www.bsi.bund.de (2017 a) S. 15]

[28] Sowa, A. (2017) S. 13
[29] ebd.
[30] www.bsi.bund.de (2017 a) S. 15
[31] Vgl. ebd.

2.1.3 IT-GRUNDSCHUTZ – DIE BSI-STANDARDS

„Der IT-Grundschutz des BSI ist eine bewährte Methodik, um das Niveau der IS in Behörden und Unternehmen jeder Größenordnung zu erhöhen. Die Angebote des IT-Grundschutzes gelten in Verwaltung und Wirtschaft als Maßstab, wenn es um die Absicherung von Informationen und den Aufbau eines Managementsystems für Informationssicherheit (ISMS) geht.“[32]

Die Standards des Bundesamtes für Sicherheit in der Informationstechnik (nachfolgend kurz BSI) beinhalten bzw. beschreiben verschiedene Methoden und Vorgehensweisen zu Themen aus dem Bereich der IS. Im BSI-Standard 200-1 werden allgemeine Anforderungen an ein ISMS beschrieben. Der BSI-Standard 200-2 dient dem Aufbau eines ISMS durch die Beschreibung der IT-Grundschutz-Methodik.[33] „Dabei steht mit der Standard-Absicherung die bewährte IT-Grundschutz-Vorgehensweise zur Verfügung. Sie wird ergänzt durch die Basis-Absicherung, die eine grundlegende Erst-Absicherung in der Breite ermöglicht, sowie durch die Kern-Absicherung, die sich dem Schutz der besonders schützenswerten Daten einer Institution widmet.“[34] Der BSI-Standard 200-3 enthält alle risikobezogenen Arbeitsschritte bei der Umsetzung des IT-Grundschutzes zum Risikomanagement. Das BSI bietet Behörden zwei Möglichkeiten an, Aktivitäten zur Erhöhung der IS testieren bzw. zertifizieren zu lassen. Zum Einen gibt es die Möglichkeit der Testierung nach der Basis-Absicherung und zum Anderen die Zertifizierung der Standard- bzw. Kern-Absicherung. Die Basis-Absicherung testiert die Umsetzung der Basis-Anforderungen des IT-Grundschutz-Kompendiums. Diese Anforderungen lassen sich mit einem relativ geringen finanziellen, personellen und zeitlichen Aufwand umsetzen. Daher ist die Basis-Absicherung auch für kleine Kommunen gut geeignet, erste Maßnahmen zur ganzheitlichen IS umzusetzen. Wenn z. Bsp. Kommunen vorrangig die wichtigsten Geschäftsprozesse bzw. Fachaufgaben schützen möchten, bietet sich die Kern-Absicherung des IT-Grundschutzes an. Wenn die IS ganzheitlich nach dem Stand der Technik umgesetzt werden soll, sollte die Standard-Absicherung angestrebt werden. Zusammenfassend ermöglicht die Basis-Absicherung einen schnellen Einstieg und eine grundlegende Absicherung in der Breite. Die Kern-Absicherung bietet für einen Teilbereich einen umfassenden Schutz in der Tiefe. [35]

---

[32] www.bsi.bund.de (o.J.a)
[33] Vgl. ebd.
[34] ebd.
[35] Vgl. ebd.

2.1.4 Übersicht über den Informationssicherheits-prozess

„Die Vorgehensweisen nach IT-Grundschutz bieten Hilfestellungen beim Aufbau und bei der Aufrechterhaltung des Prozesses der Informationssicherheit in einer Institution, indem Wege und Methoden für das generelle Vorgehen, aber auch für die Lösung spezieller Probleme aufgezeigt werden.“[36] Bei der Gestaltung des Sicherheitsprozesses ist ein systematisches Vorgehen erforderlich. Somit kann ein angemessenes Sicherheitsniveau erreicht werden.[37]

Wie in der Abbildung 4 dargestellt ist, besteht der Sicherheitsprozess aus verschiedenen Phasen.

Dabei ist im Rahmen der Initiierung des Sicherheitsprozesses die Verantwortung der Leitungsebene bedeutsam. Diese beinhaltet im Rahmen der IS die Initiierung, Steuerung und Kontrolle des Informationssicherheitsprozesses. Auch Entscheidungen zum Umgang mit Risiken sowie die notwendigen Ressourcen zur Verfügung zu stellen, fallen in den Verantwortungsbereich der Leitungsebene. Die Leitungsebene muss für die Bedeutung der IS sensibilisiert werden. Dazu gehören z. Bsp. die Beschreibung von Anforderungen aus gesetzlichen Vorgaben sowie das Aufzeigen von Risiken für die Organisation und deren Prozesse mit den damit verbundenen Auswirkungen und Kosten.[38]

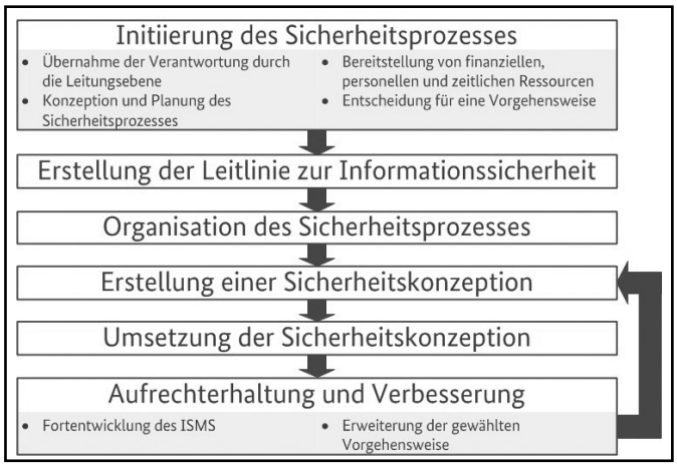


Abb. 4: Phasen des Sicherheitsprozesses
[Quelle : www.bsi.bund.de (2017 b) S. 15]

[36] www.bsi.bund.de (2017 b) S. 14
[37] Vgl. ebd.
[38] Vgl. www.bsi.bund.de (2017 b) S. 16

Für die Gestaltung des Sicherheitsprozesses ist die Erstellung einer Leitlinie zur IS essentiell. Durch sie werden die Sicherheitsziele und das angestrebte Sicherheitsniveau beschrieben. Für das Informationssicherheitsmanagement ist der Aufbau einer Organisationsstruktur notwendig, die in ihrer Größe und Art geeignet sein muss. Ebenfalls ist die Erstellung eines Sicherheitskonzepts für die Institution erforderlich. Grundlagen dafür finden sich in den Bausteinen des IT-Grundschutz-Kompendiums beispielsweise für Komponenten von Geschäftsprozessen, Anwendungen, IT-Systeme und weiteren Objekten entsprechende Sicherheitsanforderungen. Dabei muss unterschieden werden, ob eine Basis-, Standard- oder Kern-Absicherung angestrebt wird. Je nach Absicherung sehen die Aktivitäten zur Erstellung einer Sicherheitskonzeption etwas anders aus. Jedoch basieren alle grundsätzlich auf den Vorarbeiten, die mit der Erstellung des IT-Grundschutz-Kompendiums geleistet worden sind.[39] Die ABBILDUNG 5 gibt einen Überblick über den Lebenszyklus eines Sicherheitskonzepts.

Abb. 5: Überblick über den Lebenszyklus eines Sicherheitskonzepts [Quelle : www.bsi.bund.de (2017 a) S. 33]

Im Rahmen der Umsetzung des Sicherheitskonzepts lässt sich ein ausreichendes Sicherheitsniveau nur durch die Ermittlung der bestehenden Defizite und die konse-

[39] Vgl. www.bsi.bund.de (2017 b) S. 16-17

quente Umsetzung der erforderlichen und identifizierten Maßnahmen erreichen. Die kontinuierliche Verbesserung der IS zielt darauf ab, dass angestrebte Sicherheitsniveau zu erreichen, dauerhaft aufrechtzuerhalten und zu verbessern. Daher müssen die Sicherheitsprozesse und die Organisationsstrukturen für IS regelmäßig auf Angemessenheit, Wirksamkeit und Effizienz überprüft werden.[40]

2.1.5 SCHUTZMAßNAHMEN/ SCHUTZBEDARFE

Ein weiterer Bestandteil des IT-Sicherheitskonzepts ist die Festlegung der Schutzbedarfe.

Durch Veränderungen in der Gesetzeslage können hohe Bußgelder bei Datenpannen im Zusammenhang mit der EU Datenschutzgrundverordnung anfallen.[41] „Es stellt sich also nicht die Frage, ob man Informationssicherheit und Datenschutz in seinem Unternehmen adressiert, sondern nur wann und in welchem Umfang.“[42] „Systeme sind sicher, wenn der Aufwand eines Angreifers dessen Nutzen erheblich übersteigt. […] Der konkrete Schutzbedarf hängt hierbei stark von der unternehmensindividuell eingeschätzten Kritikalität der jeweiligen Unternehmenswerte, wie z.B. Informationen oder Systeme, ab. Jedoch ist eine hundertprozentige Sicherheit auch mit noch so hohem Aufwand nicht zu erreichen. Ein hinreichender Informationsschutz ist hierbei ebenso wie eine Standard-Absicherung der IT schon aber mit verhältnismäßig geringen Mitteln zu erreichen.“[43]

Um ein erforderliches Schutzniveau zu erreichen, müssen die Sicherheitsmaßnahmen zur Erreichung und Aufrechterhaltung einer störungsfreien Informationsverarbeitung einerseits wirksam (effektiv) und andererseits wirtschaftlich angemessen (effizient) sein. Das Schutzniveau wird maßgeblich von der Kritikalität der zu schützenden Vermögenswerte eines Unternehmens (Assets) wie z. Bsp. Kundendaten beschrieben, sowie durch geltende Gesetze und Regularien, die eingehalten werden müssen, bestimmt. Wirtschaftlich angemessen müssen die Schutzmaßnahmen sein, damit sie die Organisation im Hinblick auf Beeinträchtigungen der Aufbau- und Ablauforganisation sowie weiterer Randbedingungen nicht überfordern. Schutzbedarfe werden festgelegt für Anwendungen (Informationen, Prozesse), räumliche Infrastrukturen, Informationstechniken und Netze.[44]

[40] Vgl. www.bsi.bund.de (2017 b) S. 16-17
[41] Vgl. Hanschke, I. (2019) S. 2
[42] Hanschke, I. (2019) S. 2
[43] Hanschke, I. (2019) S. 2-3
[44] Vgl. Müller, K.-R. (2014) S. 180-182

Ein Zielbild der Schutzmaßnahmen ist in der nachfolgenden ABBILDUNG 6 dargestellt.

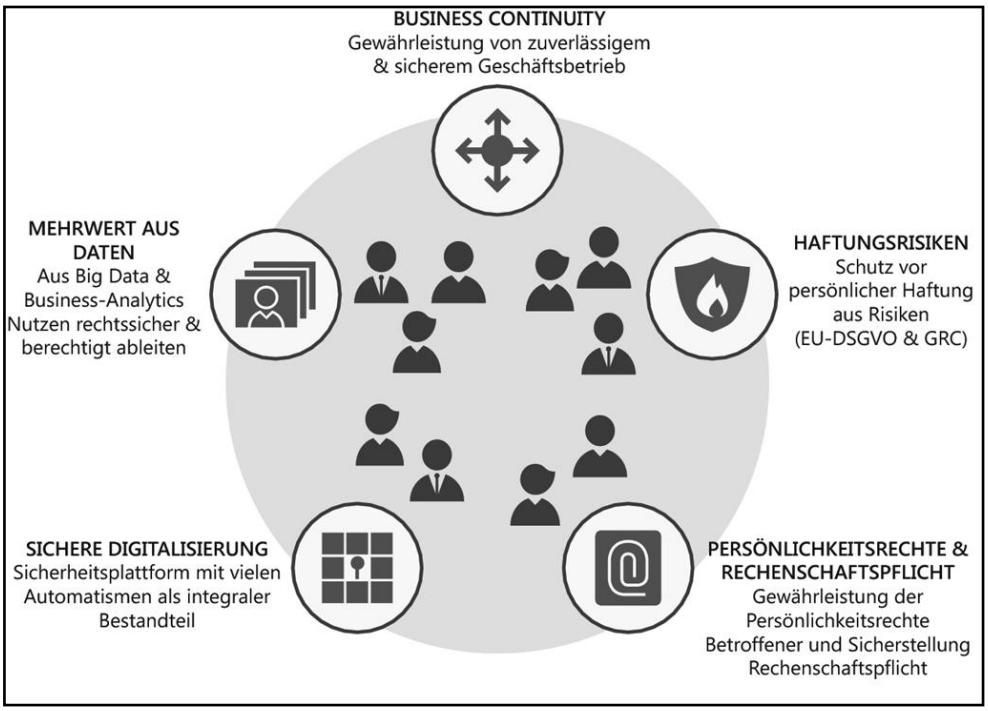


Abb. 6: Nutzen-stiftende Sicherheit
[Quelle : Hanschke, I. (2019) S. 5]

Die Schutzbedarfsfeststellung dient der Ermittlung, welcher Schutz für die in Geschäftsprozessen verarbeiteten Informationen und die eingesetzte Informationstechnik als ausreichend und angemessen betrachtet werden kann. Dabei wird für jede Anwendung sowie die verarbeiteten Informationen eine Betrachtung der zu erwartenden Schäden, die bei einer Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können, durchgeführt. Ebenfalls ist es wichtig, die möglichen Folgeschäden realistisch einzuschätzen. Die Einteilung erfolgt dabei in die drei Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“.[45]
Die ANLAGE 1 gibt einen Überblick über die einzelnen Schutzbedarfskategorien im Sinne des in KAPITEL 2.1.3 aufgezeigten BSI Standard 200-2. In der ABBILDUNG 7 erfolgt eine grafische Darstellung der Einteilung der Schutzbedarfe.

[45] Vgl. www.bsi.bund.de (2017 b) S. 72

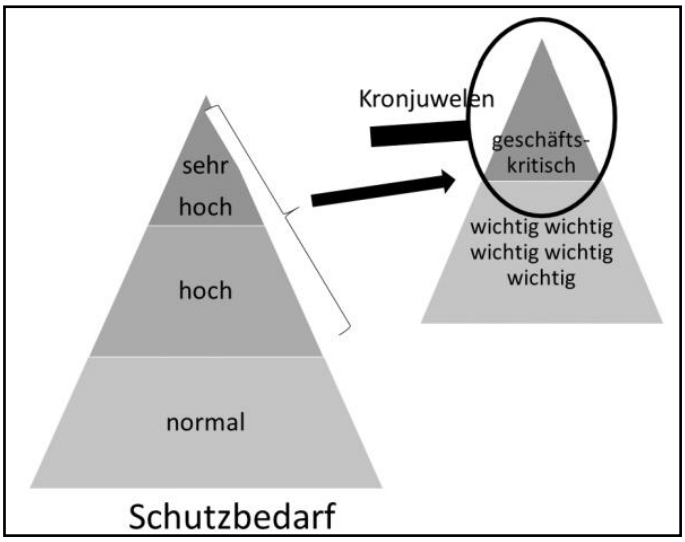


Abb. 7: Schutzbedarf
[Quelle : www.bsi.bund.de (2017 b) S. 73]

2.1.6 DER INFORMATIONSSICHERHEITSBEAUFTRAGTE

Die Ernennung eines Informationssicherheitsbeauftragten (nachfolgend kurz ISB) dient der Verhinderung von unklaren Zuständigkeiten im Rahmen der IS. Dadurch ist eine Übertragung der Verantwortung auf einen Hauptansprechpartner für alle Aspekte rund um die IS möglich. Dieser koordiniert die Aufgabe „Informationssicherheit“ und treibt diese innerhalb der Institution voran. Dabei hängt es von der Art und Größe der Institution ab, ob es eine oder weitere Personen mit Sicherheitsaufgaben gibt. Geeignet ist die Position des ISB direkt der obersten Leitungsebene zuzuordnen. Ein Nachteil der Verankerung der Tätigkeit eines ISB in der IT-Abteilung liegt darin, dass es hierbei zu Rollenkonflikten kommen kann. Die Verantwortlichkeiten bei der Planung, Umsetzung und Aufrechterhaltung des Sicherheitsprozesses müssen klar definiert werden. Es muss eine Definition von Rollen für die verschiedenen Aufgaben im Hinblick auf das Erreichen der Informationssicherheitsziele erfolgen. Damit diese Rollen ausgefüllt werden können, bedeutet dies ebenfalls, dass Personen benannt sein müssen, die qualifiziert sind und denen im ausreichenden Maße Ressourcen zur Verfügung stehen.[46]

[46] Vgl. www.bsi.bund.de (2017 b) S. 40

Zuständigkeiten und Aufgaben

Die Zuständigkeit des ISB liegt in der Wahrnehmung aller Belange der IS innerhalb der Institution. Dabei besteht die Hauptaufgabe des ISB in der Beratung und Unterstützung der Behörden- bzw. Unternehmensleitung bei der Aufgabenwahrnehmung und Umsetzung bezüglich der IS.
Aufgaben des ISB sind unter anderem:[47]

- „den Informationssicherheitsprozess zu steuern und an allen damit zusammenhängenden Aufgaben mitzuwirken,
- die Leitungsebene bei der Erstellung der Leitlinie zur Informationssicherheit zu unterstützen,
- die Erstellung des Sicherheitskonzepts, des Notfallvorsorgekonzepts und anderer Teilkonzepte und System-Sicherheitsrichtlinien zu koordinieren sowie weitere Richtlinien und Regelungen zur Informationssicherheit zu erlassen, die Realisierung von Sicherheitsmaßnahmen zu initiieren und zu überprüfen,
- der Leitungsebene und dem IS-Management-Team über den Status quo der Informationssicherheit zu berichten,
- sicherheitsrelevante Projekte zu koordinieren,
- Sicherheitsvorfälle zu untersuchen und Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit zu initiieren und koordinieren.“[48]

Bei größeren Projekten, die Auswirkungen auf die Informationsverarbeitung haben können, ist der ISB zu beteiligen. Somit kann die Beachtung von Sicherheitsaspekten in den einzelnen Projektphasen gewährleistet werden.[49]

Anforderungsprofil

Es ist empfehlenswert, dass der ISB zur Erfüllung dieser Aufgaben über Wissen und Erfahrung auf den Gebieten der IS/ IT und ebenfalls über Kenntnisse der Geschäftsprozesse der Institution verfügt. Unter anderem sollten folgende Kenntnisse vorhanden sein:[50]

- „Identifikation mit den Zielsetzungen der Informationssicherheit, Überblick über Aufgaben und Ziele der Institution.

[47] Vgl. www.bsi.bund.de (2017 b) S. 41
[48] ebd.
[49] Vgl. ebd.
[50] Vgl. ebd.

- Kooperations- und Teamfähigkeit, aber auch Durchsetzungsvermögen (Kaum eine Aufgabe erfordert so viel Fähigkeit und Geschick im Umgang mit anderen Personen: Die Leitungsebene muss in zentralen Fragen des Sicherheitsprozesses immer wieder eingebunden werden. Entscheidungen müssen eingefordert werden und die Mitarbeiter müssen, eventuell mithilfe des Bereichs-Sicherheitsbeauftragten, in den Sicherheitsprozess eingebunden werden).
- Erfahrungen im Projektmanagement, idealerweise im Bereich der Systemanalyse und Kenntnisse über Methoden zur Risikoanalyse.
- Grundlegende Kenntnisse über die Prozesse und Fachaufgaben innerhalb der Institution und, soweit erforderlich, Grundkenntnisse in den Bereichen IT und ICS.
- Ein Informationssicherheitsbeauftragter muss zudem die Bereitschaft mitbringen, sich in neue Gebiete einzuarbeiten und Entwicklungen in der IT zu verfolgen. Er sollte sich so aus- und fortbilden, dass er die erforderlichen Fachkenntnisse für die Erledigung seiner Aufgaben besitzt.“[51]

UNABHÄNGIGKEIT

Es empfiehlt sich, die Position des ISB organisatorisch als Stabstelle (direkt der Leitungsebene zugeordnete Position) einzurichten. Der ISB muss ein direktes und jederzeitiges Vorspracherecht gegenüber der Behörden- bzw. Unternehmensleitung haben. Somit kann er direkt der Leitungsebene über Sicherheitsvorfälle, -risiken und -maßnahmen informieren. Eine frühzeitige und umfassende Unterrichtung des ISB über das Geschehen in der Institution muss sichergestellt werden, soweit diese Bezug zu seiner Tätigkeit haben. Wie bereits erwähnt, sollte der ISB organisatorisch nicht der IT-Abteilung zugeordnet werden.[52] „Die Erfahrung hat zeigt, dass dies häufig dazu führt, dass die Aufgabe der Informationssicherheit auf IT-Absicherung reduziert wird und der ganzheitliche Schutz von Informationen in den Hintergrund gerückt wird.“[53]

[51] www.bsi.bund.de (2017 b) S. 41-42
[52] vgl. www.bsi.bund.de (2017 b) S. 42
[53] ebd.

2.2 Informationssicherheit in Sachsen

Zu Beginn des vergangenen Jahres wurden durch die Sächsische Landesregierung zwei Gesetzentwürfe in den Landtag eingebracht: Zum Einen das Gesetz zur Gewährleistung der IS im Freistaat Sachsen (Sächsisches Informationssicherheitsgesetz) und zum Anderen ein Gesetz zur Änderung des IT-Staatsvertrags.[54] Der Beauftragte für Informationstechnologie (nachfolgend kurz CIO) des Freistaates Sachsen Thomas Popp beschreibt das Inkrafttreten des SächsISichG in einem Beitrag der Fachzeitschrift Sachsenlandkurier wie folgt: „Mit dem Informationssicherheitsgesetz schafft der Freistaat die Grundlage, dass alle Behörden in Sachsen moderne Erkennungs- und Abwehrtechnologien einsetzen dürfen, um Cyber-Angriffe zu identifizieren und abzuwehren. […] Mit der zunehmenden Digitalisierung der Verwaltung vertrauen die Bürgerinnen und Bürger der Verwaltung immer mehr Daten an […]. Die Möglichkeit des Bürgers, seine persönlichen Daten online mitzuteilen, geht daher mit der Pflicht der Verwaltung einher, diese Daten zu schützen.“[55] Die Änderung des IT-Staatsvertrages beinhaltet die Gründung einer Bund-Länder-Anstalt öffentlichen Rechts. In dieser sollen personelle und finanzielle Ressourcen bei der föderalen IT-Kooperation gebündelt werden.[56]

2.2.1 Gesetz zur Gewährleistung der Informationssicherheit im Freistaat Sachsen (Sächsisches Informationssicherheitsgesetz – SächsISichG)

CIO Thomas Popp beschreibt in seinem vorhergehend genannten Beitrag, dass das SächsISichG technische und organisatorische Umsetzungsmaßnahmen sowie rechtliche Regelungen miteinander verbindet.[57] Mit dem Gesetz zur Neuordnung der Informationssicherheit im Freistaat Sachsen trat entsprechend Artikel 1 zum 02. August 2019 zum Einen das Gesetz zur Gewährleistung der Informationssicherheit im Freistaat Sachsen (SächsISichG) in Kraft. Zum Anderen wurden entsprechend Artikel 2 des Gesetzes zur Neuordnung der Informationssicherheit im Freistaat Sachsen die Änderung des Sächsischen E-Government-Gesetzes (nachfolgend kurz SächsEGovG) beschlossen. Durch die Regelungen des SächsISichG soll ein umfassenderer Einblick in die IT-Systeme der sächsischen Verwaltungen er-

[54] Vgl. www.medienservice.sachsen.de (2019)
[55] ebd.
[56] Vgl. ebd.
[57] Vgl. Sachsenlandkurier (2019) S. 186

möglicht werden.[58] Auch beschreibt Popp, dass vorgesehen ist, „ […] dass die zentralen Stellen der IT-Sicherheit genauer und umfassender als bisher die Datenströme in den Verwaltungen auf gefährliche Inhalte untersuchen und auswerten. Nur so lassen sich die Schutzmaßnahmen wirkungsvoller ausrichten. Hierfür braucht es eine Rechtsgrundlage, weil z.B. E-Mails auch personenbezogene Daten enthalten können bzw. nur noch verschlüsselt ausgetauscht werden. Wir müssen aber unter Wahrung der informationellen Selbstbestimmung des Einzelnen dennoch die Erlaubnis haben E-Mails zu analysieren, um einen wirkungsvollen Schutz aufrecht zu erhalten.“[59] Das Gesetz soll Ermächtigungen für alle Behörden im Freistaat Sachsen schaffen, damit moderne Erkennungs- und Abwehrtechnologien eingesetzt werden können und zu jedem Zeitpunkt ein hochaktuelles Gefahrenabwehrsystem besteht. Durch das SächsISichG soll als weiteres Ziel die Sicherheitsorganisation gestärkt werden, indem sie mit strategisch und operativ ausreichenden Handlungskompetenzen ausgestattet wird. Ebenfalls wird im SächsISichG geregelt, dass alle Mitarbeiter jeder Behörde im Rahmen der IS zu sensibilisieren sind.[60] Es ergeben sich durch den Beschluss des SächsISichG umfangreiche Änderungen im Hinblick auf die IS in Sachsen.

Bisherige Verwaltungsvorschriften zur IS sowie die jeweiligen Regelungen im SächsEGovG werden zusammengefasst und durch das SächsISichG erweitert. Ebenfalls werden durch die Neuerungen u.a. auch die Kommunen in den Anwendungsbereich des Gesetzes einbezogen. Gleichfalls werden die Befugnisse der Beauftragten für Informationssicherheit (nachfolgend kurz BfIS) und des Computer Emergency Response Team des Freistaates Sachsen (nachfolgend kurz Sicherheitsnotfallteams oder SAX.CERT) ausgeweitet. Eine Rechtsgrundlage für die Möglichkeit des Einsatzes modernen Erkennungs- und Abwehrtechnologien sowie die Einführung verschiedener Meldepflichten über Sicherheitsvorfälle wurden mit dem Gesetz geschaffen bzw. eingeführt.[61]

Im nun folgenden Absatz sollen die wesentlichen Bestandteile des einzelnen Paragraphen des SächsISichG aufgezeigt werden.[62]

Die allgemeinen Vorschriften des ersten Abschnittes regeln unter anderem den Anwendungsbereich des Gesetzes. In diesen Bereich fallen die staatlichen Stellen des Freistaates Sachsen sowie die seiner Aufsicht unterliegenden Körperschaften (also

[58] Vgl. Sachsenlandkurier (2019) S. 186
[59] ebd.
[60] Vgl. ebd.
[61] Vgl. Sachsenlandkurier (2019) S. 187
[62] Wenn in den nachfolgenden Absätzen des Kapitels 2.2.1 der Begriff „Gesetz“ genannt wird, ist damit – insbesondere aufgrund der besseren Lesbarkeit – das SächsISichG gemeint.

die Kommunen), Anstalten und Stiftungen des öffentlichen Rechts als nicht-staatliche Stellen. Die in § 4 genannten Grundsätze der IS sind im Wesentlichen identisch mit den Regelungen aus dem SächsEGovG. Ziel dieses Paragraphen ist die Festlegung der zu treffenden organisatorischen und technischen Vorkehrungen der staatlichen Stellen zur Einhaltung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit für die in ihren IT-Systemen verarbeiteten Daten. Dabei sind die BSI-Standards in Verbindung mit dem BSI-Grundschutz einzubeziehen. Als eine weitere wesentliche Neuerung ist zu erwähnen, dass der Stand der Technik für technische Maßnahmen maßgeblich ist. Überdies sollen staatliche Stellen ein ISMS erstellen. Auch nicht-staatliche Stellen, also auch Kommunen, wird die Absicherung eines angemessenen Informationssicherheitsniveaus vorgeschrieben. Diese Regelung ist jedoch bereits Bestandteil der Regelungen des SächsEGovG.[63]

Die gesetzlichen Regelungen des zweiten Abschnittes beziehen sich auf die Organisation der IS. Änderungen gibt es durch das Gesetz im Hinblick auf die Zuständigkeit des SAX.CERT. Die Zuständigkeit des Sicherheitsnotfallteams erstreckt sich dabei auf die operativen Fragen der IS aller staatlichen und nicht-staatlichen Stellen. Der Aufgabenbereich des SAX.CERT wird durch das Gesetz um die Erfassung und Analyse von Sicherheitsgefährdungen erweitert und gleichfalls wird im SAX.CERT eine zentrale Meldestelle (nach dem BSI-Gesetz) für Sicherheitsvorfälle in den staatlichen und nicht-staatlichen Stellen etabliert. Der BfIS Land und das SAX.CERT stehen auch den nicht-staatlichen Stellen (u.a. den Kommunen) beratend zur Verfügung. Das Gesetz regelt ebenfalls, dass in den staatlichen Stellen BfIS zu ernennen sind. Nicht staatliche-Stellen sollen eine Informationssicherheitsorganisation aufbauen, können jedoch dabei flexibel vorgehen, indem sich mehrere Kommunen zusammenschließen und zusammen einen BfIS benennen, deren Aufgaben auch an Externe übertragen werden können.[64]

Im dritten Abschnitt des Gesetzes werden die Maßnahmen zur Sicherstellung der IS definiert, in dem es die Rechtsgrundlage für die Erhebung und automatisierte Auswertung von Daten, die beim Betrieb von IT-Systemen der staatlichen und nicht-staatlichen Stellen anfallen, schafft. Dies darf jedoch nur im Zusammenhang mit einer eventuellen Verhinderung oder Abwehr von Angriffen auf die IT-Systeme stehen. Auch ebnet das Gesetz die Rechtsgrundlage zur Nachverfolgung von Datenströmen, wenn z. Bsp. Schadprogramme oder Sicherheitslücken festgestellt werden.[65]

[63] Vgl. Sachsenlandkurier (2019) S. 187 i.V.m. www.itof2018.org (2018)
[64] Vgl. ebd.
[65] Vgl. ebd.

Der vierte Abschnitt des Gesetzes regelt die Meldepflichten behördenübergreifend sowie die Meldepflichten der staatlichen und nicht-staatlichen Stellen. Die Schlussvorschriften werden im fünften und letzten Abschnitt des Gesetzes geregelt.

2.2.2 GEFÄHRDUNGSLAGE

Laut dem Jahresbericht des Beauftragten für Informationssicherheit des Landes konnten im Jahr 2017 über 1.800 Angriffe aus dem Internet auf das Sächsische Verwaltungsnetz (nachfolgend kurz SVN) abgewehrt werden. Dies entspricht 28 % mehr als im Jahr 2016. Ebenfalls konnten 2017 knapp 79 Mio. Spam-E-Mails bereits im Vorfeld abgewiesen werden. Gleichzeitig konnten in dem betreffenden Jahr aus den rund 31 Mio. eingegangenen E-Mails über 36.000 Schadprogramme aufgespürt und entfernt werden.[66]

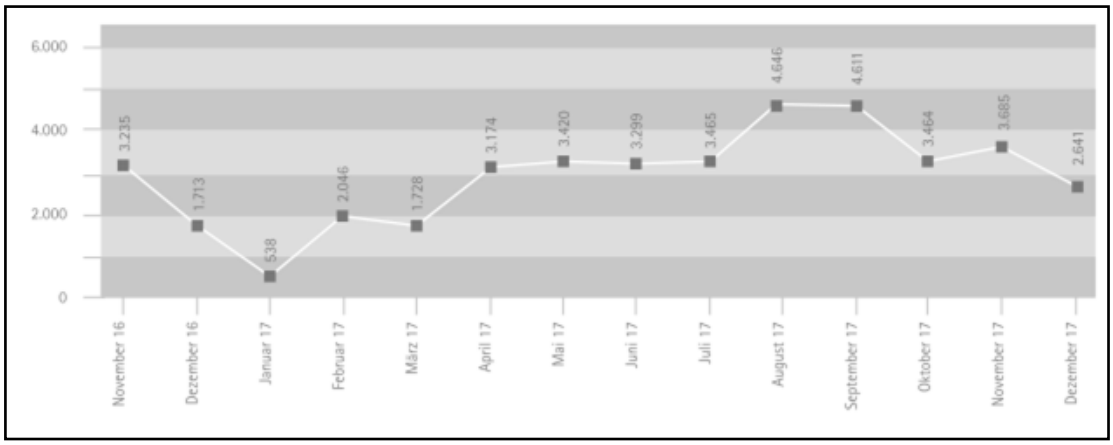


Abb. 8: Schadprogramme im SVN-Mailverkehr
[Quelle : www.publikationen.sachsen.de (2017 a) S. 10]

[66] Vgl. www.publikationen.sachsen.de (2017 a) S. 9

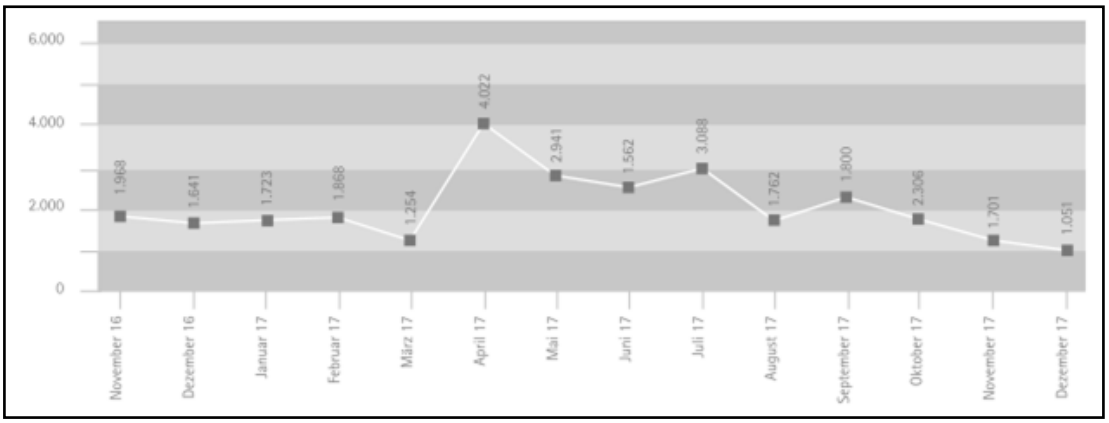


Abb. 9: Schadprogramme im SVN-Internetverkehr
[Quelle : www.publikationen.sachsen.de (2017 a) S. 10]

Entsprechend der Mitteilung der Sächsischen Staatskanzlei haben die Cyber-Angriffe auf das sächsische Verwaltungsnetz im Jahr 2018 im Vergleich zu 2017 wiederholt zugenommen. Das SAX.CERT benennt z. Bsp. die Zahl der im Jahr 2018 abgewiesenen Spam-Mails mit knapp 80 Millionen. Dies entspricht einer Steigerung von über 60 % im Vergleich zu 2017. Weiterführend sind im E-Mail-Verkehr laut SAX.CERT fast 100.000 und somit 170 % mehr Viren als im Vorjahr erkannt worden.[67]

Im Frühjahr 2019 wurden dem SAX.CERT 16 Fälle mitgeteilt, in denen infolge einer Infektion mit einer Schadsoftware Landesdaten abgeflossen sind. Die entsprechenden Hinweise über den Angriff kamen jedoch überwiegend von externen Quellen, teils auch aus dem Ausland.[68]

[67] Vgl. www.medienservice.sachsen.de (2019)
[68] Vgl. Behördenspiegel (2019) S. 28

3 METHODEN DER UMFRAGEFORSCHUNG

„Wenn man Umfrageforschung betreibt, ist man nicht an der Meinung konkreter einzelner Personen interessiert, obwohl naturgemäß immer nur Einzelpersonen befragt werden können. Dies mag widersprüchlich anmuten, ist aber eine unabdingbare Voraussetzung für Befragungen bzw. für jede Form von quantifizierbarer Forschung.“[69] Die ABBILDUNG 10 gibt einleitend in dieses Kapitel einen Überblick über den Umfrageprozess, der im Folgenden näher erläutert wird.

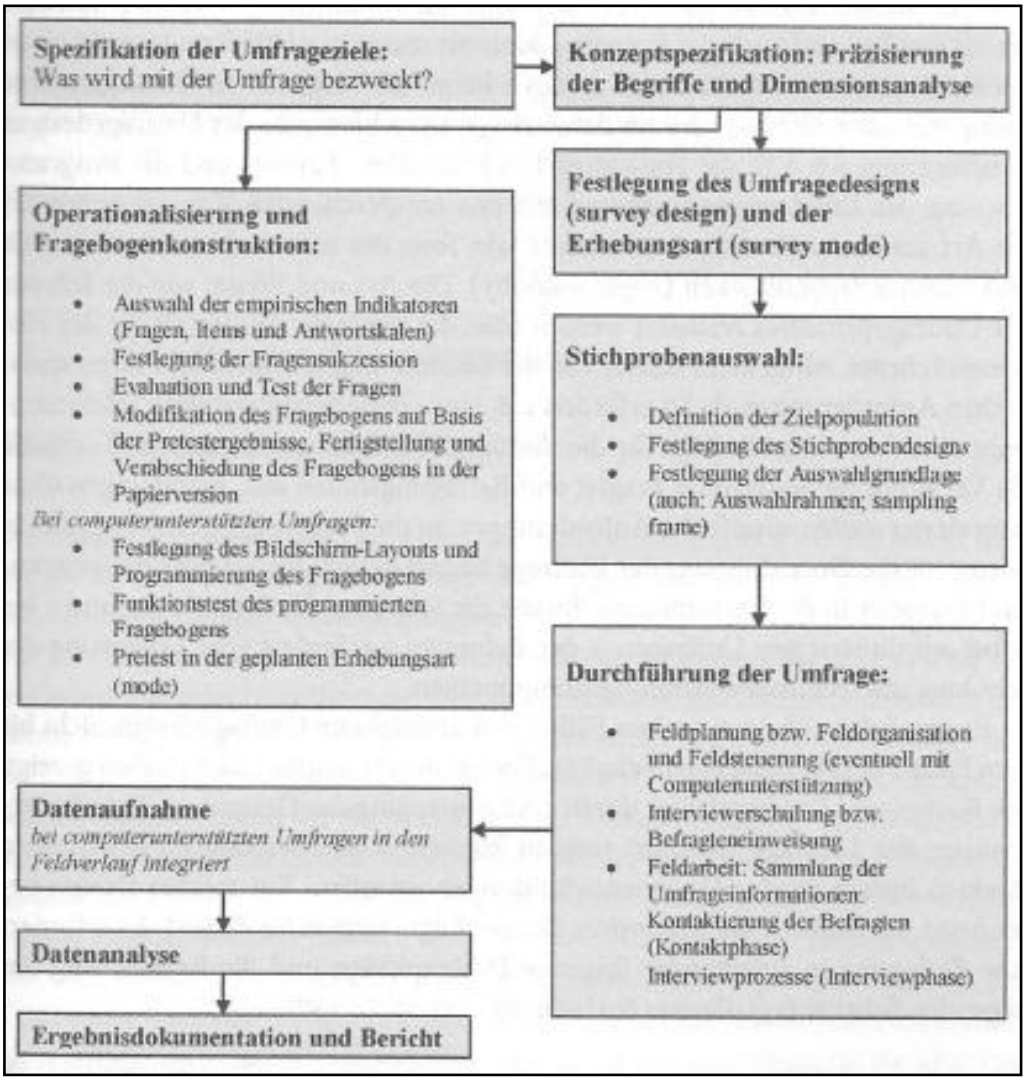


Abb. 10: Umfrageprozess
[Quelle : Faulbaum, F. (2019) S. 13]

[69] Jacob, R.; Heinz, A.; Décieux, J. P. (2013) S. 3

3.1 Überlegungen vor der Durchführung einer Umfrage

Die Frage, was man mit einer Umfrage herausfinden möchte, wonach gefragt wird und ob es bereits Antworten gibt, können als Ziele einer Umfrage betrachtet werden. Die Vorbereitung einer Umfrage beinhaltet ebenfalls die Suche nach dem richtigen bzw. für die Umfrage passenden Instrument zur Durchführung der Umfrage. Dabei stellt sich die Frage, ob man Daten standardisiert mit einem Fragebogen oder offen in einem Interview erheben möchte und ob die Umfrage schriftlich, telefonisch oder persönlich erfolgen wird. Bei der Auswahl der Umfrage stellt man sich ebenfalls die Frage, ob eine Vollerhebung notwendig ist oder eine Stichprobe als ausreichend angesehen wird. Entscheidet man sich für eine Stichprobe, empfiehlt es sich vorab eine Personenanzahl zu bestimmen, die man zu befragen erwägt. Die Teilnahmebereitschaft dieser Teilnehmer kann vorab analysiert werden, um aussagekräftige Ergebnisse zu erhalten. Überlegungen, wie man die Teilnahmebereitschaft erhöhen bzw. fördern kann, sind ebenfalls erforderlich. Es gibt verschiedene Formen des Fragens: ausgedruckter Fragebogen, Interview (persönlich oder per Telefon) und auch Online-Befragungen. Zu berücksichtigen ist, dass man die Befragten auch über die Hintergründe, den Zweck, die Ziele sowie den Nutzen der Umfrage informiert. Dies kann bei schriftlichen Umfragen in Form eines Begleitschreibens und bei persönlichen Befragungen durch einen Hinweis vor dem eigentlichen Gespräch erfolgen. Fragebögen können individuell für die Gruppe der Befragten aufgebaut sein, damit sich die Umfrageteilnehmer auch angesprochen fühlen und an der Umfrage teilnehmen.[70] „Nur mit logisch aufgebauten Fragekomplexen, die auf das spezielle Umfragethema oder Umfrageziel zugeschnitten sind, erhalten Unternehmen auswertbare Ergebnisse.“[71] Der Grundaufbau des Fragebogens besteht aus Einleitungsfragen, danach anschließend die Sachfragen, dann Kontrollfragen und dann Fragen zur Person. Sachfragen beinhalten zustimmende und ablehnende Fragen im Wechsel und auch die Fragetechniken variieren. Die Fragen einer Umfrage sind verständlich und eindeutig zu formulieren, damit es beim Umfrageteilnehmer nicht zu Fehlinterpretationen oder Missverständnissen kommen kann. Die Fragestellungen sollten möglichst so aufgebaut sein, dass die Fragen größtenteils geschlossen formuliert und die Antwortmöglichkeiten vorgegeben werden. Dadurch ist eine leichte computergestützte Auswertung möglich. Jedoch sind allein geschlossene Fragen in einem Fragebogen nur selten sinnvoll. Ideen und Anliegen der Befragten be-

[70] Vgl. www.business-wissen.de (o.J.)
[71] ebd.

kommt man eher durch offene Fragen mitgeteilt, da die Umfrageteilnehmer damit ihre Antworten individuell und ausführlich formulieren können.[72]

Im Rahmen dieser Masterarbeit wurde sich dazu entschieden, eine Onlineumfrage in Form eines im Internet veröffentlichten standardisierten Fragebogens durchzuführen. Die Anzahl an potenziellen Umfrageteilnehmern betrug 419. Alle sächsischen Kommunen wurden über die Durchführung der Umfrage informiert (näheres dazu im vierten Kapitel). Eine Durchführung von persönlichen Interviews wäre zu zeitintensiv gewesen und gemessen am Aufwand muss es nicht zwingend dazu führen, dass es mehr Teilnehmer an der Umfrage gibt als bei der Durchführung einer Online-Befragung mit einem standardisierten Fragebogen. Ebenfalls beinhaltet der Fragebogen Hinweise zu den Hintergründen, den Zweck, die Ziele sowie den Nutzen der Umfrage. Ein Begleitschreiben bzw. ein Einleitungstext vor dem eigentlichen Beginn der Umfrage ist in der ABBILDUNG 11 dargestellt.
Ebenfalls beinhaltet die Umfrage sowohl geschlossene Fragen mit vorgegebenen Antwortmöglichkeiten als auch offene Fragen. Der Umfrageteilnehmer sollte bewusst die Möglichkeit erhalten, gewünschte Unterstützungen bei bestimmten Themen der IS in einer offenen Frage anzugebenen, ohne dass es dafür begrenzte Antwortmöglichkeiten gibt.

Warum ist die Teilnahme an dieser Umfrage wichtig und welchen Nutzen hat sie?

Durch Ihre Teilnahme an der Umfrage können der Freistaat Sachsen, insbesondere das Referat 44 (Informationssicherheit in der Staatsverwaltung, Cybersicherheit) der Sächsischen Staatskanzlei sowie die kommunalen Spitzenverbände einen Überblick darüber erhalten, welche Vorgaben und Orientierungshilfen vom Freistaat Sachsen aus Ihrer Sicht benötigt werden, damit Sie als Kommune unter Berücksichtigung der Kommunalen Selbstverwaltung beim Aufbau bzw. der Weiterentwicklung der Informationssicherheit unterstützt werden können. Im Ergebnis der Umfrage können Maßnahmen zum Schutz der IT in den sächsischen Kommunen ergriffen werden.

[72] Vgl. www.business-wissen.de (o.J.)

Welche Daten werden erhoben?

Im Zuge der Umfrage werden allgemeine Daten (z.B. Einwohnerzahl) sowie Daten der Umfrage zum Thema Informationssicherheit erhoben. Alle Angaben werden vollständig **anonym** behandelt und nur zu statistischen Zwecken ausgewertet. Das heißt, dass keine Daten von Ihnen abgefragt werden, durch die man einen Rückschluss auf Sie als Umfrageteilnehmer vornehmen kann.

Aus Gründen der Lesbarkeit wurden die Fragen in der männlichen Form gestellt, beziehen sich aber auf Angehörige beider Geschlechter.

Abb. 11: Einführungstext Online-Fragebogen
[Quelle : Eigene Darstellung siehe Quelle www.buergerbeteiligung.sachsen.de (2019)]

3.2 Der Forschungsprozess - Die Planungsphase

3.2.1 Die Forschungsfrage

Bei einem Forschungsprojekt besteht zu Beginn die Frage nach dem Thema, welches untersucht werden soll. Dazu muss eine Forschungsfrage aufgestellt werden, die den kompletten Ablauf des Forschungsprojektes beeinflusst. Dies heißt, dass zu Beginn jeder Umfrage eine Forschungsfrage konkretisiert werden soll. Wie auch in dieser Masterarbeit wird im Allgemeinen das Rahmenthema z. Bsp. für eine Auftragsforschung vorgegeben. Trotzdessen sollte eine Forschungsfrage konkretisiert werden, bevor eine Umfrage erstellt wird. Abgeleitet von der Forschungsfrage bestimmen bzw. begründen sich darauf aufbauend auch die Untersuchungsfragen und Untersuchungsdimensionen für die Befragung. Die daraus gewonnenen empirischen Ergebnisse werden vor dem Hintergrund der formulierten Annahme interpretiert.[73] Es empfiehlt sich generell z. Bsp. mittels Brainstorming alles zu dem Thema zu notieren, was einem im Rahmen der Aufstellung der Forschungsfrage einfällt und dieses auch zu ordnen. Dabei gilt es zu beachten, dass die erste Systematisierung des Themas nicht abschließend sein sollte. Durch Vorkenntnisse und eventuelle Vermutungen kann ein Schlagwortkatalog für die anschließende Informationsbeschaffung erstellt werden. Parallel dazu sollte eine Literaturrecherche vorgenommen werden und eine Liste mit wichtigen Literaturdatenbanken und

[73] Vgl. Jacob, R.; Heinz, A.; Décieux, J. P. (2013) S. 58

-informationssystemen erstellt werden. Auch analoge Verzeichnisse wie beispielsweise Fachzeitschriften oder Spezialbibliographien zu bestimmten Themen sollten bei der Literaturrecherche berücksichtigt werden. Bei aktuellen Umfragethemen können auch Berichte aus den Medien verfolgt werden und somit für die Aufstellung einer Forschungsfrage dienlich sein.[74]

Durch die Konkretisierung der zuerst aufgestellten Forschungsfrage dieser Masterarbeit wurde in Abstimmung mit der Staatskanzlei Referat 44 abschließend folgende Forschungsfrage aufgestellt: „Welche Vorgaben und Orientierungshilfen vom Freistaat Sachsen werden aus Sicht der Kommunen benötigt, damit die Kommunen beim Aufbau bzw. der Weiterentwicklung der Informationssicherheit unterstützt werden können?“ Diese Frage ergab sich aus den vorgegebenen Parametern wie beispielsweise „Informationssicherheit bei den Kommunen, Vorgaben zur Umsetzung der Informationssicherheit sowie Orientierungshilfen zum Aufbau und Weiterentwicklung einer Informationssicherheit bei den Kommunen.“ Durch die Aufstellung der Forschungsfrage konnte eine Literaturrecherche durchgeführt und anschließend der erste Entwurf des Fragebogens erstellt werden.

3.2.2 Grundgesamtheit und Stichprobe

„Das Instrument der Umfrageforschung ist ein Instrument der Ermittlung der Meinung von Kollektiven, nicht von einzelnen Personen.“[75] Die Art der Gruppe ergibt sich dabei aus der Forschungsfrage und der Art der Forschung. Zu diesem Zweck wäre es am besten, wenn man alle Mitglieder der jeweiligen Kollektive befragt, welches einer Vollerhebung entspricht. Wenn man an bestimmten Mustern interessiert ist, ist dieses Vorgehen nicht notwendig, da diese Muster durch spezifische Stichprobenuntersuchungen mit hinlänglicher Genauigkeit, jedoch mit weniger Aufwand und geringeren Kosten untersucht werden können. Das Stichproben-Verfahren setzt jedoch voraus, dass man die Grundgesamtheit genau definieren kann. Grundgesamtheit meint eine bestimmte Gruppe, über die man etwas erfahren will. Untersuchungseinheit bezeichnet dabei ausgewählte Elemente dieser Gruppe. Wer zu einer Grundgesamtheit zählen soll und wer nicht, muss vor der Festlegung der Stichprobe geklärt werden. Es gilt jedoch zu berücksichtigen, dass Stichprobenbefragungen nur

[74] Vgl. Jacob, R.; Heinz, A.; Décieux, J. P. (2013) S. 59
[75] Jacob, R.; Heinz, A.; Décieux, J. P. (2013) S. 65

dann auf eine Grundgesamtheit verallgemeinert werden können, wenn sie das Ergebnis einer Zufallsauswahl sind.[76]

Bereits im Rahmen der ersten Überlegungen vor der Erstellung des Fragebogens ergab sich bereits aus der Festlegung des Themas, dass im Rahmen dieser Masterarbeit eine Vollerhebung bei allen sächsischen Kommunen vorgenommen werden sollte.

3.3 Der Forschungsprozess – Die Erhebung der Daten

3.3.1 Befragungsarten

Die Befragungsarten unterscheiden sich zwischen schriftlichen Befragungen und mündlichen Interviews, wobei mündliche Interviews untergliedert werden in persönliche Interviews und Telefoninterviews und schriftliche Befragungen untergliedert werden in postalische Befragungen und Online-Erhebungen.[77]
Aufgrund der großen Anzahl an möglichen Umfrageteilnehmern (siehe Kapitel 4.1) wurde sich dafür entschieden, eine schriftliche Umfrage in Form einer Online-Erhebung durchzuführen. Daher wird im folgenden Absatz auf diese Befragungsart näher eingegangen.
Es stellt sich nachfolgend die Frage, welche Vor- und Nachteile bei der Nutzung dieser Befragungsart auftreten können. Als Vorteile können vor allem der Wegfall der Kosten für Porto und Druck des Fragebogens und Kosten für die Dateneingabe sowie Aufwendungen für die Durchführung von Interviews gesehen werden. Durch die Nutzung des Beteiligungsportals Sachsen (siehe Kapitel 4.2.1) zur Online-Durchführung der Umfrage im Rahmen dieser Masterarbeit sind für die Erstellerin der Masterarbeit keine Kosten für eine Befragungssoftware oder die Nutzung von Servern angefallen, da die Nutzung durch die Staatskanzlei kostenfrei zur Verfügung gestellt wurde. Die Erstellung der Umfrage im Beteiligungsportal Sachsen ist im Vergleich zu einer Erstellung einer Umfrage z. Bsp. als Word-Dokument etwas aufwändiger, jedoch sprechen die übersichtliche Auswertung der eingegangen Umfrageergebnisse insgesamt für die Nutzung des Beteiligungsportals Sachsen. Auch kann durch die Nutzung verschiedener Filter gezielt nach Ergebnissen zu einer be-

[76] Vgl. Jacob, R.; Heinz, A.; Décieux, J. P. (2013) S. 65-66
[77] Vgl. Jacob, R.; Heinz, A.; Décieux, J. P. (2013) S. 98

stimmten Frage gesucht werden. Gleichfalls müssen keine Umfrageergebnisse z. Bsp. zur Auswertung in ein separates Programm übertragen werden.

3.3.2 13 GEBOTE ZUR FORMULIERUNG VON FRAGEN

Zu Beginn dieses Kapitels wird auf die ABBILDUNG 12 verwiesen, die einen Gesamtüberblick über die nachfolgend näher beschriebenen 13 Gebote zur Formulierung von Fragen in einer Umfrage/ einem Umfragebogen geben soll.
Empfehlenswert ist, Fragen einfach und möglichst ohne Fremdwörter zu formulieren. Es sind außerdem keine ungebräuchlichen Fachwörter, Abkürzungen etc. zu verwenden. Damit eine bessere Verständlichkeit der Fragen durch den Umfrageteilnehmer möglich ist, sollten sich die Fragen am allgemeinen Sprachgebrauch orientieren, auch wenn dann bestimmte Sachverhalte nicht im wissenschaftlichen Sinn korrekt beschrieben sind. Es empfiehlt sich nach dem Motto „Eine Befragung sollte nicht der Belehrung der Befragten dienen." vorzugehen. Sätze sind einfach, aber vollständig zu formulieren. Knappe Aufzählungen von Antwortalternativen sind zeitsparend, jedoch für eine angenehme Befragungsatmosphäre nicht zu empfehlen. Reizwörter wie bspw. polarisierende Begriffe sollten vermieden werden. Es ist auf suggestive Formulierungen, bei der der Befragte zu einer bestimmten Antwort genötigt werden könnte, zu verzichten. Ebenfalls ist auch bei Antworten darauf zu achten, dass die verwendeten Antwortkategorien den Befragten nicht zu einer bestimmten Antwort drängen und gleichwertige Antwortkategorien verwendet werden. Als vorteilhaft erweisen sich eindimensionale Fragen, das heißt, dass sich Fragen genau auf einen Aspekt beziehen, da sie ansonsten nicht auswertbar sind. Insofern keine Mehrfachnennungen bei einer Frage möglich sein sollen, der Befragte sich somit genau für eine Alternative zu entscheiden hat, dürfen sich die Antwortmöglichkeiten inhaltlich nicht überschneiden. Verschiedene Antwortmöglichkeiten sind möglichst sinnvoll zusammenzufassen. Es sollte dabei darauf geachtet werden, dass die Zusammenfassungen inhaltlich sinnvoll sind und auch so von dem Befragten aufgenommen bzw. verstanden werden können. Gleichfalls müssen Fragen für den Befragten auch sinnvoll sein. Fragen, die an der Wirklichkeit der Befragten vorbeigehen, sind zu vermeiden, da diese für den Befragten unrealistisch oder unverständlich sein könnten. Wichtig bei der Formulierung von Fragen ist ebenfalls, dass sie beantwortbar sein müssen, da sich der Befragte anderenfalls überfordert fühlen könnte. Auch sollten doppelte Verneinungen vermieden werden. Zwei Behauptungen in einem Statement sind nicht kausal miteinander verknüpft. Dies würde dazu führen, dass der Umfrageteilnehmer nicht nachvollziehen kann, auf welchen Teil der

Gesamtaussage sich die Ablehnung bezieht. Abschließend sei als letztes Gebot der Formulierung von Fragen darauf zu achten, dass mehrdeutige und interpretationsfähige Begriffe (gerade bei offenen Fragen oft ein Problem) vermieden werden, da es sonst dem Befragten überlassen wird, worauf er sich bei seiner Antwort bezieht.[78]

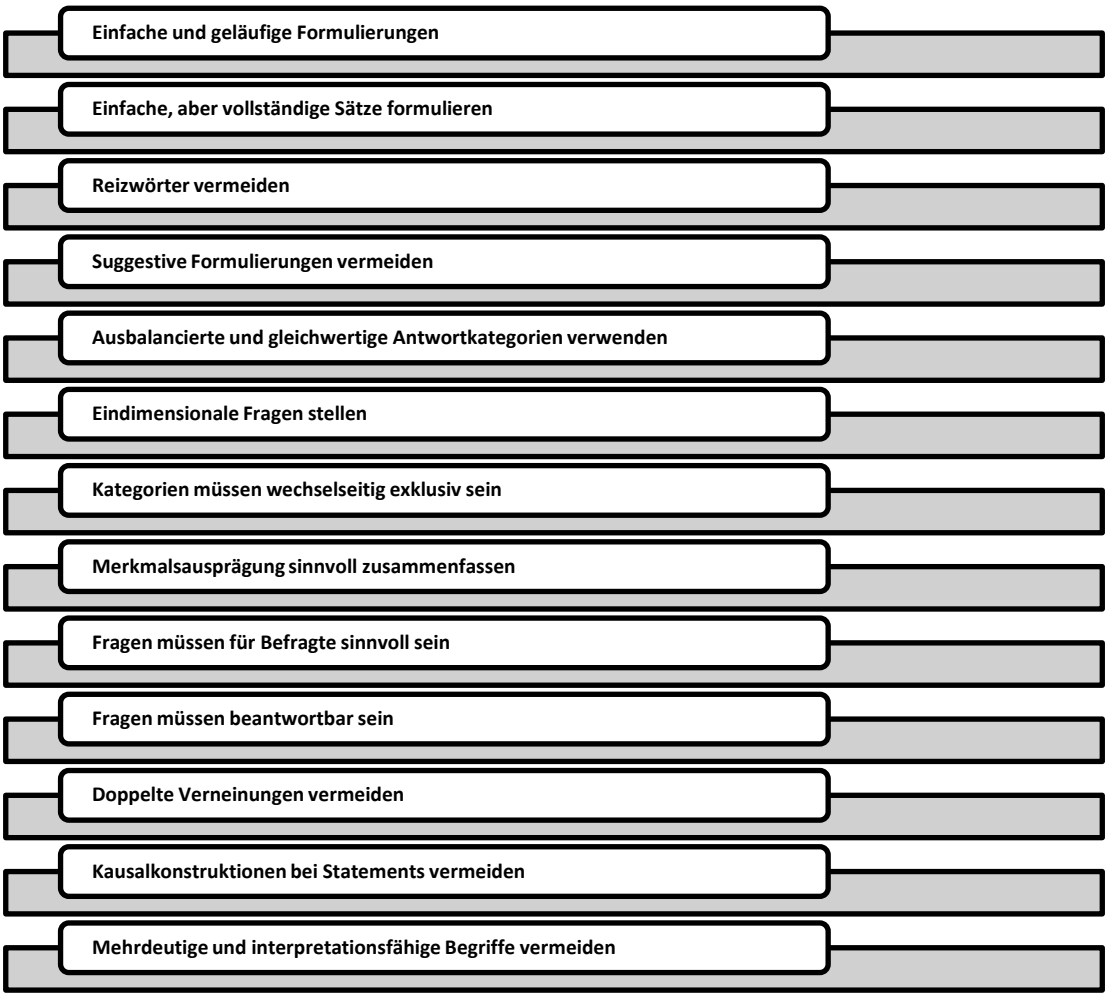


Abb. 12: 13 Gebote zur Formulierung von Fragen
[Quelle : Eigene Darstellung in Anlehnung an Jacob, R.; Heinz, A.; Décieux, J. P. (2013) S. 121-128)]

[78] Vgl. Jacob, R.; Heinz, A.; Décieux, J. P. (2013) S. 121-129

4 BEDARFSANALYSE DER INFORMATIONSSICHERHEIT BEI DEN SÄCHS. KOMMUNEN

Wie bereits im ersten Kapitel dargestellt wurde, soll im Rahmen dieser Abschlussarbeit erörtert werden, welche Vorgaben und Orientierungshilfen vom Freistaat Sachsen aus Sicht der Kommunen zu einem effektiven Aufbau bzw. zu einer Weiterentwicklung der IS benötigt werden. Zu Beginn dieses Kapitels wird die im Rahmen dieser Masterarbeit durchgeführte Umfrage theoretisch betrachtet und beschrieben, welche Phasen eine Umfrage durchläuft. Anschließend wird die Herangehensweise an die Umfrage bei den sächsischen Kommunen erläutert sowie eine Vorstellung der Umfrageteilnehmer vorgenommen. Dabei wird ebenfalls auf den Nutzen der Umfrage näher eingegangen. Weiterführend erfolgt eine Erhebung der Ausgangssituation durch die Befragung der sächsischen Kommunen zum Thema IS auf Basis der Umfrageergebnisse. Dadurch soll die Möglichkeit des Ausbaus der Zusammenarbeit zwischen den sächsischen Kommunen und dem Freistaat Sachsen im Rahmen der IS ermöglicht werden. Schwerpunkt dieses Kapitels ist zusammengefasst die Auswertung der von den Umfrageteilnehmern gewünschten Anwendungspotentiale zum Aufbau und Weiterentwicklung der IS.

4.1 VORSTELLUNG DER UMFRAGETEILNEHMER

Wie bereits in den vorherigen Kapiteln erwähnt, wird mit der Umfrage der Stand der IS bei den sächsischen Kommunen analysiert. Es soll betrachtet werden, welcher Ausbau der Zusammenarbeit zwischen den sächsischen Kommunen und dem Freistaat Sachsen im Rahmen der IS hilfreich wäre. Vor allem durch das Inkrafttreten des SächsISichG, wie bereits in KAPITEL 2.2.1 erwähnt, bestehen auch für die Kommunen gesetzliche Änderungen im Hinblick auf ihre IS.

Der Anwendungsbereich des SächsISichG erstreckt sich auch auf Kommunen, soweit sie an das Sächsische Verwaltungsnetz oder Kommunale Datennetz angeschlossen sind.[79]

Ein weiterer Grund für die Wahl der sächsischen Kommunen als Umfrageteilnehmer ist es, dass die Kommunen bei der Absicherung der Daten der Bürger sowie den Aufbau und Weiterentwicklung ihrer IS vom Freistaat Sachsen unterstützt werden sollen.

[79] Vgl. Sächsisches Informationssicherheitsgesetz (2019) § 2

„Aktuell gibt es im Freistaat Sachsen 419 Gemeinden, davon 416 kreisangehörige Gemeinden und drei Kreisfreie Städte. Nach Angaben des Statistischen Landesamtes haben 45 Gemeinden keine Gemeindeteile, während sich 374 Gemeinden aus 3580 amtlich benannten Gemeindeteilen zusammensetzen. Von den 169 Städten tragen 50 den Titel „Große Kreisstadt“.“[80]

4.2 Herangehensweise zur Erstellung des Fragebogens

4.2.1 Art der Durchführung der Umfrage

Es wurde der effektivste Weg zur Durchführung der Umfrage analysiert. Zwei potenzielle Möglichkeiten wurden näher betrachtet. Zum Einen erschien der Weg des Versands von Umfragebögen im Portable Document Format (nachfolgend kurz PDF-Format) als E-Mail sinnvoll. Der Fragebogen hatte in diesem Format einen Umfang von 17 Seiten. Eine Darstellung des Fragebogens erfolgt in der Anlage 2. Als weitere Möglichkeit ergab sich die Nutzung des Beteiligungsportals des Freistaats. Zwischen diesen beiden Varianten erfolgte eine Abwägung der Vor- und Nachteile, welche vor der Veröffentlichung der Umfrage mit der Staatskanzlei Referat 44 besprochen wurden. Ein großer Vorteil durch die Nutzung bzw. der Durchführung der Umfrage mit einem ausdruckbaren PDF-Dokument liegt dabei in der Übersichtlichkeit. Sollte ein potenzieller Umfrageteilnehmer eher den Fragebogen ausgedruckt durchlesen wollen, ist dies in dieser Variante besser möglich. Ohne bereits in diesem Abschnitt näher auf das Beteiligungsportal Sachsen und deren Möglichkeiten einzugehen (siehe Kapitel 4.2.2), sei hierbei zu erwähnen, dass ein Ausdruck des Fragebogens von dieser Internetseite (Beteiligungsportal) nicht der gleichen Übersichtlichkeit entspricht wie der Ausdruck des in der Anlage 2 dargestellten Fragebogens. Ein wesentlicher Nachteil der Versendung der Umfrage als E-Mail durch das Beifügen des Fragebogens im PDF-Format stellte jedoch der Eingang und die Auswertung der Umfragebögen dar. Der Eingang der Umfragebögen als E-Mail hätte keine Anonymität des Umfrageteilnehmers gewährleisten können. Die Auswertung der eingegangen Umfragebögen würde ebenfalls einen großen Zeitfaktor bedeuten. Gleichfalls könnten es die Teilnehmer an der Umfrage als hinderlich und aufwendig erachten, wenn sie ein 17-seitiges Dokument mit Formularfeldern ausfüllen, speichern und per E-Mail manuell zurücksenden müssten.

[80] www.statistik.sachsen.de (2019)

Die Durchführung der Umfrage mit dem Beteiligungsportal Sachsen wies mehrere Vorteile gegenüber der Versendung der Umfrage als PDF-Dokument auf. Die Umfrageteilnehmer konnten anonym an der Umfrage teilnehmen, welches eine wichtige Restriktion für diese Umfrage war. Ein Rückschluss auf den Umfrageteilnehmer war zu keiner Zeit möglich. Bei einer entsprechend grafischen Gestaltung kann eine Online-Umfrage noch übersichtlicher aufgebaut werden als bei einem PDF-Dokument und der Umfrageteilnehmer muss nicht unbegrenzt weit nach unten scrollen um zum Ende des Fragebogens zu gelangen. Gleichfalls liegt ein Vorteil der Nutzung des Beteiligungsportals auch darin, dass die verschiedenen Fragen in Pflichtfragen und freiwillig zu beantwortende Fragen aufgegliedert werden können. Ebenfalls ist die Auswertung der eingegangen Umfragebögen übersichtlicher und kann somit gerade bei einer größeren Anzahl an beantworteten Umfragebögen strukturierter erfolgen. Dadurch ergibt sich eine Zeitersparnis.
Nach Abwägung der Vor- und Nachteile beider Arten der Durchführung der Umfrage hat sich die Erstellerin der Masterarbeit für die Nutzung des Beteiligungsportals Sachsen entschieden. Die Vorteile einer Online-Umfrage mit dem Beteiligungsportal Sachsen überwiegen.

In Vorbereitung der Umfrage wurden Beratungen zum Einen mit der Staatskanzlei Referat 44 durchgeführt und zum Anderen gab es Abstimmungen mit dem Sächsischen Städte- und Gemeindetag e.V. (nachfolgend kurz SSG) und dem Sächsischen Landkreistag e.V. (nachfolgend kurz LKT). „Der Sächsische Städte- und Gemeindetag ist ein Verband der Städte und Gemeinden des Freistaates Sachsen.“[81] „Der Sächsische Landkreistag hat die Aufgabe, die kommunale Selbstverwaltung zu stärken, Angriffe auf sie abzuwehren und für die Wahrung der verfassungsmäßigen Rechte der Kommunen (Kreisfreie Städte, Landkreise, Gemeinden) einzutreten.“[82]

Eine Mitteilung an die sächsischen Kommunen über die Veröffentlichung und den Inhalt der dieser Masterarbeit zugrundeliegenden Umfrage erfolgte per E-Mail durch die SSG und LKT am 17. Dezember 2019, welches gleichzeitig der Start der Veröffentlichung der Umfrage darstellte. Dazu wurden zum Einen durch den SSG alle Mitglieder im Rahmen eines monatlichen Mitgliederrundschreibens informiert um welches Thema es sich bei der Umfrage handelt und in welchem Zeitraum die Städte und Gemeinden an der Umfrage teilnehmen können. Der LKT informierte seine Mitglieder ebenfalls in Form eines Mitgliederschreibens.

[81] www.ssg-sachsen.de (2014)
[82] www.lkt-sachsen.de (2020)

Am 06.Januar 2020 war es erforderlich, nochmalig alle Kommunen in Sachsen an die Möglichkeit der Teilnahme an der Umfrage zu informieren, da bis zu diesem Zeitpunkt nur fünf Kommunen an der Umfrage teilgenommen hatten. Dies erfolgte per E-Mail durch die Erstellerin dieser Masterarbeit an alle 419 Kommunen in Sachsen entsprechend dem Gemeindeverzeichnis[83] der Landesdirektion Sachsen. Als problematisch stellte sich dabei heraus, dass durch Restriktionen des E-Mail-Providers nicht zeitgleich alle sächsischen Kommunen von einem privaten E-Mail-Account angeschrieben werden konnten. Ebenfalls beinhaltete die von der Landesdirektion Sachsen mit Stichtag 06. Januar 2020 (siehe Quellenangabe www.lds.sachsen.de (2019)) zur Verfügung gestellten Auflistung neun nicht mehr gültige E-Mail-Adressen. Diesen neun Kommunen konnte somit am 06. Januar 2020 keine Erinnerung zur Umfrage per E-Mail zugesendet werden. Nach der Versendung der Erinnerungsnachricht an alle Mitglieder des SSG und LKT durch die Erstellerin der Masterarbeit war ein deutlicher Anstieg der Anzahl an Umfrageteilnehmern innerhalb einer Woche bis zum geplanten Ende der Umfrage am 17. Januar 2020 zu verzeichnen. Aufgrund einiger Anfragen von potenziellen Umfrageteilnehmern zur Teilnahme an der Umfrage nach dem 17. Januar 2020 wurde die Umfrage nochmalig bis zum 22. Januar 2020 verlängert.
Im nun folgenden Abschnitt wird das Beteiligungsportal Sachsen als Medium für die Durchführung der Umfrage näher betrachtet.

4.2.2 BETEILIGUNGSPORTAL SACHSEN

„Der Freistaat Sachsen stellt seinen kommunalen und staatlichen Verwaltungen zentrale Softwarekomponenten zur Umsetzung von E-Government bereit, die aus Wirtschaftlichkeitsgründen nicht mehrfach aufgebaut werden sollen. […] Die E-Government-Basiskomponenten (BaK) stehen den Beschäftigten in der Staatsverwaltung und bereits seit 2011 über die Mitnutzungsvereinbarung (zu ausgewählten BaK) auch in den sächsischen Kommunalverwaltungen zur effizienten elektronischen Aufgabenerfüllung zur Verfügung.“[84]
Das Beteiligungsportal Sachsen kann von allen staatlichen und kommunalen Behörden in Sachsen als E-Government-Basiskomponente genutzt werden. Mit dieser Basiskomponente können Beteiligungsprozesse u.a. in Kommunen online durchgeführt werden. Dabei können staatliche und kommunale Behörden das Portal in eigener Verantwortung nutzen, individuell konfigurieren und somit an ihre Anforderungen

[83] Gemeindeverzeichnis wurde bereitgestellt von der Landesdirektion Sachsen (Quelle: www.lds.sachsen.de (2019))
[84] www.egovernment.sachsen.de (o.J.)

abstimmen bzw. anpassen. Die Nutzung erfolgt dabei z. Bsp. für das Erbringen von Meinungen, Ideen, Vorschlägen und Stellungnahmen zu laufenden Beteiligungsverfahren und ist grundsätzlich für jeden möglich. Folgende vier Beteiligungsverfahren können über das Beteiligungsportal angelegt, durchgeführt und ausgewertet werden: Dialog, Formelle Beteiligungsverfahren, Umfrage, Meldeverfahren.[85] Die ABBILDUNG 13 gibt einen Überblick über diese Beteiligungsverfahren. Da im Rahmen dieser Masterarbeit die Beantwortung von Fragebögen realisiert werden sollte, wurde sich für das Beteiligungsverfahren „Umfrage“ entschieden.

Fragebögen können dabei als Instrument zur Datenerhebung genutzt werden, um z. Bsp. soziale und politische Einstellungen, Meinungen und Interessen zu erfassen. Es gibt verschiedene Arten von Fragetypen wie Offene Fragen, Ja-/Nein-Fragen und auch Matrix-Fragen.[86] Somit kann der Ersteller der Umfrage verschiedene Arten von Antworten (Freitext), vor allem im Hinblick auf die Angabe von eigenen Antworttexten (Offene Fragen), durch den Umfrageteilnehmer erhalten. Dies war bei der Umfrage im Rahmen der Masterarbeit auch aufgrund des Themenschwerpunktes „Informationssicherheit“ wichtig, da ein reines Verwenden von Ja-/Nein-Fragen nicht zielführend gewesen wäre.

[85] Vgl. www.publikationen.sachsen.de (2017 b) S. 5, 13
[86] Vgl. www.publikationen.sachsen.de (2017 b) S. 22 - 23

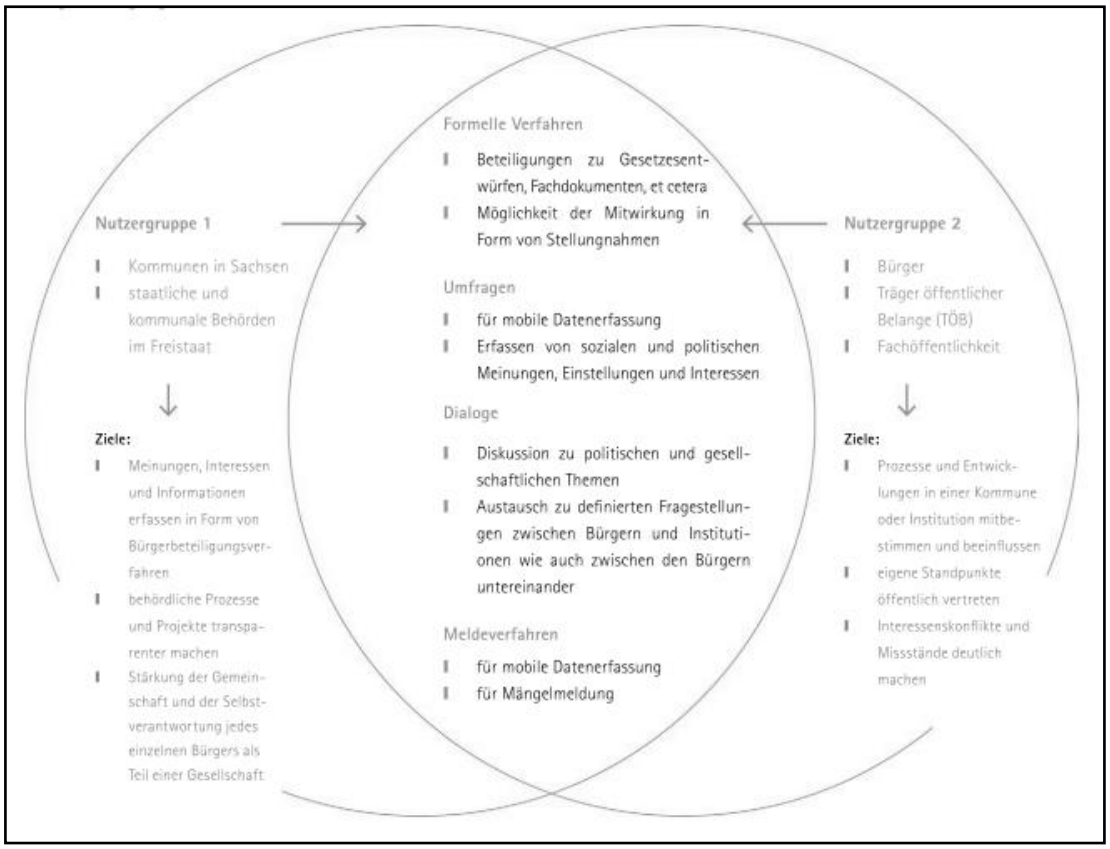


Abb. 13: Übersicht über die Beteiligungsverfahren
[Quelle : www.publikationen.sachsen.de (2017 b) S. 13]

Die ANLAGE 3 beinhaltet den Fragebogen aus dem Beteiligungsportal Sachsen in der Form, wie er im Zeitraum vom 17. Dezember 2019 bis einschließlich 22. Januar 2020 veröffentlicht wurde.[87]

Für die Teilnahme an der Umfrage sollen die Umfrageteilnehmer ca. 10 bis 20 Minuten einplanen. Die Umfrage ist in die drei Bereiche

Teil A - Sachstand Informationssicherheit in sächsischen Kommunen

Teil B - Gewünschte Unterstützung

Teil C - Hemmnisse

gegliedert, wobei durch die thematische Strukturierung bereits mit der Beantwortung des Teil A 80 % der Fragen der Umfrage beantwortet werden.

Im nun folgenden Kapitel wird der Fragebogen mit seinen einzelnen Bereichen näher betrachtet.

[87] Die dieser Masterarbeit zugrundeliegende Umfrage ist unter folgendem Link zu erreichen: https://buergerbeteiligung.sachsen.de/portal/egov/beteiligung/aktuelle-themen/1018996

4.2.3 Ermittlung relevanter Fragen zur Umfrage

In Vorbereitung auf die Veröffentlichung der Umfrage wurden zu Beginn in einer gemeinsamen Beratung mit der Staatskanzlei Referat 44 die Themenschwerpunkte der Umfrage abgestimmt. Dabei sind die bereits vorliegenden Umfrageergebnisse einer Umfrage des Deutschen Landkreistages zur Informationssicherheit in Kreisverwaltungen sowie die Auswertung der genannten Umfrage für die Landkreise des Freistaats Sachsen aus dem Jahr 2018 analysiert worden. Im Ergebnis der Beratungen ist man zu dem Entschluss gekommen, dass mit den vorliegenden Umfrageergebnissen keine Bedarfsanalyse zur Unterstützung des Aufbaus bzw. Weiterentwicklung der IS aller Kommunen des Freistaates Sachsen möglich ist. Der Kreis der Umfrageteilnehmer bezog sich 2018 lediglich auf die Kreisverwaltungen. Mit der aktuellen Umfrage wurden nun auch die Städte und Gemeinden in Sachsen befragt.
Ebenfalls wurden einige Aspekte der damaligen Umfrage vom Deutschen Landkreistag im Rahmen dieser Masterarbeit nochmalig aufgegriffen und z. Bsp. um detailliertere Antwortmöglichkeiten, ergänzende Fragestellungen und Offene Fragen (mit der Möglichkeit des freien Formulierens von Antworten durch den Umfrageteilnehmer) erweitert bzw. angepasst. Somit war der Umfrageteilnehmer nicht verpflichtet, eine der vorgegebenen Antwortmöglichkeiten auszuwählen, sondern sie konnten eigene Antworten formulieren. Auch ist diese Umfrage detaillierter im Hinblick auf die einzelnen Themenschwerpunkte aufgebaut worden, um eine Konzeptentwicklung zum Aufbau und Weiterentwicklung der IS in den sächsischen Kommunen zu ermöglichen.
Die einzelnen Umfragebestandteile wurden nach der Erstellung eines ersten Entwurfs des Fragebogens in einer gemeinsamen Beratung im Dezember 2019 mit dem SSG und dem LKT besprochen. Es wurden sowohl von dem SSG als auch von dem LKT konstruktive Vorschläge zur Anpassung der Umfrage besprochen, die nach Abstimmung mit der Staatskanzlei Referat 44 umgesetzt wurden.
Die Anlage 3 enthält die vollständige Umfrage, wie sie am 17. Dezember 2019 im Beteiligungsportal Sachsen veröffentlichte wurde. Daher erfolgt auf den nachfolgenden Seiten eine ergänzende Erläuterung der gewählten Fragen zu den einzelnen Themen.

Abb. 14: Veröffentlichung der Umfrage im Beteiligungsportal Sachsen
[Quelle : Eigene Darstellung siehe Quelle www.buergerbeteiligung.sachsen.de (2019)]

Die ABBILDUNG 14 zeigt die Veröffentlichungsanzeige der Umfrage im Beteiligungsportal Sachsen.
Im Zuge der Umfrage wurden allgemeine Daten (z.B. Einwohnerzahl) sowie Daten der Umfrage zum Thema IS erhoben. Alle Angaben wurden vollständig anonym behandelt und nur zu statistischen Zwecken ausgewertet. Das heißt, dass keine Daten abgefragt wurden, die einen Rückschluss auf den Umfrageteilnehmer ermöglichen.
Der Umfrageteilnehmer wurde zu Beginn der Umfrage aufgefordert anzugeben, ob es sich bei dem Teilnehmer um einen Landkreis, eine kreisfreie Stadt oder eine Gemeinde handelt. Ebenfalls erfolgte die Abfrage nach der Größe der Kommune (siehe ABBILDUNG 15). Aus Gründen der Lesbarkeit wurden die Fragen in der männlichen Form gestellt.

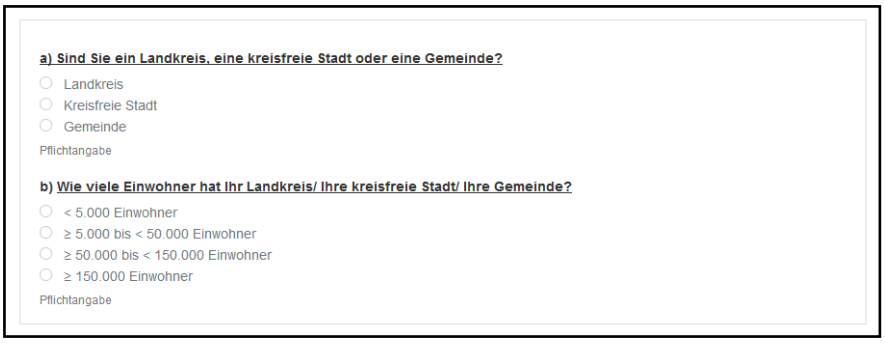


Abb. 15: Umfrage - Eingangsfragestellung
[Quelle : Eigene Darstellung siehe Quelle www.buergerbeteiligung.sachsen.de (2019)]

Wie bereits erwähnt, wurde die Umfrage in drei Bereiche aufgeteilt. Der Teil A - Sachstand Informationssicherheit in sächsischen Kommunen unterteilt sich in 7. Themenschwerpunkte.

Zu Beginn des Teil A erfolgte die Abfrage zum Stand der Benennung eines BfIS. Wie bereits im KAPITEL 2.2.1 detaillierter beschrieben, sollen die Kommunen einen BfIS im Sinne des § 20 SächsISichG bis zum 31. Dezember 2020 benennen. Daher kann die Beantwortung der Frage zur Benennung eines BfIS bereits schon jetzt einen groben Überblick über den aktuellen Stand in den sächsischen Kommunen geben.

Zur Einleitung in den Teil A der Umfrage wurden ebenfalls allgemeine Fragestellungen zur IS in den sächsischen Kommunen gestellt: „Wie viel Budget steht Ihnen pro Jahr für die Informationssicherheit zur Verfügung (Schätzung)?“, „Wie viele Mitarbeiter sind bei Ihnen im Bereich der Informationssicherheit beschäftigt (Angabe Schätzung Stunden pro Jahr)?“ und die Frage nach einer Cyberversicherung. Diese Fragen wurden in gemeinsamen Beratungen mit der Staatskanzlei Referat 44 sowie dem SSG und dem LKT entwickelt. Sie wurden bewusst zu Beginn der Umfrage gestellt, da es sich dabei nicht um Themen handelt, bei denen eine Unterstützung zum Aufbau bzw. Weiterentwicklung der IS durch den Freistaat Sachsen erfolgen soll.

Nach diesem allgemeinen Themenkomplex folgten im Fragebogen sieben Fragestellungen mit verschiedenen Ergänzungsfragen. Bei allen sieben Themenbereichen des Teil A hatte der Umfrageteilnehmer die Möglichkeit, gewünschte Unterstützungen des Freistaates und auch Schwierigkeiten, die z. Bsp. bei der Umsetzung des jeweiligen Themas befürchtet werden oder bestehen, in einem Freitextfeld zu benennen.

Zu Beginn erfolgte die Frage nach dem Vorliegen einer kommunalen Informationssicherheitsleitlinie. „Die Leitlinie zur Informationssicherheit beschreibt allgemein verständlich, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der Institution hergestellt werden soll.“[88]

Folgende Antwortmöglichkeiten (Pflichtangabe) waren möglich: keine Angabe, nicht geplant, geplant, in Vorbereitung und in Kraft getreten. Weiterführend beinhaltete die Umfrage in jeder Frage des Teil A die Möglichkeit, Schwierigkeiten und Unterstützungsmöglichkeiten zum jeweiligen Themengebiet anzugeben (siehe ABBILDUNG 16). Diese Frage (Informationssicherheitsleitlinie) wurde bewusst zu Beginn der Abfrage zum Sachstand der IS gewählt, da diese Richtlinie eine grundlegende Voraus-

[88] www.bsi.bund.de (2017 b) S. 32

setzung für die Ausgestaltung des Informationssicherheitsprozesses darstellt. Im Gegensatz zu den anderen Fragen im Teil A der Umfrage zielt diese Fragestellung jedoch nicht grundsätzlich auf eine mögliche Unterstützung des Freistaates Sachsen bei der Erstellung einer Informationssicherheitsleitlinie für die Kommunen ab. Die Verfügbarkeit von Vorlagen und Muster für Informationssicherheitsleitlinien sind ausreichend im Internet vorhanden. Daher sollte diese Information zum allgemeinen Überblick über den Stand der IS in den sächsischen Kommunen dienen.

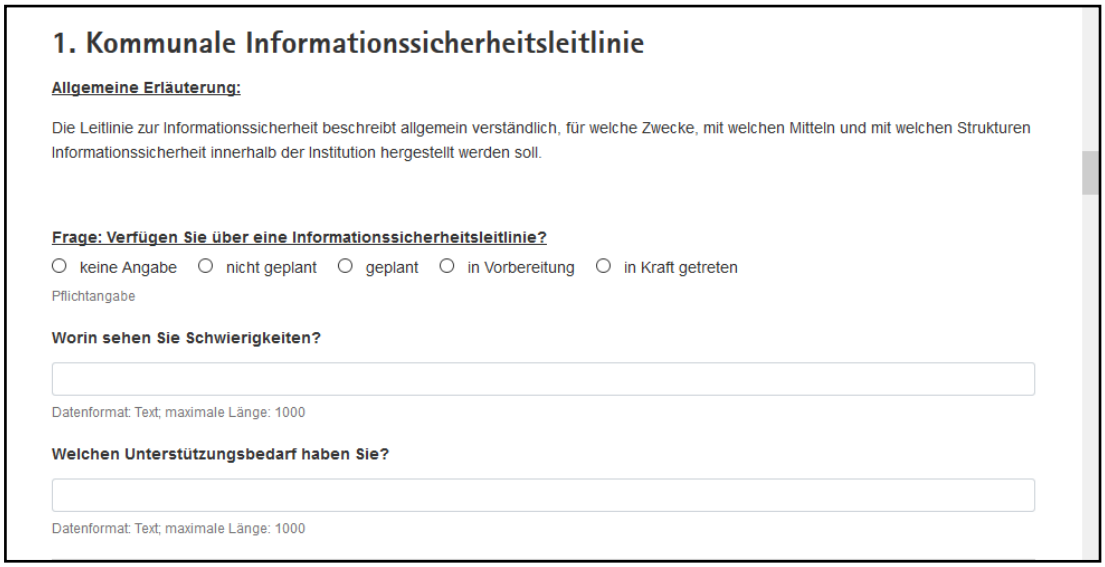


Abb. 16: Umfrage Teil A – Fragestellung Informationssicherheitsleitlinie [Quelle : Eigene Darstellung siehe Quelle www.buergerbeteiligung.sachsen.de (2019)]

Nach der Abfrage zum Vorhandensein einer Informationssicherheitsleitlinie wurde in der Umfrage die Verfügbarkeit eines IT-Sicherheitskonzepts abgefragt. Wie bei der Frage nach der Informationssicherheitsleitlinie waren hier die Antwortmöglichkeiten „keine Angabe, nicht geplant, geplant, in Vorbereitung und in Kraft getreten“ möglich.

Im dritten Themenbereich des Teil A der Umfrage erfolgte im Fragebogen die Abfrage, ob in der jeweiligen sächsischen Kommune ein ISMS etabliert, in Vorbereitung, geplant oder nicht geplant ist. Als ergänzende Fragen wurde nach Abstimmung mit der Staatskanzlei, dem SSG und LKT festgelegt, dass ebenfalls die Abfrage nach der Beteiligung des BfIS an Verwaltungsprojekten und Verwaltungsent-

scheidungen sowie die Durchführung von Sicherheitschecks abgefragt werden sollte.

Auch das Thema der Sicherheitsorganisation war als vierter Themenbereich Bestandteil des Fragebogens. Die Frage nach der Sicherheitsorganisation diente wie auch die einleitenden Fragen zum Beginn der Umfrage zur Schaffung eines Überblickes zum Stand der IS bei den sächsischen Kommunen. Es erfolgte lediglich eine Abfrage der Größe der Sicherheitsorganisation sowie die organisatorische Einordnung des BfIS in die Aufbau- und Ablauforganisation. Eine Unterstützung z. Bsp. in Form von Checklisten oder Mustern durch den Freistaat Sachsen sind bei diesem Thema nicht angedacht.

Der fünfte Themenbereich der Umfrage beinhaltete die Abfrage nach Maßnahmen zur Durchführung von Informations- und Sensibilisierungsveranstaltungen für Mitarbeiter. „Es ist nur dann möglich, Informationssicherheit innerhalb einer Institution erfolgreich und effizient zu verwirklichen, wenn alle Mitarbeiter erkennen und akzeptieren, dass sie ein bedeutender und notwendiger Faktor für den Erfolg der Institution ist und wenn sie bereit sind, Sicherheitsmaßnahmen wirkungsvoll zu unterstützen. Um den Mitarbeitern das nötige Wissen zu vermitteln, sind gleichermaßen Sensibilisierungs- und Schulungsmaßnahmen erforderlich.“[89] Neben der Abfrage, ob in den sächsischen Kommunen Maßnahmen in Form von Informations- und Sensibilisierungsveranstaltungen für die Mitarbeiter regelmäßig oder sporadisch durchgeführt werden oder geplant bzw. nicht geplant sind, hatte der Umfrageteilnehmer ebenfalls die Möglichkeit, bestehende Schwierigkeiten oder Unterstützungsbedarfe anzugeben. Wenn Maßnahmen in Form von Informations- und Sensibilisierungsveranstaltungen geplant sind oder bereits durchgeführt wurden, ist vom Teilnehmer der Umfrage abgefragt worden, welche Zielgruppe (z. Bsp. Behördenleitung, Sachbearbeiter oder andere) soll oder wurde bisher damit angesprochen. Gleichfalls wurde die Bekanntheit verschiedener vom Freistaat Sachsen angebotenen Sensibilisierungsveranstaltungen abgefragt. Folgende Veranstaltungen bzw. die Kenntnis über das bestehende Angebot wurden mit dem Fragebogen abgefragt: E-Learning Angebot „Informationssicherheit am Arbeitsplatz“, Sensibilisierungsveranstaltung „INFOSIC | Die Hacker kommen“ sowie die Sensibilisierungsveranstaltung „INFOSIC plus | IT-Sicherheit für Fortgeschrittene“. Dabei konnte in der Umfrage zu jeder dieser Sensibilisierungsveranstaltungen angeben werden, ob man an dieser Veranstaltung bereits in der Vergangenheit teilgenommen hat oder nicht. Sollte dies

[89] www.bsi.bund.de (o.J.b)

bisher nicht geschehen sein, bestand die Möglichkeit in der Umfrage anzugeben, ob man an dieser Veranstaltung in der Zukunft teilnehmen möchte.
Die Ergebnisse der Frage nach der Bekanntheit und Teilnahme an Sensibilisierungsveranstaltungen gibt Aufschluss darüber, ob die bisherigen Informationen/ Werbungen des Freistaates zum Bestehen dieser Veranstaltungen noch auszuweiten sind oder ob das Interesse an derartigen Veranstaltungen von Seiten der sächsischen Kommunen zu gering ist.

Im sechsten Themenbereich wurde die Identifizierung von kritischen Anwendungen abgefragt. Folgende Antworten waren durch den Umfrageteilnehmer möglich: vollständig abgeschlossen und die Schutzbedarfe hinsichtlich der Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) wurden festgelegt, vollständig abgeschlossen, aber die Schutzbedarfe wurden noch nicht festgelegt, teilweise erfolgt, in Vorbereitung, ist geplant und nicht geplant. Auch hier sollte ermittelt werden, ob die sächsischen Kommunen bei der Identifizierung der kritischen Anwendungen Schwierigkeiten haben oder sehen und ob Unterstützungen vom Freistaat aus ihrer Sicht erforderlich wären.

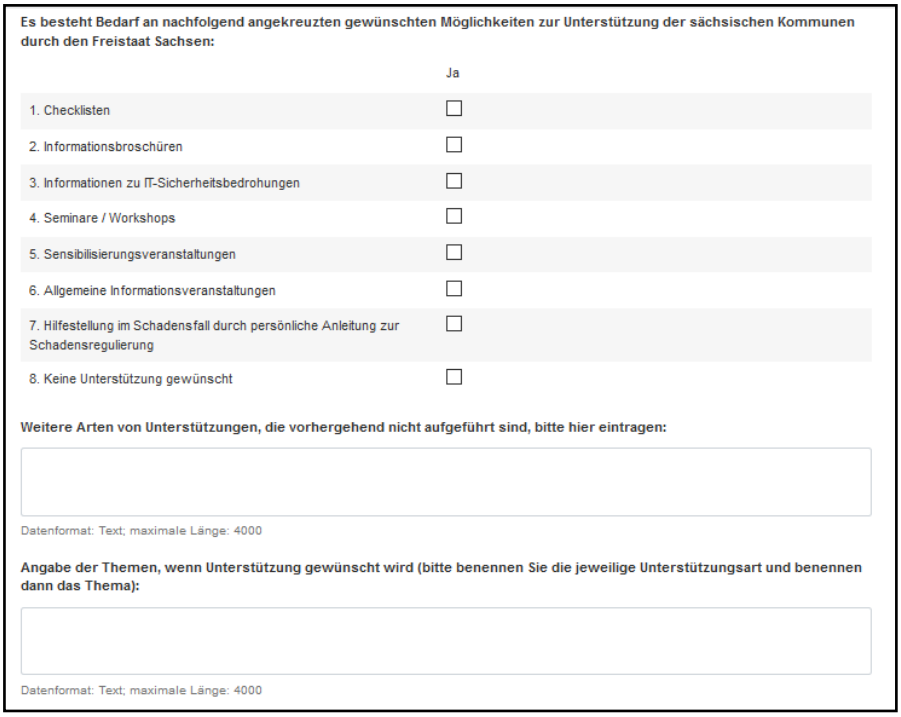
Der letzte Themenbereich des Teil A der Umfrage befasste sich mit den organisatorischen Maßnahmen für IT-Sicherheitsvorfälle. „Neben technischen Sicherheitsmaßnahmen müssen auch organisatorische Abläufe und Prozesse (wie Benutzerrichtlinien, Rechtevergaben, Sicherheitsschulungen, Test- und Freigabeverfahren) eingerichtet werden.“[90] Neben der Frage, ob organisatorische Maßnahmen für IT-Sicherheitsvorfälle bisher festgelegt wurden, sollte der Umfrageteilnehmer die Ergänzungsfrage nach dem Vorliegen von vorgeschriebenen Abläufen bei IT-Sicherheitsvorfällen, z. Bsp. durch einen Angriff auf ihre IT durch Schadsoftware, beantworten. Abschließend erfolgte die Abfrage, ob in der Vergangenheit schon einmal ein IT-Sicherheitsvorfall dem SAX.CERT gemeldet wurde.

Der Teil B der Umfrage befasste sich allgemein mit den gewünschten Unterstützungen im Rahmen der gesamten Betrachtung der IS in den sächsischen Kommunen. In diesem Abschnitt der Umfrage erhielt man die Möglichkeit, dem Referat 44 der Staatskanzlei sowie den kommunalen Spitzenverbänden einen Überblick darüber zu geben, welche Unterstützung sie sich zum Aufbau und zur Weiterentwicklung der IS vorstellen könnten bzw. ihnen hilfreich wären. Mehrfachnennungen waren möglich. Die Übersicht (siehe ABBILDUNG 17) war nicht abschließend. Daher konnte der Um-

[90] www.bsi.bund.de (2017 a) S. 34

frageteilnehmer auch Freitextfelder am Ende dieses Abschnittes der Umfrage nutzen. Mit dieser Fragestellung wurden allgemein gewünschte Unterstützungsmöglichkeiten wie Checklisten, Seminare, Workshops, Sensibilisierungsveranstaltungen etc. abgefragt, die keiner der sieben Themenbereiche im Teil A der Umfrage direkt zugeordnet werden konnten.

Teil C der Umfrage beschäftigte sich mit Hemmnissen, die die Teilnehmer im Aufbau einer systematischen IS sehen. Mehrfachnennungen waren auch hier möglich. Die Übersicht (siehe ABBILDUNG 18) war nicht abschließend. Daher konnte der Umfrageteilnehmer auch hier Freitextfelder am Ende dieses Abschnittes der Umfrage nutzen. Auch die Abfrage der Hemmnisse ist für eine Unterstützung zum Aufbau bzw. Weiterentwicklung der IS in den sächsischen Kommune wichtig, damit später geleistete Unterstützungen ihr Ziel nicht verfehlen und die Hemmnisse in der Zukunft zumindest gemindert werden können.



Es besteht Bedarf an nachfolgend angekreuzten gewünschten Möglichkeiten zur Unterstützung der sächsischen Kommunen durch den Freistaat Sachsen:

	Ja
1. Checklisten	☐
2. Informationsbroschüren	☐
3. Informationen zu IT-Sicherheitsbedrohungen	☐
4. Seminare / Workshops	☐
5. Sensibilisierungsveranstaltungen	☐
6. Allgemeine Informationsveranstaltungen	☐
7. Hilfestellung im Schadensfall durch persönliche Anleitung zur Schadensregulierung	☐
8. Keine Unterstützung gewünscht	☐

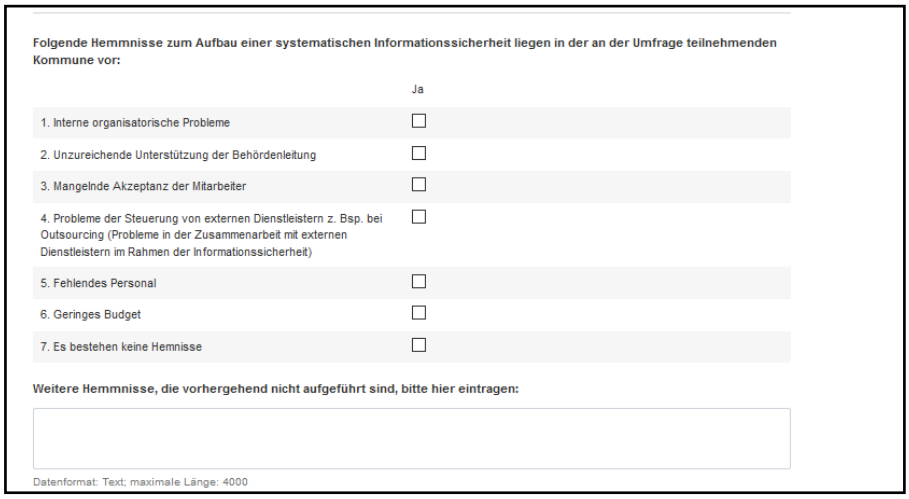
Weitere Arten von Unterstützungen, die vorhergehend nicht aufgeführt sind, bitte hier eintragen:

Datenformat: Text; maximale Länge: 4000

Angabe der Themen, wenn Unterstützung gewünscht wird (bitte benennen Sie die jeweilige Unterstützungsart und benennen dann das Thema):

Datenformat: Text; maximale Länge: 4000

Abb. 17: Umfrage Teil B – Gewünschte Unterstützung
[Quelle : Eigene Darstellung siehe Quelle www.buergerbeteiligung.sachsen.de (2019)]



Folgende Hemmnisse zum Aufbau einer systematischen Informationssicherheit liegen in der an der Umfrage teilnehmenden Kommune vor:

	Ja
1. Interne organisatorische Probleme	☐
2. Unzureichende Unterstützung der Behördenleitung	☐
3. Mangelnde Akzeptanz der Mitarbeiter	☐
4. Probleme der Steuerung von externen Dienstleistern z. Bsp. bei Outsourcing (Probleme in der Zusammenarbeit mit externen Dienstleistern im Rahmen der Informationssicherheit)	☐
5. Fehlendes Personal	☐
6. Geringes Budget	☐
7. Es bestehen keine Hemnisse	☐

Weitere Hemmnisse, die vorhergehend nicht aufgeführt sind, bitte hier eintragen:

Datenformat: Text; maximale Länge: 4000

Abb. 18: Umfrage Teil C – Hemmnisse
[Quelle : Eigene Darstellung siehe Quelle www.buergerbeteiligung.sachsen.de (2019)]

4.3 Darstellung der Umfrageergebnisse

In den nachfolgenden vier Unterkapiteln werden die Umfrageergebnisse, unterteilt in Teil A bis C, analysiert und ausgewählte Ergebnisse durch Diagramme grafisch dargestellt. Eine komplette Übersicht der Ergebnisse der Umfrage ist in der Anlage 4 tabellarisch dargestellt. Auf die Abbildung einzelner beantworteter Fragebögen wird daher verzichtet. Im Umfragezeitraum vom 17. Dezember 2019 bis einschließlich 22. Januar 2020 sind insgesamt 32 Fragebögen von den sächsischen Kommunen ausgefüllt worden. Wie bereits im Kapitel 4.2 erwähnt, wurden zur Einleitung in die Umfrage allgemeine Fragen zum Umfrageteilnehmer gestellt.

4.3.1 Allgemeine Fragen und Ergebnisse

Zu Beginn erfolgte eine Abfrage, ob die Beantwortung der Umfrage aus der Sicht eines Landkreises, einer kreisfreien Stadt oder einer Gemeinde erfolgt (Pflichtangabe). Die Umfrage ergab, dass mit 78,1 % die meisten Umfrageteilnehmer Gemeinden waren (25 Teilnehmer). Ebenfalls haben sieben Landkreise an der Umfrage teilgenommen. Von den drei kreisfreien Städten in Sachsen gab es keine Teilnahme an der Umfrage (siehe Abbildung 19).

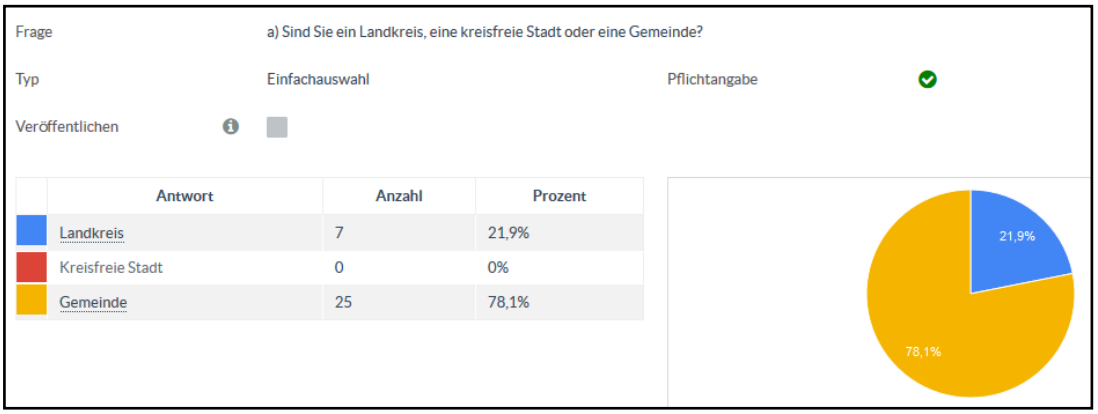


Abb. 19: Umfrage – Antwort einleitende Frage zur Kommune
[Quelle : Passwortgeschütztes Auswertungstool Bürgerbeteiligung Sachsen siehe www.buergerbeteiligung.sachsen.de (2019)]

Es erfolgte anschließend die Abfrage nach der Anzahl der Einwohner der jeweiligen Kommune. Antwortmöglichkeiten wurden in vier Skalen eingeteilt. Die ABBILDUNG 20 gibt einen Überblick über die eingegangen Antworten.

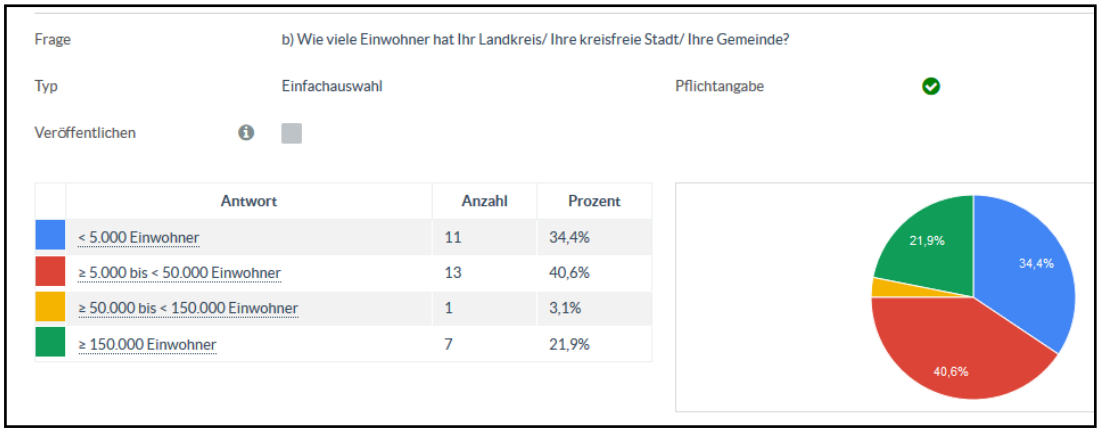


Abb. 20: Umfrage – Antwort einleitende Frage nach der Anzahl der Einwohner
[Quelle : Passwortgeschütztes Auswertungstool Bürgerbeteiligung Sachsen siehe www.buergerbeteiligung.sachsen.de (2019)]

50 % der Umfrageteilnehmer gaben bei der nachfolgende Frage (Pflichtangabe) nach dem aktuellen Stand der Benennung eines BfIS an, dass sie einen BfIS benannt haben. 50 % der Teilnehmer hatten bis zum Tag der Teilnahme an der Umfrage keinen BfIS in ihrer Kommune benannt. Die Auswertung ergab ebenfalls, dass

von den 16 Kommunen, die einen BfIS benannt haben, sieben Kommunen mehr als 150.000 Einwohner, sechs Kommunen zwischen 5.000 und 50.000 Einwohner und drei Kommunen weniger als 5.000 Einwohner haben.
Von den 16 Kommunen, die bisher keinen BfIS benannt haben, haben acht Kommunen weniger als 5.000 Einwohner. Sieben Kommunen haben 5.000 bis 50.000 Einwohner und eine Kommune zwischen 50.000 und 150.000 Einwohner.

Im Anschluss an diese Fragen erfolgte die Abfrage nach dem Budget, welches pro Jahr für die IS zur Verfügung steht (freiwillige Angabe). Acht Kommunen haben diese Frage nicht beantwortet. Sechs Kommunen gaben an, dass ihnen kein Budget für die IS zur Verfügung steht. Acht Kommunen steht ein Budget zwischen 100 Euro und 3.000 Euro pro Jahr für die IS zur Verfügung. Zehn Kommunen haben pro Jahr ein Budget zwischen 5.000 Euro und 25.000 Euro.
Nachfolgend konnten die Umfrageteilnehmer im Fragebogen angeben (freiwillige Angabe), wie viele Mitarbeiter bei ihnen im Bereich der IS beschäftigt sind. Zu Beginn sei angemerkt, dass man auf Basis der Umfrageergebnisse vermuten kann, dass die Frage eventuell von den Umfrageteilnehmern anders interpretiert wurde als ursprünglich gedacht und somit die Ergebnisse dieser Frage im weiteren Verlauf nicht weiter analysiert werden können. Es liegen große Unterschiede bei den getätigten Angaben vor. Fünf Kommunen gaben an, dass im Bereich der IS keine Mitarbeiter beschäftigt sind. Ebenfalls fünf Kommunen machten keine Angaben. Die übrigen Kommunen gaben an, dass mit dem Thema IS zwischen einem und 3000 Beschäftigen befasst sind.

Den allgemeinen Fragenteil abschließend erfolgte eine Frage nach dem Bestehen einer Cyberversicherung (Pflichtangabe). Neun Kommunen verfügen über eine Cyberversicherung. Von diesen Kommunen haben sechs Kommunen zwischen 5.000 und 50.000 Einwohner und drei Kommunen weniger als 5.000 Einwohner.
Keine Cyberversicherung haben von den Umfrageteilnehmern 22 Kommunen. Davon haben acht Kommunen weniger als 5.000 Einwohner, sieben Kommunen haben zwischen 5.000 und 50.000 Einwohner, eine Kommune zwischen 50.000 und 150.000 Einwohner und sechs Kommunen haben mehr als 150.000 Einwohner. Eine Kommune machte keine Angabe.

Im nun folgenden Unterkapitel werden die sieben Fragen aus der Umfrage Teil A mit den jeweiligen Ergebnissen dargestellt. Damit eine Übersichtlichkeit und klare Trennung der Fragen vorgenommen werden kann, wird zu Beginn die jeweilige Frage aus der Umfrage wortwörtlich übernommen.

4.3.2 Ergebnisse Umfrage Teil A

1. Frage: Verfügen Sie über eine Informationssicherheitsleitlinie?

Bei 15 Umfrageteilnehmern ist eine Informationssicherheitsleitlinie in Kraft getreten. Dies entspricht 46,9 % der an der Umfrage teilgenommenen Kommunen (siehe Abbildung 21).

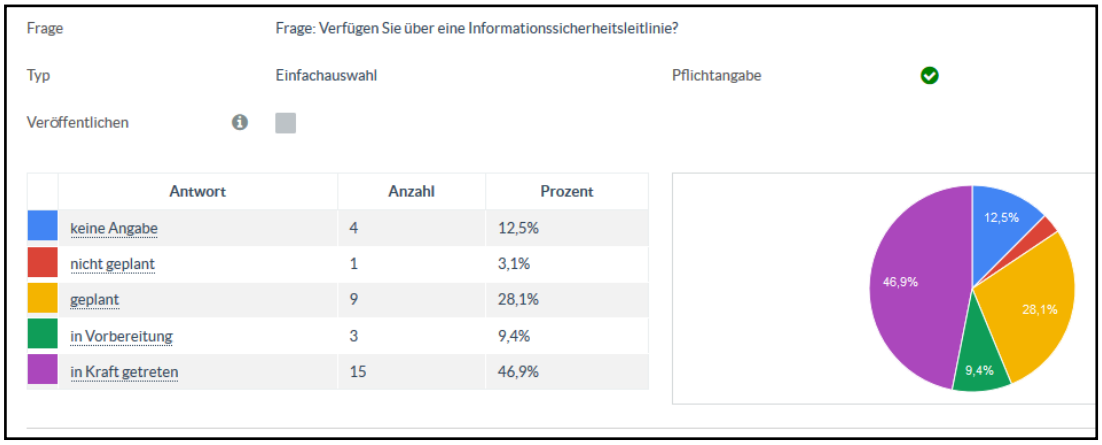


Abb. 21: Umfrage – 1. Frage des Teil A
[Quelle : Passwortgeschütztes Auswertungstool Bürgerbeteiligung Sachsen siehe www.buergerbeteiligung.sachsen.de (2019)]

Im Rahmen einer offenen Frage konnten die Umfrageteilnehmer für sie bestehende Schwierigkeiten zum Thema „Informationssicherheitsleitlinie“ angeben. Diese Möglichkeit haben 18 Kommunen genutzt. Kommunen gaben an, dass zu wenig Know-how vor Ort besteht und die finanziellen Mittel nicht ausreichen würden. Ebenfalls gibt es zu wenig Informationsfluss von oben nach unten. Weitere Schwierigkeiten sehen die Teilnehmer darin, dass die Informationssicherheitsleitlinie von wenigen gelesen, verstanden oder im „Tagesgeschäft“ umgesetzt wird. Beschäftigte würden diese Leitlinie lediglich als „Geschäftsanweisung“ für die IT-Abteilung betrachten. Gleichfalls fehle Fachpersonal. Der Zeitfaktor und bürokratische Hürden spielen für die Kommunen bei der Umsetzung dieser Leitlinie ebenfalls eine entscheidende Rolle. Problematisch ist für die Kommunen auch die korrekte fachliche Formulierung einer Informationssicherheitsleitlinie. Weiterhin ständen für dieses Thema keine Mitarbeiter zur Verfügung bzw. die notwendigen Qualifikationen würden fehlen. Für eine Kommune war der Begriff „Informationssicherheitsleitlinie“ nicht bekannt, jedoch soll das Thema in der Kommune aufgegriffen werden.

Acht Kommunen machten keine Angaben zu bestehenden Schwierigkeiten.
Der Großteil der Umfrageteilnehmer sah Probleme in den Bereichen Budget, fehlendes Personal, Fachwissen bzw. Qualifikation, zeitlicher Aufwand und Durchsetzung der Regelungen der Informationssicherheitsleitlinie.
Von den 18 Kommunen, die Schwierigkeiten im Rahmen der Informationssicherheitsleitlinie sehen bzw. benannt haben, haben neun Kommunen weniger als 5.000 Einwohner, sieben Kommunen haben zwischen 5.000 und 50.000 Einwohner, eine Kommune hat zwischen 50.000 und 150.000 Einwohner und eine weitere Kommune hat mehr als 150.000 Einwohner.
Sechs Kommunen, welche bereits eine Informationssicherheitsleitlinie haben, geben an, dass die bestehende Leitlinie nicht mehr den aktuellen Gegebenheiten bzw. gesetzlichen Regelungen der IS entspreche.
Bei den in Vorbereitung befindlichen Informationssicherheitsleitlinien bestehen Probleme durch fehlendes Know-how, finanzielle Mittel und auch der Zeitfaktor wurde benannt. Kommunen, die eine Leitlinie planen, sehen größtenteils Schwierigkeiten beim Fachwissen zu diesem Thema.

16 Umfrageteilnehmer machten folgende Angaben zum gewünschten Unterstützungsbedarf (offene Frage):

- Grundkonzepte zur Verfügung stellen
- konkrete Ansprechpartner beim Land benennen
- Benennung der Inhalte, die zu diesem Thema wichtig sind
- Informationen an Bürgermeister für besseres Verständnis und dadurch größere Unterstützung
- Sensibilisierung der Führungskräfte
- Checklisten zur Verfügung stellen
- ausreichende Finanzausstattung der Kommunen allgemein
- Unterstützung monetärer Art, um Dienstleister für die Aufgaben hinzuziehen zu können
- Mustertexte bzw. Handreichungen zur Verfügung stellen
- Musterleitlinie zur Verfügung stellen
- Kommunale Schulungen bzw. Beratungen zum Thema durch den Freistaat

2. Frage: Verfügen Sie über ein IT-Sicherheitskonzept?

Bei acht Umfrageteilnehmern liegt ein IT-Sicherheitskonzept vor. Dies entspricht 25 % der an der Umfrage teilgenommenen Kommunen (siehe ABBILDUNG 22). Der Großteil hat die Erstellung eines IT-Sicherheitskonzepts geplant bzw. in Vorbereitung (17 Kommunen).

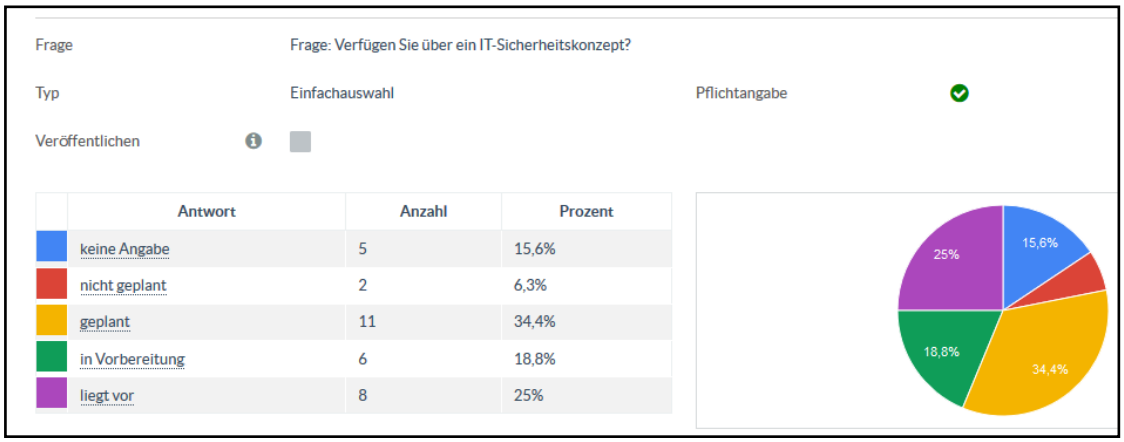


Abb. 22: Umfrage – 2. Frage des Teil A
[Quelle : Passwortgeschütztes Auswertungstool Bürgerbeteiligung Sachsen siehe www.buergerbeteiligung.sachsen.de (2019)]

Im Rahmen einer offenen Frage konnten die Umfrageteilnehmer für sie bestehende Schwierigkeiten zum Thema IT-Sicherheitskonzept angeben. Diese Möglichkeit haben 20 Kommunen genutzt. Kommunen gaben an, dass zu wenig Know-how vor Ort besteht und die finanziellen Mittel nicht ausreichen würden. Ebenfalls gibt es zu wenig Informationsfluss von oben nach unten. Ein weiteres Problem liegt in der Unvollständigkeit des vorliegenden IT-Sicherheitskonzepts. Auch die Ermittlung der Schutzbedarfe wird bei der Planung eines IT-Sicherheitskonzepts als schwierig erachtet. Es würden die personellen und zeitlichen Kapazitäten für diese Aufgaben nicht genügen und grundsätzliche Schwierigkeiten bei der Erstellung und Umsetzung des IT-Sicherheitskonzepts bestehen.
Zwölf Kommunen machten keine Angaben. Der Großteil der Umfrageteilnehmer sah Herausforderungen in den Bereichen Budget, fehlendes Personal, Fachwissen bzw. Qualifikation und dem zeitlichen Aufwand zur Erstellung eines IT-Sicherheitskonzepts.
Von den 20 Kommunen, die Schwierigkeiten im Rahmen der Erstellung eines IT-Sicherheitskonzepts sehen bzw. benannt haben, haben acht Kommunen weniger

als 5.000 Einwohner, sieben Kommunen haben zwischen 5.000 und 50.000 Einwohner, eine Kommune hat zwischen 50.000 und 150.000 Einwohner und vier Kommunen haben mehr als 150.000 Einwohner.
Vier Kommunen, bei denen ein IT-Sicherheitskonzept vorliegt, sehen ungeachtet davon Schwierigkeiten im Hinblick auf die Aktualität und die Vollständigkeit des bestehenden IT-Sicherheitskonzepts.

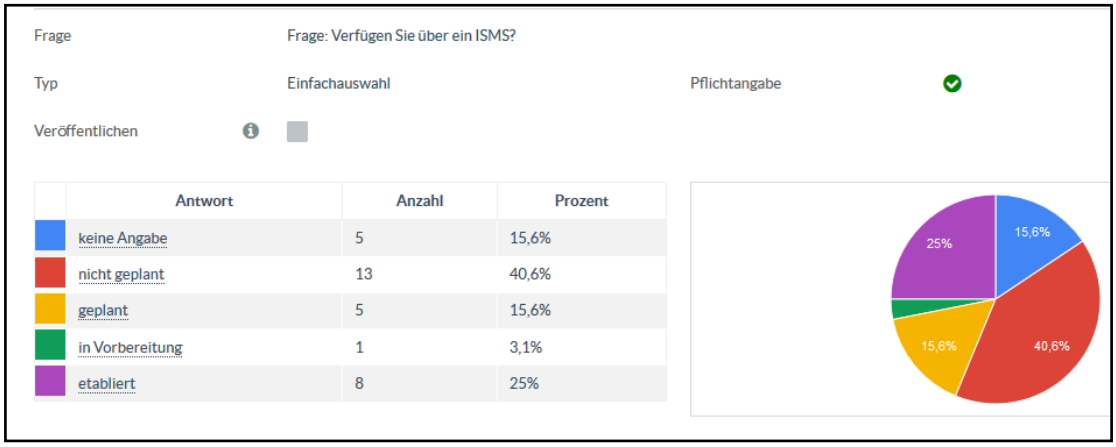
16 Umfrageteilnehmer machten folgende Angaben zum gewünschten Unterstützungsbedarf (offene Frage):

- Grundkonzepte zur Verfügung stellen
- konkrete Ansprechpartner beim Land benennen
- Benennung der Inhalte, die zu diesem Thema wichtig sind
- Informationen an Bürgermeister für besseres Verständnis und dadurch größere Unterstützung
- begrenzte Beteiligungen am Sicherheitskonzept durch starke Belastung der Fachabteilungen
- Kooperationen innerhalb der sächsischen Kommunen
- Mustertexte bzw. Handreichungen zur Verfügung stellen
- personelle und finanzielle Ressourcen bereitstellen
- Vermittlung von Know-how
- vor-Ort-Unterstützung durch Experten

Bei der ergänzenden Frage „Halten Sie es für möglich mit einem Muster eines IT-Sicherheitskonzepts zu arbeiten?“ (Pflichtangabe) haben 24 Kommunen mit JA, fünf Kommunen mit NEIN und drei Kommunen keine Angaben getätigt.

3. Frage: Verfügen Sie über ein ISMS?

Bei acht Umfrageteilnehmern ist ein ISMS etabliert. Dies entspricht 25 % der an der Umfrage teilgenommenen Kommunen (siehe ABBILDUNG 23). Der Großteil der Kommunen hat die Etablierung eines ISMS nicht geplant (13 Kommunen).



Antwort	Anzahl	Prozent
keine Angabe	5	15,6%
nicht geplant	13	40,6%
geplant	5	15,6%
in Vorbereitung	1	3,1%
etabliert	8	25%

Abb. 23: Umfrage – 3. Frage des Teil A
[Quelle : Passwortgeschütztes Auswertungstool Bürgerbeteiligung Sachsen siehe www.buergerbeteiligung.sachsen.de (2019)]

Im Rahmen einer offenen Frage konnten die Umfrageteilnehmer für sie bestehende Schwierigkeiten zum Thema ISMS angeben. Diese Möglichkeit haben 13 Kommunen genutzt. Wie auch zuvor gaben Kommunen an, dass zu wenig Know-how vor Ort bestände und die finanziellen Mittel nicht ausreichen würden, wodurch externe Firmen mit der Aufgabe nicht beauftragt werden können. Weiterhin wurde festgestellt, dass diese Aufgabe bisher nicht als Aufgabe der Führungsebene erkannt worden ist. Auch würden die personellen und zeitlichen Kapazitäten für diese Aufgaben nicht genügen und es existieren grundsätzlich Probleme bei der Erstellung, Umsetzung und dem Betrieb eines ISMS.
19 Kommunen machten keine Angaben zu bestehenden Schwierigkeiten bzw. sahen keine Schwierigkeiten.
Der Großteil der Umfrageteilnehmer sah erneut Schwierigkeiten in den Bereichen Budget, fehlendes Personal, Fachwissen bzw. Qualifikation und dem zeitlichen Aufwand zur Erstellung eines ISMS.
Von den 13 Kommunen, die Schwierigkeiten im Rahmen eines ISMS sehen bzw. benannt haben, haben sechs Kommunen weniger als 5.000 Einwohner, vier Kommunen haben zwischen 5.000 und 50.000 Einwohner, eine Kommune hat zwischen

50.000 und 150.000 Einwohner und zwei Kommunen haben mehr als 150.000 Einwohner.
Die Angaben zum gewünschten Unterstützungsbedarf (offene Frage) sind identisch mit denen der vorhergehenden Frage zum IT-Sicherheitskonzept.

Folgende spezifische Fragestellungen wurden den Umfrageteilnehmern ergänzend gestellt:

„1. Wird bei Ihnen der BfIS an Verwaltungsprojekten und Verwaltungsentscheidungen beteiligt?“

Die Ergebnisse dieser Frage sind in der ABBILDUNG 24 dargestellt. Der Großteil der Umfrageteilnehmer, der bisher einen BfIS benannt hat, gab an, dass dieser an Verwaltungsprojekten und Verwaltungsentscheidungen sporadisch beteiligt wird.

Teilfrage 1 — 1. Wird bei Ihnen der BfIS an Verwaltungsprojekten und Verwaltungsentscheidungen beteiligt?

Antwort	Anzahl	Prozent
systematisch beteiligt	5	15,6%
sporadisch beteiligt	10	31,3%
keine Beteiligung	1	3,1%
bisher kein BfIS ernannt	9	28,1%
keine Angabe	7	21,9%

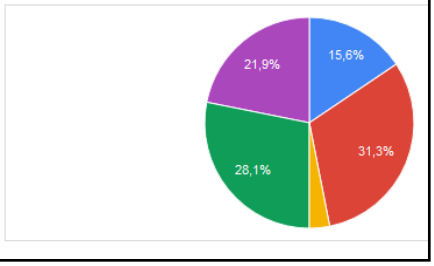


Abb. 24: Umfrage – 3. Frage des Teil A – Teilfrage 1
[Quelle : Passwortgeschütztes Auswertungstool Bürgerbeteiligung Sachsen siehe www.buergerbeteiligung.sachsen.de (2019)]

„2. Werden bei Ihnen Sicherheitschecks (Bsp.: IT-Sicherheits-Quick-Check für kleine Kommunalverwaltungen) zur Beurteilung der Informationssicherheit durchgeführt?“

Die Ergebnisse dieser Frage sind in der ABBILDUNG 25 dargestellt. 17 der 32 Kommunen, die an der Umfrage teilnahmen, haben bisher keine Sicherheitschecks durchgeführt.

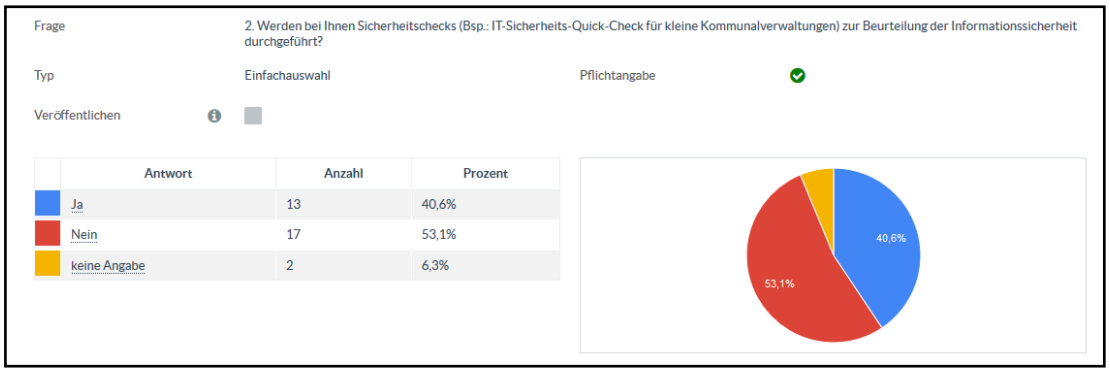


Abb. 25: Umfrage – 3. Frage des Teil A – Teilfrage 2
[Quelle : Passwortgeschütztes Auswertungstool Bürgerbeteiligung Sachsen siehe www.buergerbeteiligung.sachsen.de (2019)]

Wurde diese zweite Teilfrage mit JA beantwortet, gab es die Möglichkeit durch eine offene Frage anzugeben, in welchem Umfang bei ihnen Sicherheitschecks durchgeführt (kurze Beschreibung der Maßnahme) werden.
Von den 13 Kommunen, die diese Frage beantwortet haben, sind folgende Angaben gemacht worden:

- interne Revisionen zur Prüfung der Umsetzung des IT-Grundschutz
- Grundschutz-Check
- IS-Kurzrevision/ Zertifizierungsaudit im Fachbereich
- Kurzaudits im Rahmen EU-Zahlstellentätigkeit, beschränkt auf ausgewählte Bausteine
- sporadisch und nach Neuerungen
- Computerfirma (Dritter) prüft aktuelle Software
- Basis-Sicherheitscheck, externe Audits EU-Zahlstelle
- durch den IT-Sicherheitsbeauftragten mittels Kontrollsoftware

Ebenfalls konnte von den Umfrageteilnehmern im Rahmen einer offenen Frage angegeben werden, mit welcher Häufigkeit/ Regelmäßigkeit Sicherheitschecks durchgeführt werden. Die nachfolgende Aufzählung gibt die Spanne der Antworten an:

- nicht regelmäßig, sondern Fallabhängig
- bei Verfahrensänderungen, zyklisch, bei Veränderungen des Standes der Technik, etc.
- jeweils ca. alle 3 Jahre
- Abstand 3-4 Jahre

- sporadisch
- ca. aller 3-4 Monate
- aller 2 Jahre
- einmalig

4. Frage: Wie groß ist Ihre Sicherheitsorganisation und wie ist die organisatorische Ansiedlung des Beauftragten für Informationssicherheit (BfIS) geregelt?

Die Angaben zur Größe der Sicherheitsorganisation sind sehr unterschiedlich. Elf Kommunen antworteten, dass sie keine Beschäftigten innerhalb einer Sicherheitsorganisation haben.17 Kommunen gaben an, dass ihre Sicherheitsorganisation aus einer bis zu 50 Beschäftigten besteht. Bei vier Kommunen besteht die Sicherheitsorganisation aus 140 Beschäftigten bis 220 Beschäftigten.
Von den elf Kommunen, die keine Beschäftigten innerhalb einer Sicherheitsorganisation haben, haben drei Kommunen weniger als 5.000 Einwohner, sechs Kommunen haben zwischen 5.000 und 50.000 Einwohner, eine Kommune hat zwischen 50.000 und 150.000 Einwohner und eine weitere Kommune hat mehr als 150.000 Einwohner.
Von den 17 Kommunen, die zwischen einer und 50 Beschäftigten innerhalb einer Sicherheitsorganisation haben, haben acht Kommunen weniger als 5.000 Einwohner, vier Kommunen haben zwischen 5.000 und 50.000 Einwohner und fünf Kommunen haben mehr als 150.000 Einwohner.

Die Frage nach der Einordnung der Tätigkeit des BfIS in die Aufbau- und Ablauforganisation wurde entsprechend der ABBILDUNG 26 beantwortet.

Frage: 2. Wie ist die Tätigkeit Ihres BfIS in die Aufbau- und Ablauforganisation eingeordnet (zutreffendes bitte ankreuzen)?

Typ: Mehrfachauswahl — Pflichtangabe

Veröffentlichen

Antwort	An-zahl	Pro-zent
keine Angabe	4	12,5%
bisher kein BfIS benannt	10	31,3%
Stabstelle beim Amtsleiter	0	0%
IT- oder Organisationsdezernat	1	3,1%
Extern	10	31,3%
eigene Angabe (bitte Anmerkung im nachfolgenden Feld vornehmen)	7	21,9%

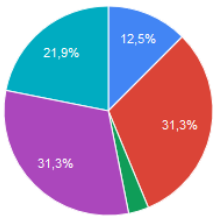


Abb. 26: Umfrage – 4. Frage des Teil A – Teilfrage 2
[Quelle : Passwortgeschütztes Auswertungstool Bürgerbeteiligung Sachsen siehe www.buergerbeteiligung.sachsen.de (2019)]

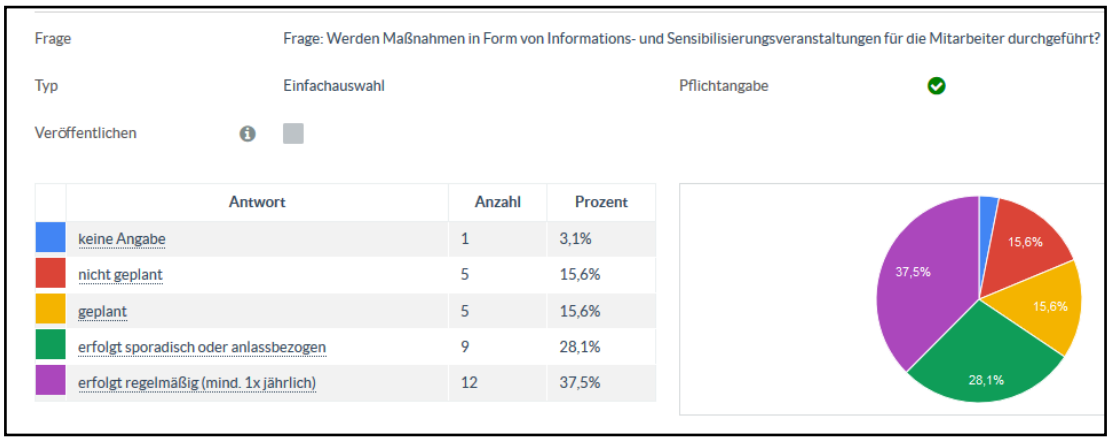
Neben den Angaben, dass bisher kein BfIS benannt wurde, ist festzustellen, dass zehn Umfrageteilnehmer die Tätigkeit eines BfIS extern vergeben haben. Von diesen zehn Kommunen, haben vier Kommunen weniger als 5.000 Einwohner, fünf Kommunen haben zwischen 5.000 und 50.000 Einwohner und eine Kommune hat mehr als 150.000 Einwohner.

Die Umfrageteilnehmer konnten zu dieser 2. Teilfrage auch ebenfalls eigene Angaben vornehmen (offene Frage), insofern die in der Umfrage vorgeschlagenen Angaben nicht zutreffend waren. Zehn Umfrageteilnehmer haben folgende Angaben getätigt:

- Beauftragter - direkt dem Landrat zugeordnet
- als Stabsstelle beim Beigeordneten
- als Stabstelle beim Landrat
- Sachbearbeiter im Fachgebiet IT
- ext. Datenschutzbeauftragter ist IT-Sicherheitsbeauftragter
- direkte Zuordnung zur Behördenleitung

5. Frage: Werden Maßnahmen in Form von Informations- und Sensibilisierungsveranstaltungen für die Mitarbeiter durchgeführt?

Bei zwölf Umfrageteilnehmern erfolgen regelmäßig (mind. 1x jährlich) Informations- und Sensibilisierungsveranstaltungen zum Thema IS. Dies entspricht 37,5 % der an der Umfrage teilgenommenen Kommunen. Weitere neun Kommunen führen sporadisch oder anlassbezogen Veranstaltungen zum Thema IS durch. Weitere Antworten ergeben sich aus der nachfolgenden ABBILDUNG 27.



Antwort	Anzahl	Prozent
keine Angabe	1	3,1%
nicht geplant	5	15,6%
geplant	5	15,6%
erfolgt sporadisch oder anlassbezogen	9	28,1%
erfolgt regelmäßig (mind. 1x jährlich)	12	37,5%

Abb. 27: Umfrage – 5. Frage des Teil A
[Quelle : Passwortgeschütztes Auswertungstool Bürgerbeteiligung Sachsen siehe www.buergerbeteiligung.sachsen.de (2019)]

Im Rahmen einer offenen Frage konnten die Umfrageteilnehmer für sie bestehende Schwierigkeiten von Informations- und Sensibilisierungsveranstaltungen zum Thema IS angeben. Diese Möglichkeit haben 18 Kommunen genutzt. Die Kommunen gaben u.a. an, dass zu wenig Verständnis zu Informations- und Sensibilisierungsveranstaltungen sowie verschiedene Wissens- und Motivationsstände der Mitarbeiter zum Thema IS beständen. Auch wird der Aufwand (personell und zeitlich) von den Kommunen als zu hoch angesehen, vor allem bei größeren Kommunen. Weiterhin genannt werden Schwierigkeiten bei der Organisation der Teilnahme der Beschäftigten an diesen Veranstaltungen aufgrund der Arbeitsbelastung genannt. Das Erfordernis solcher Veranstaltungen wird durch die Beschäftigten laut dieser Umfrage nicht gesehen und der damit verbundene Aufwand gescheut. Kleinere Verwaltungen betrachten den Aufwand für eine Organisation und Durchführung der Veranstaltungen als zu hoch. Auch wird hier das Problem der Finanzierung dieser Veran-

staltungen, dass fehlende Personal und auch die fehlende Zeit, wiederholt von den Kommunen festgehalten.
14 Kommunen machten keine Angaben zu bestehenden Schwierigkeiten.
Der Großteil der Umfrageteilnehmer sah Schwierigkeiten in den Bereichen Budget, fehlendes Personal, Fachwissen bzw. Qualifikation und dem zeitlichen Aufwand zur Durchführung der Informations- und Sensibilisierungsveranstaltungen zum Thema IS.
Von den 17 Kommunen, die Schwierigkeiten im Rahmen der Durchführung von Informations- und Sensibilisierungsveranstaltungen zum Thema IS sehen bzw. benannt haben, haben sieben Kommunen weniger als 5.000 Einwohner, fünf Kommunen haben zwischen 5.000 und 50.000 Einwohner, eine Kommune hat zwischen 50.000 und 150.000 Einwohner und vier Kommunen haben mehr als 150.000 Einwohner.

15 Umfrageteilnehmer machten folgende Angaben zum gewünschten Unterstützungsbedarf (offene Frage):

- externe E-Learning Angebote und Möglichkeiten der "Flächensensibilisierung"
- Muster, Checklisten
- personelle und finanzielle Ressourcen bereitstellen
- zentrale Angebote für Behörden
- Angebot Sensibilisierung In-House / "Die Hacker kommen" u. a. / Aufbauveranstaltungen

Folgende spezifische Fragestellungen wurden den Umfrageteilnehmern ergänzend gestellt:

„1. Wenn Maßnahmen in Form von Informations- und Sensibilisierungsveranstaltungen durch Sie geplant sind oder durchgeführt wurden, welche Zielgruppe (z. Bsp. Behördenleitung, Sachbearbeiter oder andere) soll oder wurde bisher damit angesprochen (kurze Beschreibung der Zielgruppe dieser Maßnahme)?“

Im Rahmen dieser offenen Frage wurden von den Umfrageteilnehmern folgende, oftmals identische, Angaben gemacht:

- alle Mitarbeiter, die Zugang zu Bildschirmarbeitsplätzen mit Netzwerkzugang haben
- alle Mitarbeiter der Verwaltung und Außenstellen, die mit Daten arbeiten

- Behördenleitung/ Leitungspersonal und Sachbearbeiter sowie technisches Personal
- alle Verwaltungsmitarbeiter mit Zugang zum Datenverarbeitungssystem
- Verwaltungsmanagement, Regiebetriebsleiter/-mitarbeiter

Es wurden in der Umfrage nachfolgende Fragen zum Kenntnisstand über die bereits bestehenden Informations- und Sensibilisierungsveranstaltungen gestellt:

„2. Kennen Sie das E-Learning Angebot „Informationssicherheit am Arbeitsplatz“?“

14 Umfrageteilnehmer beantwortete diese Frage mit JA, 18 mit NEIN.

Von den 18 Kommunen, die das Angebot nicht kennen, haben acht Kommunen weniger als 5.000 Einwohner und zehn Kommunen haben zwischen 5.000 und 50.000 Einwohner.

„2.1 Zusatz Frage 2: Nutzen Sie das Angebot bzw. würden Sie das Angebot gern nutzen?“

Neun Umfrageteilnehmer beantwortete diese Frage mit JA, vier mit NEIN.
19 Umfrageteilnehmer würden dieses Angebot nutzen.

Von den 19 Kommunen, die das Angebot nutzen würden, haben neun Kommunen weniger als 5.000 Einwohner, weitere neun Kommunen haben zwischen 5.000 und 50.000 Einwohner und eine Kommune hat mehr als 150.000 Einwohner.

„3. Kennen Sie die Sensibilisierungsveranstaltung „INFOSIC | Die Hacker kommen“?“

20 Umfrageteilnehmer beantwortete diese Frage mit JA, einer mit NEIN.

„3.1 Zusatz Frage 3: Nutzen Sie das Angebot bzw. würden Sie das Angebot gern nutzen?“

13 Umfrageteilnehmer beantwortete diese Frage mit JA, vier mit NEIN.
15 Umfrageteilnehmer würden dieses Angebot nutzen.

Von den 15 Kommunen, die das Angebot nutzen würden, haben sieben Kommunen weniger als 5.000 Einwohner und acht Kommunen haben zwischen 5.000 und 50.000 Einwohner.

„4. Kennen Sie die Sensibilisierungsveranstaltung „INFOSIC plus | IT-Sicherheit für Fortgeschrittene“?“

Neun Umfrageteilnehmer beantwortete diese Frage mit JA, 23 mit NEIN.

Von den 23 Kommunen, die das Angebot nicht kennen, haben zehn Kommunen weniger als 5.000 Einwohner, elf Kommunen haben zwischen 5.000 und 50.000 Einwohner, eine Kommune zwischen 50.000 und 150.000 Einwohner und eine weitere Kommune hat mehr als 150.000 Einwohner.

„4.1 Zusatz Frage 4: Nutzen Sie das Angebot bzw. würden Sie das Angebot gern nutzen?“

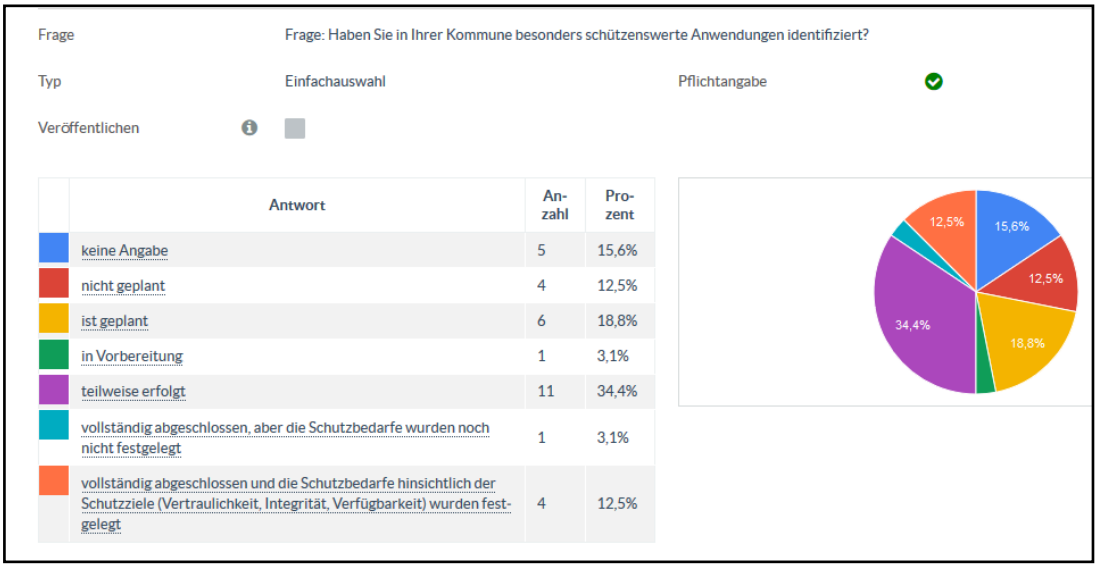
Neun Umfrageteilnehmer beantwortete diese Frage mit JA, sechs mit NEIN.
16 Umfrageteilnehmer würden dieses Angebot nutzen.

Von den 16 Kommunen, die das Angebot nutzen würden, haben sieben Kommunen weniger als 5.000 Einwohner, acht Kommunen haben zwischen 5.000 und 50.000 Einwohner und eine Kommune hat mehr als 150.000 Einwohner.

6. **Frage:** Haben Sie in Ihrer Kommune besonders schützenswerte Anwendungen identifiziert?

Bei vier Umfrageteilnehmern wurden schützenswerte Anwendungen vollständig identifiziert und die Schutzbedarfe hinsichtlich der Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) festgelegt. Dies entspricht 12,5 % der an der Umfrage teilgenommenen Kommunen. Bei dem Großteil der an der Umfrage teilgenommenen Kommunen ist die Identifizierung der schützenswerten Anwendungen teilweise erfolgt (elf Kommunen). Eine grafische Darstellung ergibt sich aus der nachfolgenden ABBILDUNG 28.
Bei den Kommunen, bei denen eine Identifizierung der schützenswerten Anwendungen teilweise erfolgt ist, haben vier Kommunen weniger als 5.000 Einwohner,

drei Kommunen haben zwischen 5.000 und 50.000 Einwohner und vier Kommunen haben mehr als 150.000 Einwohner.
Bei den Kommunen, bei denen eine Identifizierung der schützenswerten Anwendungen geplant ist, haben fünf Kommunen weniger als 5.000 Einwohner und eine Kommune hat zwischen 5.000 und 50.000 Einwohner.



Frage: Frage: Haben Sie in Ihrer Kommune besonders schützenswerte Anwendungen identifiziert?

Typ: Einfachauswahl — Pflichtangabe

Veröffentlichen

Antwort	Anzahl	Prozent
keine Angabe	5	15,6%
nicht geplant	4	12,5%
ist geplant	6	18,8%
in Vorbereitung	1	3,1%
teilweise erfolgt	11	34,4%
vollständig abgeschlossen, aber die Schutzbedarfe wurden noch nicht festgelegt	1	3,1%
vollständig abgeschlossen und die Schutzbedarfe hinsichtlich der Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) wurden festgelegt	4	12,5%

Abb. 28: Umfrage – 6. Frage des Teil A
[Quelle : Passwortgeschütztes Auswertungstool Bürgerbeteiligung Sachsen siehe www.buergerbeteiligung.sachsen.de (2019)]

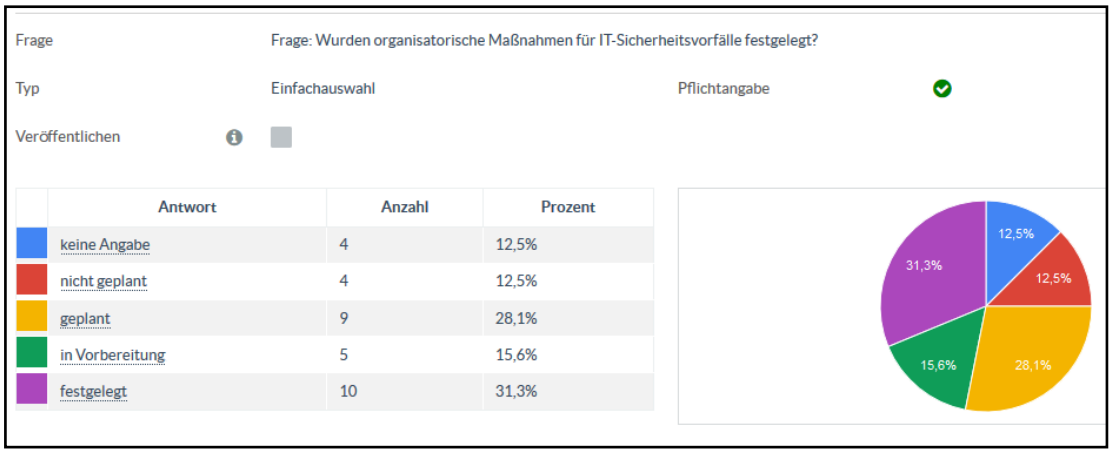
Im Rahmen einer offenen Frage konnten die Umfrageteilnehmer für sie bestehende Schwierigkeiten zum Thema „schützenswerte Anwendungen“ angeben. Diese Möglichkeit haben 18 Kommunen genutzt. Sie gaben an, dass die Identifikation der Anwendungen und die Komplexität der Aufgabe mit zu hohem Zeitaufwand verbunden sind. Als Ursache wurden die verschiedenen Fachverfahren genannt.
14 Kommunen machten keine Angaben zu bestehenden Schwierigkeiten.
Der Großteil der Umfrageteilnehmer sah Schwierigkeiten in den Bereichen Personal, Fachwissen bzw. Qualifikation und dem zeitlichen Aufwand zur Identifizierung der schützenswerten Anwendungen.
Von den 16 Kommunen, die Schwierigkeiten benannt haben, haben sechs Kommunen weniger als 5.000 Einwohner, vier Kommunen haben zwischen 5.000 und 50.000 Einwohner, eine Kommune hat zwischen 50.000 und 150.000 Einwohner und fünf Kommunen haben mehr als 150.000 Einwohner.

Zwölf Umfrageteilnehmer machten folgende Angaben zum gewünschten Unterstützungsbedarf (offene Frage):

- klare Vorgaben an die Einstufung der Vertraulichkeit von Daten (ab wann erhöhter Schutzbedarf?)
- konkrete Ansprechpartner beim Land benennen
- wünschenswerte Zentralisierung der Anwendungen z.B. in Form der Nutzung von Basiskomponenten
- personelle und finanzielle Ressourcen bereitstellen
- Schulung der Beschäftigten

7. Frage: Wurden organisatorische Maßnahmen für IT-Sicherheitsvorfälle festgelegt?

Bei zehn Umfrageteilnehmern wurden organisatorische Maßnahmen für IT-Sicherheitsvorfälle festgelegt. Dies entspricht 31,3 % der an der Umfrage teilgenommenen Kommunen. Bei neun von ihnen sind organisatorische Maßnahmen für IT-Sicherheitsvorfälle geplant (siehe ABBILDUNG 29)



Antwort	Anzahl	Prozent
keine Angabe	4	12,5%
nicht geplant	4	12,5%
geplant	9	28,1%
in Vorbereitung	5	15,6%
festgelegt	10	31,3%

Abb. 29: Umfrage – 7. Frage des Teil A
[Quelle : Passwortgeschütztes Auswertungstool Bürgerbeteiligung Sachsen siehe www.buergerbeteiligung.sachsen.de (2019)]

Bei den Kommunen, bei denen organisatorische Maßnahmen für IT-Sicherheitsvorfälle festgelegt wurden, haben zwei Kommunen weniger als 5.000

Einwohner, vier Kommunen haben zwischen 5.000 und 50.000 Einwohner und nochmalig vier Kommunen haben mehr als 150.000 Einwohner.
Bei den Kommunen, bei denen sich organisatorische Maßnahmen für IT-Sicherheitsvorfälle in Vorbereitung befinden, haben zwei Kommunen weniger als 5.000 Einwohner, weitere zwei Kommunen haben zwischen 5.000 und 50.000 Einwohner und eine Kommune hat mehr als 150.000 Einwohner.
Bei den Kommunen, bei denen organisatorische Maßnahmen für IT-Sicherheitsvorfälle geplant sind, haben fünf Kommunen weniger als 5.000 Einwohner, zwei Kommunen haben zwischen 5.000 und 50.000 Einwohner und nochmalig zwei Kommunen haben mehr als 150.000 Einwohner.

Im Rahmen einer offenen Frage konnten die Umfrageteilnehmer für sie bestehende Schwierigkeiten zum Thema „organisatorische Maßnahmen für IT-Sicherheitsvorfälle“ angeben. Diese Möglichkeit haben zwölf Kommunen genutzt. Sie gaben an, dass Probleme im Hinblick auf die Prozessabstimmung, Praktikabilität und Umsetzbarkeit im Verwaltungsalltag sowie der Akzeptanz für Prozesse bestehen. Auch wurde genannt, dass diese organisatorischen Maßnahmen nicht als Führungsaufgabe angesehen werden. Die Umfrageteilnehmer hielten ebenfalls Schwierigkeiten in den Bereichen Personal, Fachwissen bzw. Qualifikation und dem zeitlichen Aufwand zur Umsetzung organisatorischer Maßnahmen fest.
Von den elf Kommunen, die Schwierigkeiten benannt haben, haben fünf Kommunen weniger als 5.000 Einwohner, eine Kommune hat zwischen 5.000 und 50.000 Einwohner, eine weitere Kommune hat zwischen 50.000 und 150.000 Einwohner und vier Kommunen haben mehr als 150.000 Einwohner.
14 Kommunen machten keine Angaben zu bestehenden Schwierigkeiten bzw. sahen keine Schwierigkeiten.

Neun Umfrageteilnehmer machten folgende Angaben zum gewünschten Unterstützungsbedarf (offene Frage):

- Vorlage eines Sicherheitskonzepts zur Prüfung und evtl. Anregungen zur Verbesserung
- Mustervorlagen
- personelle und finanzielle Ressourcen bereitstellen

Folgende spezifische Fragestellungen wurden den Umfrageteilnehmern ergänzend gestellt:

„1. Gibt es bei Ihnen vorgeschriebene Abläufe bei IT-Sicherheitsvorfällen z. Bsp. durch einen Angriff auf Ihre IT durch Schadsoftware?“

15 Umfrageteilnehmer beantwortete diese Frage mit JA, zehn mit NEIN.
Sieben Umfrageteilnehmer machten keine Angaben.

„2. Haben Sie schon einmal einen IT-Sicherheitsvorfall dem "Computer Emergency Response Team" (SAX.CERT) der Landesverwaltung des Freistaates gemeldet?“

Vier Umfrageteilnehmer beantwortete diese Frage mit JA, 26 mit NEIN.
Zwei Umfrageteilnehmer machten keine Angaben.

Eine Betrachtung von potenziellen Lösungsmöglichkeiten der hier dargestellten Probleme aus Basis der Umfrageergebnisse zum Teil A erfolgt im fünften Kapitel. Nachfolgend werden nun die Ergebnisse des Teil B der Umfrage aufgezeigt.

4.3.3 ERGEBNISSE UMFRAGE TEIL B

In diesem Abschnitt der Umfrage erhielten die Umfrageteilnehmer die Möglichkeit, der Staatskanzlei sowie den kommunalen Spitzenverbänden einen Überblick darüber zu geben, welche Unterstützung sie sich beim Aufbau und zur Weiterentwicklung der IS vorstellen könnten bzw. ihnen hilfreich wäre. Mehrfachnennungen waren möglich. Die Aufzählung im Fragebogen war jedoch nicht abschließend. Es gab die Möglichkeit eigene Angaben vorzunehmen.
In der nachfolgenden TABELLE 2 wird eine Übersicht über die vorgeschlagenen Unterstützungsmöglichkeiten gegeben. Ebenfalls ist aus dieser Tabelle erkennbar, wie häufig die jeweilig vorgegebenen Antwortmöglichkeiten von den 32 Umfrageteilnehmern ausgewählt wurden.

Unterstützungsmöglichkeiten	Anzahl der Kommunen, die diese Unterstützungsmöglichkeit wünschten
Hilfestellung im Schadensfall durch persönliche Anleitung zur Schadensregulierung	27
Informationen zu IT-Sicherheitsbedrohungen	26
Checklisten	25
Sensibilisierungsveranstaltungen	24
Seminare / Workshops	23
Informationsbroschüren	15
Allgemeine Informationsveranstaltungen	15
Keine Unterstützung gewünscht	0

Tab. 2: Umfrage – Teil B – gewünschte Unterstützungen
[Quelle : Passwortgeschütztes Auswertungstool Bürgerbeteiligung Sachsen siehe www.buergerbeteiligung.sachsen.de (2019)]

Die Analyse der Umfrageergebnisse zum Teil B ergibt, dass aus denen im Fragebogen vorgegeben Antwortmöglichkeiten verstärkt Unterstützungsbedarf im Rahmen der IS durch Checklisten, Informationen zu IT-Sicherheitsbedrohungen, Seminaren, Workshops, Sensibilisierungsveranstaltungen und Hilfestellungen im Schadenfall

durch persönliche Anleitung zur Schadensregulierung von den Kommunen gewünscht wird.

Ebenfalls konnten die Kommunen im Rahmen dieser Umfrage eigene gewünschte Unterstützungen formulieren. Diese Möglichkeit haben neun Kommunen in Anspruch genommen. Gewünschte Unterstützungen sehen die Kommunen weiterführend zu den Angaben in der TABELLE 2 auch in folgenden Bereichen, die sich teilweise mit den Antworten der sieben Fragen (ohne einleitende Fragen) des Teil A der Umfrage decken:

- Einstellung von Fachkräften beim Land, die für die kleineren Kommunen zuständig sind und auch vor Ort unterstützen
- zentrale Vorgaben und Möglichkeiten um die IT-Sicherheit zu erhöhen (zentrale technische Lösungen)
- Standardverfahren (Fachanwendungen) die im Freistaat gehostet werden; anbieten als Basiskomponente, Entfall von Berichtspflichten in der Fachanwendung (funktionierende Beispiele: EU-Zahlstelle, Wohngeld, etc.)
- Bereitstellung eines zentralen Grundschutztools
- Erstellung und kostenlose Bereitstellung von allgemeinen Mustertexten
- besseres Finanz-, Zeit- und Personalbudget
- technische Schutzsysteme zur Mitnutzung durch Kommunen
- IT-fachliche Überprüfung/ Freigabe zur Nutzung von seiten des Freistaates empfehlen oder verpflichtend einführen
- rechtzeitige Information bei geplanten Umstellungen

Beratungs- und Unterstützungsbedarf besteht für die Kommunen zu folgenden Themen:

- fachliche Beratung zu allen in den letzten Jahren vorgegeben und durch Gesetz auferlegten Aufgaben
- Sicherheitsbedrohungen – Newsletter
- Grundinformationen in Broschürenform als Unterweisungsmöglichkeit
- Sensibilisierung als kurze Demosoftware/ Filmclip

4.3.4 ERGEBNISSE UMFRAGE TEIL C

In diesem Abschnitt der Umfrage erhielten die Umfrageteilnehmer die Möglichkeit, der Staatskanzlei sowie den kommunalen Spitzenverbänden einen Überblick darüber zu geben, welche Hemmnisse sie für den Aufbau einer systematischen Informationssicherheit in ihrer Kommune sehen. Die Übersicht war jedoch nicht abschließend. Daher sind eigene Angaben möglich gewesen.
In der nachfolgenden TABELLE 3 wird eine Übersicht über die vorgeschlagenen Unterstützungsmöglichkeiten gegeben. Ebenfalls ist aus dieser Tabelle erkennbar, wie häufig die jeweilig vorgegebenen Antwortmöglichkeiten von den 32 Umfrageteilnehmern ausgewählt wurden.

Hemmnisse	Anzahl der Kommunen, die Hemmnisse angegeben haben
Fehlendes Personal	28
Geringes Budget	23
Interne organisatorische Probleme	16
Mangelnde Akzeptanz der Mitarbeiter	9
Unzureichende Unterstützung der Behördenleitung	8
Probleme der Steuerung von externen Dienstleistern z. Bsp. bei Outsourcing (Probleme in der Zusammenarbeit mit externen Dienstleistern im Rahmen der Informationssicherheit)	7
Es bestehen keine Hemmnisse	1

Tab. 3: Umfrage – Teil C – Hemmnisse
[Quelle : Passwortgeschütztes Auswertungstool Bürgerbeteiligung Sachsen siehe www.buergerbeteiligung.sachsen.de (2019)]

Auch hier konnten die Kommunen im Rahmen dieser Umfrage weitere eigene Hemmnisse formulieren. Diese Möglichkeit haben drei Kommunen in Anspruch genommen. Auch ist die Frage gestellt worden, ob die „Produktion von IT immer noch der effektivste Weg für die Kommunalverwaltung ist sowie, ob regionale Kooperationen in einem Verbund nicht ein systematischer Ansatz für mehr Informationssicherheit“ wären.

5 KONZEPTENTWICKLUNG ZUM AUFBAU UND WEITERENTWICKLUNG DER INFORMATIONSSICHERHEIT IN DEN SÄCHSISCHEN KOMMUNEN

5.1 ZUSAMMENFASSUNG PROBLEMFELDER AUS UMFRAGEERGEBNISSEN

Die im KAPITEL 4.3 dargestellten Umfrageergebnisse machen eins deutlich: Die im **Teil A** der Umfrage genannten Probleme sind bei mehrere Fragen identisch. Vermehrt wurden die begrenzten finanziellen und personellen Ressourcen und auch der zeitliche Aufwand für das Thema IS benannt. Vor der Veröffentlichung der Umfrage ist mit der Staatskanzlei abgestimmt worden, dass die vorhergehend genannten Punkte jedoch nicht Bestandteil der Konzeptentwicklung sein sollen. Daher werden im Rahmen dieser Masterarbeit diese Aspekte nicht weiter betrachtet.

Ein wichtiges Ergebnis der Umfrage war, dass unter den Umfrageteilnehmern bisher nur 50 % der Kommunen einen BfIS benannt haben. Wie bereits im dritten Kapitel erläutert wurde, müssen die Kommunen bis Ende 2020 einen BfIS benannt und dem Freistaat mitgeteilt haben. Dazu wurde bereits von Seiten der Staatskanzlei die Möglichkeit der Onlinemeldung über die Benennung eines BfIS für die Kommunen eingeräumt.

Problemfeld 1 – Informationssicherheitsleitlinie

Die Auswertung der Umfrage ergab, dass das geringe oder teilweise auch fehlende Fachwissen zum Thema „Informationssicherheitsleitlinie“ von den Umfrageteilnehmern als problematisch angesehen wird. Auch wurde das fehlende Verständnis der Bedeutung einer Informationssicherheitsleitlinie bei den Beschäftigten genannt.

Problemfeld 2 – IT-Sicherheitskonzept

Die Umfrageteilnehmer sehen grundsätzliche Schwierigkeiten bei der Erstellung und Umsetzung des IT-Sicherheitskonzepts. Weiterführend bestehen auch hier Probleme im geringen oder teilweise fehlenden Fachwissen zu diesem Thema. Positiv wurde die Frage aufgenommen, ob sich die Kommunen vorstellen könnten, mit einem Muster eines IT-Sicherheitskonzepts zu arbeiten.

Problemfeld 3 – ISMS

Die Auswertung der Umfrage ergab auch hier, dass das geringe oder teilweise fehlende Fachwissen zum Thema „ISMS“ von den Umfrageteilnehmern als problematisch angesehen wird. Auch wurde das fehlende Verantwortungsbewusstsein der Führungsebene in diesem Bereich genannt. Schwierigkeiten gibt es bei der Erstellung, Umsetzung und dem Betrieb eines ISMS. Der BfIS wird an Verwaltungsprojekten und Verwaltungsentscheidungen bei den meisten Umfrageteilnehmern nur sporadisch beteiligt oder es bisher noch kein BfIS benannt. Sicherheitschecks wurden bei mehr als der Hälfte der Umfrageteilnehmer bisher nicht durchgeführt.

Problemfeld 4 – Sicherheitsorganisation

Die Umfrage ergab, dass bei den Kommunen, die eine Sicherheitsorganisation etabliert haben, keine Problempunkte zu diesem Thema bestehen. Jedoch besteht bei 34 % der Umfrageteilnehmer laut eigenen Angaben keine Sicherheitsorganisation.

Problemfeld 5 - Informations- und Sensibilisierungsveranstaltungen

Auch hier sei zusammengefasst nochmal zu erwähnen, dass bei den Kommunen teilweise zu wenig Verständnis zu Informations- und Sensibilisierungsveranstaltungen sowie verschiedene Wissens- und Motivationsstände der Mitarbeiter zum Thema IS existieren. Das Erfordernis von Sensibilisierungen wird durch die Beschäftigten nicht gesehen und der damit verbundene Aufwand wird gescheut.

18 Kommunen erfuhren erst durch die Umfrage, dass das E-Learning Angebot „Informationssicherheit am Arbeitsplatz“ auch von den Kommunen genutzt werden kann. Die Umfrage macht deutlich, dass die Kommunen, die dieses Angebot noch nicht genutzt haben, es zukünftig nutzen würden.

Auch die Sensibilisierungsveranstaltung „INFOSIC | Die Hacker kommen“ ist bei dem Großteil der Umfrageteilnehmer bekannt; 15 Umfrageteilnehmer würden dieses Angebot gern nutzen.

Die Sensibilisierungsveranstaltung „INFOSIC plus | IT-Sicherheit für Fortgeschrittene“ ist bei dem Großteil der Umfrageteilnehmer nicht bekannt (23 Umfrageteilnehmern). 16 Umfrageteilnehmer würden dieses Angebot gern nutzen.

Das Umfrageergebnis zu diesem Thema ergibt, dass vor allem bei den Kommunen mit weniger als 50.000 Einwohnern das Bestehen der genannten Sensibilisierungsveranstaltungen nicht bekannt ist, dass Interesse zur Teilnahme an solch einer Veranstaltung jedoch gegeben ist.

Problemfeld 6 - schützenswerte Anwendungen

Die Identifikation der Anwendungen, die Komplexität der Aufgabe mit zu hohem Zeitaufwand und die in den Kommunen genutzten verschiedenen Fachverfahren wurden als bestehende Probleme in diesem Bereich benannt. Auch fehle es hier an Personal und Fachwissen zu diesem Thema.

Problemfeld 7 - organisatorische Maßnahmen für IT-Sicherheitsvorfälle

Für die Kommunen bestehen Schwierigkeiten im Hinblick auf die Prozessabstimmung, Praktikabilität und Umsetzbarkeit im Verwaltungsalltag sowie der Akzeptanz für Prozesse. Auch wurde hier angemerkt, dass diese organisatorischen Maßnahmen nicht als Führungsaufgabe angesehen werden. Wiederholt wurden ebenfalls das geringe oder teilweise fehlende Fachwissen bzw. die fehlenden Qualifikationen zur Umsetzung organisatorischer Maßnahmen.

5.2 Zusammenfassung gewünschter Unterstützungen

Wie bereits im Kapitel 4.3 dargestellt wurde, ist von den Umfrageteilnehmern vermehrt der Wunsch geäußert worden, Grundkonzepte zu den Umfragethemen zur Verfügung zu stellen.

Zum Thema „Informationssicherheitsleitlinie“ kam zusätzlich der Wunsch nach einer Musterleitlinie auf bzw. die Benennung von Inhalten, die zu diesem Thema wichtig sind.

Unterstützungen werden ebenfalls durch Checklisten, Musterkonzepte/ Mustervorlagen oder Handreichungen gewünscht. Darüber hinaus äußerten die Teilnehmer vermehrt den Wunsch der Benennung konkreter Ansprechpartner beim Land zum Thema IS. Laut den Umfrageteilnehmern ist eine Sensibilisierung der Führungskräfte ebenfalls notwendig, damit das Thema IS in den Kommunen mehr an Bedeutung gewinnt. Dabei sei es auch laut den Kommunen erforderlich, gezielt Informationen zum Thema IS gegenüber den Bürgermeistern zu kommunizieren, damit ein besseres Verständnis und dadurch größere Unterstützung möglich wird. Die Themen „In-House-Schulungen, Seminare/ Workshops, Beratungen, externe E-Learning Angebote“ zur Vermittlung von Know-how zum Thema IS wurden in allen Fragestellungen als eine mögliche Unterstützung für die Kommunen genannt.

Aus Sicht der Teilnehmer sind Kooperationen innerhalb der sächsischen Kommunen zu den Umfragethemen sinnvoll. Auch wurden vor-Ort-Unterstützungen durch Experten in der Umfrage genannt.

Beim Thema „schützenswerte Anwendungen“ wünschen sich die Kommunen klare Vorgaben an die Einstufung der Vertraulichkeit von Daten (ab wann besteht erhöhter Schutzbedarf).
Im Bereich der „organisatorische Maßnahmen für IT-Sicherheitsvorfälle“ ergeben die Umfrageergebnisse den Wunsch nach der Prüfung der kommunalen Sicherheitskonzepte durch den Freistaat Sachsen sowie die Feststellung von potenziellen Verbesserungen in den eingereichten IT-Sicherheitskonzepten.

Zusammenfassend ergab der Teil B der Umfrage zusätzlich zu den vorhergehend genannten Unterstützungen, dass die Kommunen einen verstärkten Bedarf im Rahmen der IS an Informationen zu IT-Sicherheitsbedrohungen sowie Hilfestellungen im Schadenfall durch persönliche Anleitung zur Schadensregulierung haben.

5.3 Möglichkeiten der Realisierbarkeit der gewünschten Unterstützungen

5.3.1 Information Security Awareness

“Neben technischen Sicherheitsmaßnahmen, z.B. dem Einsatz kryptographischer Verfahren und Zugriffskontrollmechanismen, ist eine Vielzahl weiterer Instrumente zum kritischen Erfolgsfaktor für die Informationssicherheit im Unternehmenskontext geworden. Eine entscheidende Rolle nimmt dabei die Security Awareness […] ein.“[91] „Um die Anwender für ihre wichtige Rolle als Stütze des Informationssicherheitskonzepts fit zu machen, müssen sie sensibilisiert werden. Der Fachbegriff dafür lautet Information Security Awareness.“ [92] „Information Security Awareness ist der – bezüglich der Sicherheitsgefahren – bewusste Umgang mit Informationen, unabhängig vom Medium.“ [93] Durch Awareness-Maßnahmen sollen Anwender überzeugt werden, sich (sowohl beruflich als auch privat) so zu verhalten, dass sie weder wissentlich noch unwissentlich die Sicherheit der Informationssysteme ihres Unternehmens schaden. Anwender sollen dabei mithelfen, Informationen und Informationssysteme vor Gefahren zu schützen, auch bezeichnet als informationssicherheitskonformes Verhalten. Menschen verhalten sich nicht immer „informationssicherheitskonform“. Durch unbedachtes Verhalten z. Bsp. am Arbeitsplatz kann die Sicherheit

[91] Schulz, T. (2020) S. 316
[92] Weber, K., Schütz, A. E., Fertig, T. (2019) S. 3
[93] Weber, K., Schütz, A. E., Fertig, T. (2019) S. 9

von sensiblen Informationen gefährden werden.[94] Um nur einige Beispiele zu nennen, sollen nachfolgende Erläuterungen die verschiedenen Verhaltensweisen, näher erklären.

PASSWÖRTER

Der Zugriff auf Informationssysteme erfolgt fast ausschließlich durch die korrekte Kombination aus Benutzername und Passwort. Menschen, die diese Kombination kennen, erhalten Zugriff auf die Informationssysteme. Dabei ist zu nennen, dass im Arbeitsalltag der Benutzername häufig (von der IT-Fachabteilung) vorgegeben wird. Das Passwort hingegen kann von den Anwendern selbst gewählt werden. Gibt es keine internen Regelungen zur Zusammensetzung eines Passwortes, kann es dazu kommen, dass einfache Passwörter gewählt werden, die auch selten von den Beschäftigten in ihrem kompletten Aufbau regelmäßig geändert werden. Auch die vertretungsweise Weitergabe der Passwörter an Kollegen ist dabei ein oft diskutiertes Thema.[95] Hier könnten, insofern nicht bereits vorhanden, Hilfestellungen gegenüber den Kommunen bspw. bei der Erstellung einer Handlungsanleitung zur korrekten Festlegung von Passwörter durch die Beschäftigten erfolgen (Erstellung Verwaltungsvorschrift) sowie Unterstützungen bei der technischen Umsetzung von Vorschriften zur Passwortvergabe.

SCHÄDLICHE E-MAILS

„E-Mails werden häufig genutzt, um Schadsoftware zu verbreiten und auf dem Rechner der Adressaten zu installieren oder um die Zugangsdaten (Benutzernamen, Passwörter) der Adressaten auszuspähen. Letzteres wird als Phishing bezeichnet.“ [96] Dabei kam es in der Vergangenheit auch immer wieder dazu, dass auch an öffentliche Einrichtungen per E-Mail z. Bsp. Rechnungen versendet wurden mit der Angabe eines Internetlinks. Der Virus installiert sich dann selbst z. Bsp. durch Klicken auf den Link. Auch hierbei können die Kommunen zum Beispiel durch Sensibilisierungsmaßnahmen unterstützt werden.

[94] Vgl. Weber, K., Schütz, A. E., Fertig, T. (2019) S. 3
[95] Vgl. Weber, K., Schütz, A. E., Fertig, T. (2019) S. 4
[96] ebd.

SOCIAL ENGINEERING

„Neben dem unabsichtlichen und absichtlichen Fehlverhalten der Anwender gibt es noch eine weitere Gefahr für die Informationssicherheit, bei welcher der Faktor Mensch eine entscheidende Rolle spielt. Der Mensch selbst wird gezielt angegriffen. […] Die am meisten verwendete Angriffstechnik auf den Menschen ist das sogenannte Social Engineering. Social Engineering beschreibt die gezielte Manipulation von Menschen.“[97] Dabei sollen die Menschen so beeinflusst werden, dass sie unbewusst nicht in ihrem eigenen Interesse handeln. Ein Beispiel dafür sind die vorhergehend genannten Phishing-E-Mails. Der Empfänger einer solchen E-Mail soll dazu verleitet werden, z. Bsp. Logindaten oder Kreditkartennummer auf einer manipulierten Internetseite (von den Angreifern erstellt) einzugeben. Jedoch werden neben Geld auch oftmals Ideen und auch geheime Daten erbeutet. Dieser Betrug muss vom Herausgebenden nicht zwingend sofort erkannt bzw. aufgedeckt werden.[98]

Den Kommunen kann dabei eine Hilfestellung bei diesem Thema durch Schulungen und Informationsveranstaltungen gegeben werden.

Die vorhergehende Auswahl von Beispielen zeigt somit, wie durch nicht korrekte Handlungen die IS in jeder Kommune gefährdet sein kann. Auch die durch die Medien bereits zu Beginn des Jahres 2020 veröffentlichten Nachrichten über großflächige Hackerangriffe in öffentlichen Verwaltungen und auch gemeinnützigen Vereinen machen deutlich, wie wichtig die Sensibilisierung von Mitarbeiter durch Schulungen, Workshops oder Fortbildung ist. Auch hat die Umfrage ergeben, dass der Bedarf an derartigen Angeboten bei den sächsischen Kommunen durchaus besteht. Wie bereits dargestellt, sind die im Rahmen der Umfrage abgefragten Kenntnisse über das Bestehen von Sensibilisierungsangeboten unterschiedlich ausgefallen (siehe KAPITEL 4.3.2). Vor allem für das E-Learning Angebot „Informationssicherheit am Arbeitsplatz“ und die Sensibilisierungsveranstaltung „INFOSIC plus | IT-Sicherheit für Fortgeschrittene“ wird empfohlen, vermehrt „Werbung“ bei den Kommunen über die Möglichkeit der Teilnahme an diesen Angeboten zu betreiben. Auch sollte darüber nachgedacht werden, ob das E-Learning Angebot „Informationssicherheit am Arbeitsplatz“ auch als Schulung, zentral organisiert ähnlich der Sensibilisierungsveranstaltung „INFOSIC | Die Hacker kommen“, für die Kommunen angeboten werden kann. Die Erfahrung zeigt, dass es im täglichen Berufsalltag oftmals

[97] Weber, K., Schütz, A. E., Fertig, T. (2019) S. 6
[98] Vgl. Weber, K., Schütz, A. E., Fertig, T. (2019) S. 6-7

schwierig ist, zeitintensive E-Learning Angebote am Arbeitsplatz wahrzunehmen. Es sollte darüber hinaus stärker kommuniziert werden, dass IS auch die Führungsverantwortlichen betrifft. Darauf wurde verstärkt im Rahmen der Umfrage durch die Kommunen hingewiesen.

5.3.2 KOMMUNIKATION MIT KOMMUNEN

Es stellt sich ebenfalls die Frage, wie man mit den Kommunen noch effizienter Informationen bspw. zur aktuellen Gefährdungslage oder auch zu Neuerungen in Sachen IS austauschen kann. Dabei müssen sowohl bestehende als auch potenziell neue Vorgehensweisen betrachtet werden.

Die bisherigen Erfahrungen der Erstellerin dieser Masterarbeit zeigen, dass überprüft werden sollte, wie allgemeinverständlich die vom SAX.CERT versendeten Warnmeldungen bspw. zu aktuell bestehenden „Wellen“ von gefälschten E-Mails, die an die Verwaltungen versendet werden, aufgebaut sein können. Der Empfänger solcher Warnmeldungen muss nicht zwangsläufig über den fachlichen Hintergrund verfügen, um den Inhalt und die Fachbegriffe in diesen Warnmeldungen zu verstehen. Die vom SAX.CERT versendeten Warnmeldungen werden von den jeweiligen IT-Fachbereichen der jeweiligen Verwaltungseinrichtungen ohne weitere Hinweise oder Erläuterungen an die Beschäftigten versendet. Sind dann bereits die ersten Sätze in diesen Meldungen mit komplexen IT-Begrifflichkeiten und Erläuterungen versehen, kann dies dazu führen, dass die Meldungen ungelesen gelöscht werden, da der Leser zwangsläufig nicht versteht, was er an seinem eigenen Verhalten in Sachen IS verändern muss.

Als weiteres Medium zur Übermittlung von Informationen im Bereich IS dient ebenfalls der zuletzt 2018 veröffentlichte „Jahresbericht Informations- und Cybersicherheit 2017“. Es sollte überprüft werden, ob eine weitere Auflage veröffentlicht werden kann.

Um einen neuen Weg zur Kommunikation mit den Kommunen zu gehen, wäre auch die Vermittlung von Informationen zum Thema IS über eine eigens dafür erstellte Internetseite denkbar. Durch diese können sich Kommunen dann mittels Registrierung aktuelle Informationen und Berichte zur IS beschaffen, Warnmeldungen abrufen und Informationen über Sensibilisierungsveranstaltungen (inkl. direkter Anmeldung) erhalten. Hierüber wäre es dann ebenfalls möglich, die gewünschten Checklisten, Mustervorlagen, Handreichungen oder Grundkonzept zur Verfügung zu stellen.

5.3.3 Vor-Ort-Unterstützung

Ob es die Möglichkeit einer Vor-Ort-Unterstützung der Kommunen durch den Freistaat gibt, kann von Seiten der Erstellerin dieser Masterarbeit nicht beantwortet werden. Sollte es die Möglichkeit nicht geben, wäre eine Option eine Diskussion darüber bei den verantwortlichen Personen zu platzieren.

Bei einer Informationssicherheitsberatung könnten konkrete und individuelle Maßnahmenpakete sowie Empfehlungen und Tipps zur Verbesserung der IS bei den Kommunen erfolgen. Dadurch können ebenfalls die Digitalisierungsvorhaben der öffentlichen Verwaltung auch unter dem Aspekt der Umsetzung des Onlinezugangsgesetzes gestärkt und unterstützt werden.[99]

Auch wäre es denkbar, dass im Rahmen von Vor-Ort-Beratungen bspw. die erstellten Handlungsanleitungen oder die Identifizierung schützenswerter Anwendungen mit dem Freistaat besprochen und auf ihre korrekte Umsetzung hin gemeinsam überprüft werden, um den Kommunen eine Hilfestellung beim Aufbau und der Weiterentwicklung der IS zu geben.

5.3.4 Mitarbeiter zielgerichtet sensibilisieren

„Mitarbeiter sind eine wichtige Stütze für das Informationssicherheitskonzept jedes Unternehmens. Die Awareness der Mitarbeiter – also der Grad der Sensibilisierung – für die Informationssicherheit entscheidet darüber, wie gut sie ihre Funktion als Stütze wahrnehmen können. Je mehr die Mitarbeiter über mögliche Bedrohungen und entsprechende Gegenmaßnahmen wissen und je mehr sie sich entsprechend ihres Wissens verhalten, umso besser ist es um die Sicherheit von sensiblen Unternehmensinformationen bestellt.“[100] Vor der Sensibilisierung der Beschäftigten in den Kommunen wäre es sinnvoll, die Ist-Situation zu analysieren. Daraus können verschiedene Verhaltensweisen wie Widerstände, Überzeugungen, Emotionen oder mögliche Barrieren der Beschäftigten analysiert werden. Dies kann durch Interviews bspw. mit Fragebögen, die dann von entsprechender Stelle analysiert werden, bei den jeweiligen Behörden durchgeführt werden.[101] Auf Basis der vorliegenden Ergeb-

[99] Vgl. www.bundesregierung.de (2019) S. 47
[100] Weber, K., Schütz, A. E., Fertig, T. (2019) S. 19
[101] Vgl. Weber, K., Schütz, A. E., Fertig, T. (2019) S. 19, 23, 26, 37

nisse können dann die Kommunen bei der Auswahl von Maßnahmen und die Planung von eigenen Sensibilisierungsveranstaltungen sowie deren Durchführung unterstützt werden. Die Umfrage hat, wie bereits ausführlich in den vorhergehenden Kapiteln beschrieben, ergeben, dass bei den Kommunen insgesamt zum Thema IS ein Bedarf an Sensibilisierungsveranstaltungen (bzw. der Hilfe zur Vorbereitung und Durchführung eigener Sensibilisierungsveranstaltungen) besteht.

5.3.5 Mindmap der möglichen Unterstützungen der sächsischen Kommunen

Die in diesem 5. Kapitel aufgestellten Unterstützungsmöglichkeiten der Kommunen zum Aufbau und zur Weiterentwicklung der IS in sächsischen Kommunen werden in der nachfolgenden Abbildung in Form eines Mindmap grafisch dargestellt, damit die vorhergehend beschriebenen Unterstützungsmöglichkeiten noch einmal übersichtlich zusammengefasst sind.

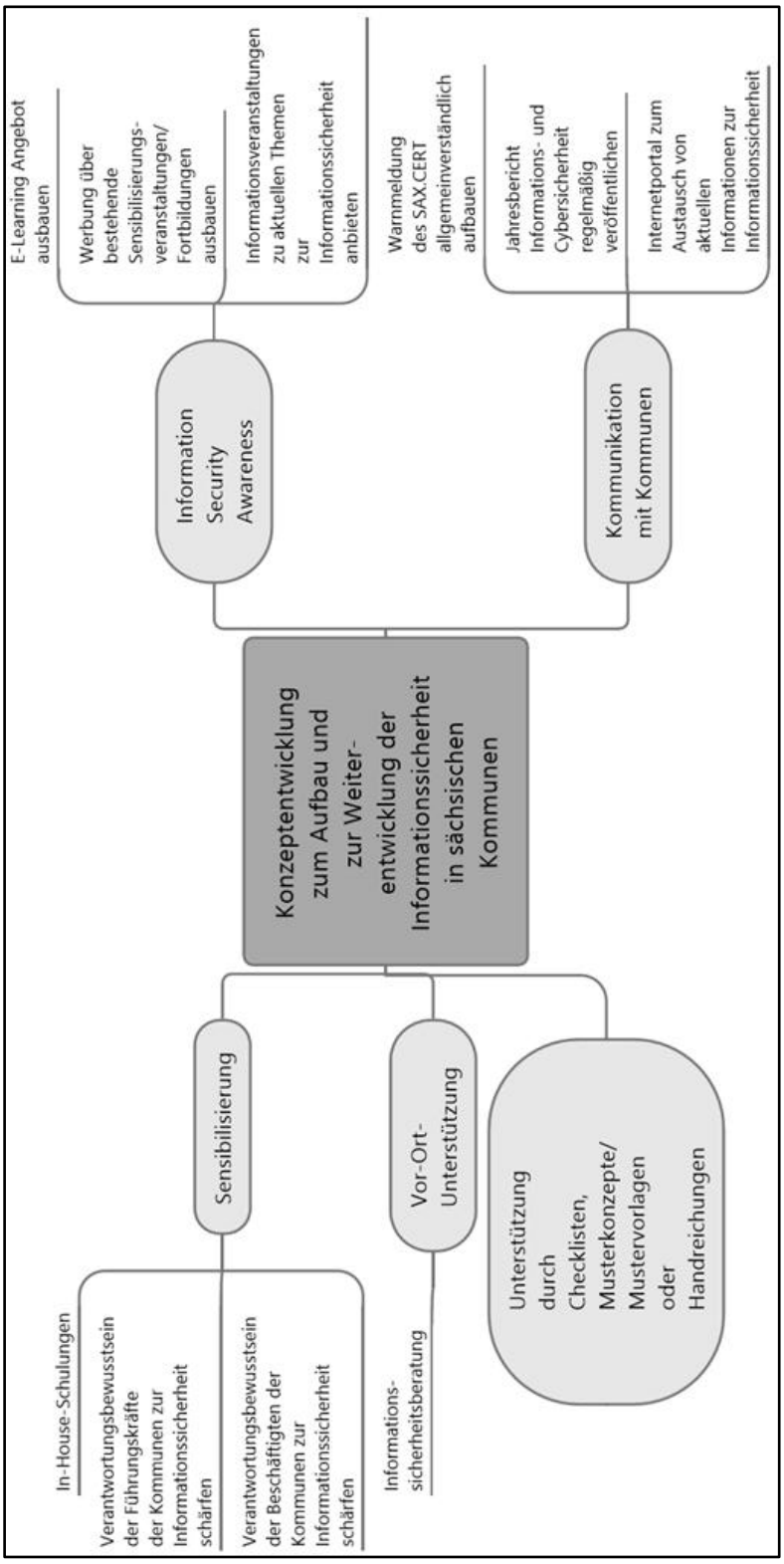


Abb. 30: Mindmap Zusammenfassung Unterstützungsmöglichkeiten
[Quelle : Eigene Darstellung]

6 SCHLUSSBETRACHTUNG UND AUSBLICK

6.1 ZUSAMMENFASSUNG

Im Rahmen dieser Masterarbeit konnten Schwachstellen und Verbesserungspotenziale zum Aufbau und Weiterentwicklung der IS bei den sächsischen Kommunen erkannt werden. Durch die genannten Erkenntnisse konnten erste Handlungsempfehlungen definiert werden. Auch wenn die genannten Probleme „fehlendes Personal und fehlendes Budget“, wie bereits erwähnt, im Rahmen dieser Masterarbeit nicht weiter betrachten wurden, ist darauf in den meisten Fragestellungen innerhalb der Umfrage von den Umfrageteilnehmern eingegangen worden. Auch wurde vermehrt das fehlende Know-how bzw. Verantwortungsbewusstsein gegenüber der IS in den Kommunen benannt. Erkennbar ist, dass die genannten Probleme bzw. Schwierigkeiten sich in den einzelnen Fragen des Teil A der Umfrage wiederholen. Diese Themen sollten neben den anderen Umfrageergebnissen vom Freistaat in Zusammenarbeit mit den Kommunen aufgegriffen werden.

6.2 KRITISCHE WÜRDIGUNG

Zusammenfassend wird bei der Durchführung der Umfrage innerhalb dieser Abschlussarbeit jedoch kritisch gesehen, dass die Resonanz der Teilnahme an der Befragung gemessen an der Anzahl der möglichen Umfrageteilnehmern in Höhe von 419 Kommunen nur bei 7,6 % lag. Als Ursachen kann zum Einen der Zeitpunkt der Umfrage gesehen werden als auch zum Anderen die Art der Informationsübermittlung der Veröffentlichung der Umfrage gegenüber den Kommunen. Die Umfrage wurde in einem Zeitraum veröffentlicht, in dem die Kommunen einerseits vielfältige Aufgaben im Rahmen des Jahresabschlusses zu absolvieren haben. Desweiteren wurde die Umfrage in einer potenziellen Urlaubszeit durchgeführt. Um weiteren Kommunen die Teilnahme an der Umfrage zu ermöglichen, erfolgten Erinnerungen per E-Mail an alle Kommunen sowie die Verlängerung des Umfragezeitraums. Darüber hinaus hätte bei der Art der Informationsvermittlung gegenüber den Kommunen zur Veröffentlichung der Umfrage, rückwirkend betrachtet, eine direkte E-Mail an alle Kommunen durch die Erstellerin dieser Masterarbeit eventuell zu einer größeren Resonanz geführt. Diese Feststellung ergibt sich aus der gestiegenen Anzahl an Umfrageteilnehmern nach dem Versand der Erinnerungen an die Umfrage per E-Mail. Nach dem erstmaligen Hinweis auf die Umfrage hatten lediglich fünf Kommu-

nen an der Umfrage teilgenommen. Nach dem Versand der Erinnerung beteiligten sich 27 Kommunen an der Umfrage.
Damit man zukünftige identische Umfragen noch zielgerichteter aufbauen kann, hätte ebenfalls die Meinung der Umfrageteilnehmer zum Inhalt und die Struktur der Umfrage abgefragt werden können. Es empfiehlt sich, dies bei einer nochmaligen Durchführung dieser Umfrage mit aufzunehmen.

6.3 AUSBLICK

Um den aktuellen Stand der IS in den sächsischen Kommunen nochmalig abzufragen, kann diese Umfrage in den kommenden Jahren erneut durchgeführt werden. Dazu sollten jedoch die eben genannten Aspekte analysiert werden und die Umfrage in diesen Bereichen angepasst werden.
Auch ist zu untersuchen, warum die Teilnehmerresonanz bei größeren Kommunen mit mehr als 50.000 Einwohnern geringer ausgefallen ist als bei Kommunen mit weniger Einwohnern.

„Die technologischen Entwicklungen unserer Zeit sorgen für eine große Dynamik, die Staat, Wirtschaft, Gesellschaft und jeden Einzelnen gleichermaßen erfasst. Die Herausforderung ist, mit dieser Dynamik Schritt zu halten, damit sie in geordneten Bahnen sicher abläuft und allen Zielgruppen größtmöglichen Nutzen bringen kann.“[102]

„Ohne Sicherheit ist keine Freiheit.“
(Wilhelm von Humboldt)

[102] www.bundesregierung.de (2019) S. 75

QUELLENVERZEICHNIS

SELBSTÄNDIGE SCHRIFTEN

Faulbaum, F. (2019):

Faulbaum, Frank: *Methodische Grundlagen der Umfrageforschung*. 1. Auflage, Wiesbaden, Springer VS, 2019.

Hanschke, I. (2019):

Hanschke, Inge: *Informationssicherheit und Datenschutz systematisch und nachhaltig gestalten*. 1. Auflage, Wiesbaden, Springer Vieweg, 2019.

Jacob, R.; Heinz, A.; Décieux, J. P. (2013):

Jacob, Rüdiger; Heinz, Andreas; Décieux, Jean: *Umfrage – Einführung in die Methoden der Umfrageforschung*. 3. Auflage, München, Oldenburg Verlag, 2013.

Lühr, H., Jabkowski, R., Smentek, S. (2019):

Lühr, Henning; Jabkowski, Roland; Smentek, Sabine*: Handbuch Digitale Verwaltung*. 1. Auflage, Wiesbaden, Kommunal- und Schul- Verlag GmbH & Co. KG, 2019.

Müller, K.-R. (2014):

Müller, Klaus-Rainer*: IT-Sicherheit mit System – Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement – Sichere Anwendungen – Standards und Practices.* 5. Auflage, Wiesbaden, Springer Vieweg, 2014.

Schulz, T. (2020):

Schulz, Thomas*: Cyber-Sicherheit – Für vernetzte Anwendungen in der Industrie 4.0*. 1. Auflage, Würzburg, Vogel Communications Group GmbH & Co. KG, 2020.

Sowa, A. (2017):

Sowa, Aleksandra: *Management der Informationssicherheit – Kontrolle und Optimierung*. 1. Auflage, Wiesbaden, Springer Vieweg, 2017.

Weber, K., Schütz, A. E., Fertig, T. (2019):

Weber, Kerstin; Schütz, Andreas E.; Fertig, Tobias: *Grundlagen und Anwendung von Information Security Awareness - Mitarbeiter zielgerichtet für Informationssicherheit sensibilisieren.* 1. Auflage, Wiesbaden, Springer Vieweg, 2019.

Wegener, C.; Milde, T.; Dolle, W. (2016):

Wegener, Christoph; Milde, Thomas; Dolle, Wilhelm: *Informationssicherheits-Management – Leitfaden für Praktiker und Begleitbuch zur CISM-Zertifizierung*. 1. Auflage, Wiesbaden, Springer Vieweg, 2016.

INTERNET-QUELLEN

www.bsi.bund.de (o.J.a):

Bundesamt für Sicherheit in der Informationstechnik – BSI: *IT-Grundschutz.* o.J., verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzAbout/itgrundschutzAbout_node.htmll [Zugriff am 17.11.2019]

www.bsi.bund.de (o.J.b):

Bundesamt für Sicherheit in der Informationstechnik – BSI: *IT-Grundschutz Umsetzungshinweise zum Baustein ORP.3 Sensibilisierung und Schulung*. o.J., verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/ORP/Umsetzungshinweise_zum_Baustein_ORP_3_Sensibilisierung_und_Schulung.html [Zugriff am 14.11.2019]

www.bsi.bund.de (2012):

Bundesamt für Sicherheit in der Informationstechnik – BSI (Hrsg.): *Leitfaden Informationssicherheit.* Bonn 2012, verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile&v=3 [Zugriff am 17.11.2019]

www.bsi.bund.de (2017 a):

Bundesamt für Sicherheit in der Informationstechnik – BSI (Hrsg.): *BSI-Standard 200-1, Managementsysteme für Informationssicherheit (ISMS)*. Bonn 2017, verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_1.pdf?__blob=publicationFile&v=8 [Zugriff am 17.11.2019]

www.bsi.bund.de (2017 b):

Bundesamt für Sicherheit in der Informationstechnik – BSI (Hrsg.): *BSI-Standard 200-2, IT-Grundschutz-Methodik.* Bonn 2017, verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_2.pdf;jsessionid=C651C4F8D8148E24518DDAF7A26BBC73.2_cid360?__blob=publicationFile&v=7
[Zugriff am 17.11.2019]

www.buergerbeteiligung.sachsen.de (2019):

Sächsisches Staatskanzlei: *Umfrage zur Informationssicherheit in den sächsischen Kommunen – Umfrage erstellt von Ehret, Mareen.* 17.12.2019, verfügbar unter:
https://buergerbeteiligung.sachsen.de/portal/egov/beteiligung/aktuelle-themen/1018996
[Zugriff am 17.01.2020]

www.bundesregierung.de (2019):

Bundesministerium des Innern, für Bau und Heimat (Hrsg.): *Die Lage der IT-Sicherheit in Deutschland 2019.* Berlin 2019, verfügbar unter:
http://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2019.pdf?__blob=publicationFile&v=4
[Zugriff am 06.02.2020]

www.business-wissen.de (o.J.):

b-wise GmbH: *Befragung - Umfragen selbst durchführen*. o.J., verfügbar unter:
https://www.business-wissen.de/artikel/befragung-umfragen-selbst-durchfuehren/
[Zugriff am 29.01.2020]

www.egovernment.sachsen.de (o.J.):

Sächsisches Staatskanzlei: *E-Government-Basiskomponenten.* o.J., verfügbar unter:
https://www.egovernment.sachsen.de/basiskomponenten.html
[Zugriff am 22.12.2019]

www.kritis.bund.de (o.J.):

Bundesamt für Sicherheit in der Informationstechnik – BSI: *Glossar*. o.J., verfügbar unter:
https://www.kritis.bund.de/SubSites/Kritis/DE/Servicefunktionen/Glossar/Functions/glossar.html?lv3=2254842&lv2=4968594
[Zugriff am 09.02.2020]

www.lds.sachsen.de (2020):

Landesdirektion Sachsen (Hrsg.): *Gemeindeverzeichnis Stand 06.01.2020*, Dresden 2020, verfügbar unter:
https://www.lds.sachsen.de/?ID=2392&art_param=155
[Zugriff 06.01.2020]

www.lkt-sachsen.de (2020):

Sächsischer Landkreistag e.V.: *Aufgaben des Sächsischen Landkreistages*. 2020, verfügbar unter:
https://www.lkt-sachsen.de/landkreistag/content/10/05012005175246.asp
[Zugriff 01.01.2020]

www.medienservice.sachsen.de (2019):

Sächsische Staatskanzlei: *Mehr IT-Sicherheit im Verwaltungsnetz und bessere föderale IT-Kooperation.* 14.02.2019, verfügbar unter: https://medienservice.sachsen.de/medien/news/223719
[Zugriff 21.12.2019]

www.onpulson.de (o.J.b.):

Onpulson Wirtschaftslexikon: *Definition Begriff Mindmap.* o.J., verfügbar unter:
https://www.onpulson.de/lexikon/mind-map/
[Zugriff am 09.02.2020]

www.publikationen.sachsen.de (2017 a):

Sächsisches Staatsministerium des Innern (Hrsg.): *Jahresbericht Informations- und Cybersicherheit.* Dresden 2017, verfügbar unter: https://publikationen.sachsen.de/bdb/artikel/30935/documents/46324
[Zugriff am 13.08.2019]

www.publikationen.sachsen.de (2017 b):

Sächsisches Staatsministerium des Innern (Hrsg.): *Beteiligungsportal Sachsen - Gesellschaftliche Mitbestimmungsprozesse online gestalten.* Dresden 2017, verfügbar unter:
https://publikationen.sachsen.de/bdb/artikel/29834
[Zugriff am 21.12.2019]

www.ssg-sachsen.de (2014):

Sächsischer Städte- und Gemeindetag e.V.: *Satzung.* 06.11.2014, verfügbar unter:
https://www.ssg-sachsen.de/index.php?id=satzung
[Zugriff 21.12.2019]

www.statistik.sachsen.de (2019):

Statistisches Landesamt des Freistaates Sachsen (Hrsg.): *Medieninformation 127/2019 - Neues Gemeindeverzeichnis für Sachsen erschienen: 419 selbständige Gemeinden.* Dresden 2019, verfügbar unter:
https://www.statistik.sachsen.de/download/200_MI-2019/MI-127-2019.pdf
[Zugriff 21.01.2020]

www.wirtschaftslexikon.gabler.de (o.J.a.):

Gabler Wirtschaftslexikon: *Definition Begriff Schadsoftware/ Malware.* o.J., verfügbar unter:
https://wirtschaftslexikon.gabler.de/definition/malware-53410
[Zugriff am 09.02.2020]

www.wirtschaftslexikon.gabler.de (o.J.b.):

Gabler Wirtschaftslexikon: *Definition Begriff Spam/ Spam-Mails.* o.J., verfügbar unter:
https://wirtschaftslexikon.gabler.de/definition/spam-44321
[Zugriff am 09.02.2020]

VERZEICHNIS VON GESETZEN UND RECHTSVERORDNUNGEN

Sächsisches Informationssicherheitsgesetz (2019) erlassen als Artikel 1 des Gesetzes zur Neuordnung der Informationssicherheit im Freistaat Sachsen in der Fassung der Bekanntmachung vom 02. August 2019 (SächsGVBl. S. 630).

SONSTIGE QUELLEN

(FACH-)ZEITSCHRIFTEN

Behördenspiegel (2019):

Stiebel, Benjamin: Führungsaufgabe für Staat und Verwaltung - Freistaat Sachsen priorisiert die Informationssicherheit. *Sonderdruck Behördenspiegel.* (Juli 2019)

Sachsenlandkurier (2019):

Popp, Thomas: Herausforderung bei der Cyber-Abwehr und der Informationssicherheit in Staat und Verwaltung. *Sachsenlandkurier*. Nr. 4 Jg. 30 (2019)

INTERNE PRÄSENTATIONEN

www.itof2018.org (2018):

Sächsische Staatskanzlei (Hrsg.): PowerPoint-Präsentation zum *Gesetzentwurf zur Neuordnung der*
Informationssicherheit im Freistaat Sachsen. Dresden 2018, verfügbar unter https://www.itof2018.org/downloads-vortraege.html (passwortgeschützt) [Zugriff am 01.11.2018]

GLOSSAR

KRITIKALITÄT: relatives Maß für die Bedeutsamkeit einer Infrastruktur in Bezug auf die Konsequenzen, die eine Störung oder ein Funktionsausfall für die Versorgungssicherheit der Gesellschaft mit wichtigen Gütern und Dienstleistungen hat: S. 14
[Quelle: www.kritis.bund.de (o.J.)].

MINDMAP: Eine Mindmap ist ein grafisches Hilfsmittel, das zur visuellen Darstellung eingesetzt werden kann und Gedanken, Ideen und Zusammenhänge verdeutlichen soll: S. 78
[Quelle: www.onpulson.de (o.J.)].

SCHADSOFTWARE/ MALWARE: Malware (zusammengesetzt aus dem engl. malicious: bösartig und ware von Software) bezeichnet ein schädliches Programm (Schadsoftware). Dies sind Computerprogramme, die entwickelt wurden, um vom Benutzer unerwünschte bzw. schädigende Funktionen auszuführen. Der Begriff bezeichnet keine schadhafte Software, obwohl auch diese Schaden anrichten kann: S. 23, 24, 74
[Quelle: www.wirtschaftslexikon.gabler.de (o.J.a)].

SPAM/ SPAM-MAILS: E-Mail mit werblichem Inhalt, die dem Empfänger unaufgefordert zugesandt wird: S. 23, 24
[Quelle: www.wirtschaftslexikon.gabler.de (o.J.b)].

ANLAGENVERZEICHNIS

SEITE

ANLAGE 1: SCHUTZBEDARFSKATEGORIEN

[**Quelle: www.bsi.bund.de (2017 b)**]

Schutzbedarfskategorie „normal“	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen • Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung erscheint nicht möglich.
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit liegt zwischen 24 und 72 Stunden.
5. Negative Innen- oder Außenwirkung	• Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen	• Der finanzielle Schaden bleibt für die Institution tolerabel.

Schutzbedarfskategorie „hoch“	
1. Verstoß gegen Gesetze/Vorschriften/Verträge	• Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen • Vertragsverletzungen mit hohen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.

Schutzbedarfskategorie „hoch“	
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. • Die maximal tolerierbare Ausfallzeit liegt zwischen einer und 24 Stunden.
5. Negative Innen- oder Außenwirkung	• Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen	• Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.

Schutzbedarfskategorie „sehr hoch“	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Fundamentaler Verstoß gegen Vorschriften und Gesetze • Vertragsverletzungen, deren Haftungsschäden ruinös sind
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. • Gefahr für Leib und Leben
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.
5. Negative Innen- oder Außenwirkung	• Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar.
6. Finanzielle Auswirkungen	• Der finanzielle Schaden ist für die Institution existenzbedrohend.

ANLAGE 2: FRAGEBOGEN ENTWURF

[**Quelle: Eigene Darstellung]**

I N F O R M A T I O N S B L A T T

z u r U m f r a g e m i t d e m T h e m a :

Bedarfsanalyse und Konzeptentwicklung zum Aufbau und zur Weiterentwicklung der Informationssicherheit in sächsischen Kommunen

ALLGEMEINE HINWEISE ZUR DURCHFÜHRUNG DER UMFRAGE:

Sehr geehrte Teilnehmerinnen und Teilnehmer,

vielen Dank, dass Sie an der Umfrage zum Thema „Bedarfsanalyse und Konzeptentwicklung zum Aufbau und zur Weiterentwicklung der Informationssicherheit in sächsischen Kommunen“ teilnehmen.

WAS SIND DIE ZIELE UND FRAGESTELLUNGEN DIESER UMFRAGE?

Auch die sächsischen Staats- und Kommunalverwaltungen befinden sich seit einigen Jahren im Prozess einer umfassenden Digitalisierung. Zum Beispiel durch die Zunahme von IT-gestützten Vernetzungen gewinnt das Thema Informationssicherheit immer mehr an Bedeutung.
Mit Hilfe Ihrer Angaben zu der oben genannten Umfrage soll im Rahmen einer Masterarbeit an der Hochschule Meißen (FH) und Fortbildungszentrum herausgefunden werden, welche Bedarfe zu einem effektiven Aufbau bzw. zu einer Weiterentwicklung der Informationssicherheit in den sächsischen Kommunen bestehen. Gleichfalls soll betrachten werden, welcher Ausbau der Zusammenarbeit zwischen den sächsischen Kommunen und dem Freistaat Sachsen im Rahmen der Informationssicherheit hilfreich wäre.

WARUM IST DIE TEILNAHME AN DIESER UMFRAGE WICHTIG UND WELCHEN NUTZEN HAT SIE?

Durch Ihre Teilnahme an der Umfrage können der Freistaat Sachsen, insbesondere das Referat 44 (Informationssicherheit in der Staatsverwaltung, Cybersicherheit) der Sächsischen Staatskanzlei sowie die kommunalen Spitzenverbände einen Überblick darüber erhalten, welche Vorgaben und Orientierungshilfen vom Freistaat Sachsen aus Ihrer Sicht benötigt werden, damit Sie als Kommune unter Berücksichtigung der Kommunalen Selbstverwaltung beim Aufbau bzw. der Weiterentwicklung der Informationssicherheit unterstützt werden können. Im Ergebnis der Umfrage können Maßnahmen zum Schutz der IT in den sächsischen Kommunen ergriffen werden.

WELCHE DATEN WERDEN ERHOBEN?

Im Zuge der Umfrage werden allgemeine Daten (Angabe, ob Umfrageteilnehmer ein Landkreis, kreisfreie Stadt oder Gemeinde ist sowie die Einwohnerzahl) sowie Daten der Umfrage zum Thema Informationssicherheit erhoben. Alle Angaben werden vollständig **anonym** behandelt und nur zu statistischen Zwecken ausgewertet. Das heißt, dass keine Daten von Ihnen abgefragt werden, durch die man einen Rückschluss auf den Umfrageteilnehmer vornehmen kann.
Aus Gründen der Lesbarkeit wurden die Fragen in der männliche Form gestellt, nichtsdestoweniger beziehen sich die Fragen auf Angehörige beider Geschlechter.

Die Teilnahme an der Umfrage ist bis zum 14.01.2020 möglich.

Fragen zur Umfrage können Sie jederzeit an die E-Mail-Adresse

umfrage_informationssicherheit@gmx.de

senden.

Vielen Dank, dass Sie sich die Zeit nehmen. Ihre Meinung ist wichtig!

Mit freundlichen Grüßen

Mareen Ehret
Masterstudentin an der Hochschule Meißen (FH) und Fortbildungszentrum
im Studiengang Public Governance

F R A G E B O G E N

Bedarfsanalyse und Konzeptentwicklung zum Aufbau und zur Weiterentwicklung der Informationssicherheit in sächsischen Kommunen

Bitte geben Sie zuerst an, ob die Fragen zur Informationssicherheit aus der Sicht eines Landkreises, einer kreisfreien Stadt oder einer Gemeinde (bitte Eingrenzung der Einwohnerzahl beachten) in Sachsen beantwortet werden:

a) Sind Sie Landkreis, eine kreisfreie Stadt oder eine Gemeinde?

1.	**Landkreis**	☐
2.	**Kreisfreie Stadt**	☐
3.	**Gemeinde**	☐

b) Wie viel Einwohner hat Ihr Landkreis/ Ihre kreisfreie Stadt/ Ihre Gemeinde?

1.	**< 5.000 Einwohner**	☐
2.	**≥ 5.000 bis < 50.000 Einwohner**	☐
3.	**≥ 50.000 bis < 150.000 Einwohner**	☐
4.	**≥ 150.000 Einwohner**	☐

T E I L A :

Sachstand Informationssicherheit in sächsischen Kommunen

Einleitende Fragen zum ThemaInformationssicherheit:

1. Haben Sie einen Beauftragten für Informationssicherheit benannt (BfIS)?	☐ JA	☐ NEIN
2. Wie viel Budget steht Ihnen für die Informationssicherheit zur Verfügung (Schätzung)?		
3. Wie viel Mitarbeiter sind bei Ihnen im Bereich der Informationssicherheit beschäftigt *(Angabe in VBE oder Schätzung Stunden pro Jahr)*?	Schätzung Stunden pro Jahr:	
4. Haben Sie eine Cyberversicherung?	☐ JA	☐ NEIN

1. Kommunale Informationssicherheitsleitlinie

Allgemeine Erläuterung:

Die Leitlinie zur Informationssicherheit beschreibt allgemein verständlich, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der Institution hergestellt werden soll. Sie beinhaltet die von der Institution angestrebten Informationssicherheitsziele sowie die verfolgte Sicherheitsstrategie. Die Sicherheitsleitlinie beschreibt damit auch über die Sicherheitsziele das angestrebte Sicherheitsniveau in einer Behörde oder einem Unternehmen. Sie ist somit Anspruch und Aussage zugleich, dass dieses Sicherheitsniveau auf allen Ebenen der Institution erreicht werden soll.

Frage: Verfügen Sie über eine Informationssicherheitsleitlinie?
Hinweis: Mehrfachnennungen sind nicht möglich!

keine Angabe	☐
geplant	☐
in Vorbereitung	☐
in Kraft getreten	☐
Worin sehen Sie Schwierigkeiten?	
Welchen Unterstützungsbedarf haben Sie?	

2. IT-Sicherheitskonzept

Allgemeine Erläuterung:

Mit welchen Maßnahmen die in der Leitlinie zur Informationssicherheit vorgegebenen Ziele und Strategien verfolgt werden sollen, wird in einem Sicherheitskonzept beschrieben. Ein solches Sicherheitskonzept hat immer einen festgelegten Geltungsbereich. Dieser wird in der IT-Grundschutz-Methodik als Informationsverbund bezeichnet.

Frage: Verfügen Sie über ein IT-Sicherheitskonzept?
Hinweis: Mehrfachnennungen sind nicht möglich!

keine Angabe	☐	
geplant	☐	
in Vorbereitung	☐	
liegt vor	☐	
Worin sehen Sie Schwierigkeiten?		
Welchen Unterstützungsbedarf haben Sie?		
Halten Sie es für möglich mit einem Muster eines IT-Sicherheitskonzepts zu arbeiten?	☐ JA	☐ NEIN

3. Informationssicherheits-Managementsystem (ISMS)

Allgemeine Erläuterung:

Ein Managementsystem umfasst alle Regelungen, die für die Steuerung und Lenkung einer Institution sorgen und letztlich zur Zielerreichung führen sollen. Der Teil des Managementsystems, der sich mit der Informationssicherheit beschäftigt, wird als Informationssicherheitsmanagementsystem (ISMS) bezeichnet.

Das ISMS legt fest, mit welchen Instrumenten und Methoden die Leitungsebene die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt (plant, einsetzt, durchführt, überwacht und verbessert).

Zu einem ISMS gehören folgende grundlegende Komponenten:

- Managementprinzipien
- Ressourcen
- Mitarbeiter
- Sicherheitsprozess:
    - Leitlinie zur Informationssicherheit, in der die Sicherheitsziele und die Strategie zu ihrer Umsetzung dokumentiert sind
    - Sicherheitskonzept
    - Sicherheitsorganisation

Frage: Verfügen Sie über ein ISMS?
Hinweis: Mehrfachnennungen sind nicht möglich!

keine Angabe	☐
geplant	☐
in Vorbereitung	☐
etabliert	☐
Worin sehen Sie Schwierigkeiten?	
Welchen Unterstützungsbedarf haben Sie?	

Spezifische Fragestellungen:

1.	**Wird bei Ihnen der BfIS an Verwaltungsprojekten und Verwaltungsentscheidungen beteiligt?**	**systematisch beteiligt**	**sporadisch beteiligt**	**keine Beteiligung**	**Bisher kein BfIS benannt**
		☐	☐	☐	☐

2.	**Werden bei Ihnen Sicherheitschecks** (Bsp.: IT-Sicherheits-Quick-Check für kleine Kommunalverwaltungen) **zur Beurteilung der Informationssicherheit durchgeführt? ***	☐ JA *	☐ NEIN

* *<u>Wenn **Frage 2** mit „JA“ beantwortet wurde:</u>* ***a)** In welchem Umfang werden bei Ihnen Sicherheitschecks durchgeführt (kurze Beschreibung der Maßnahme)?*	
***b)** Mit welcher Häufigkeit/ Regelmäßigkeit werden bei Ihnen Sicherheitschecks durchgeführt?*	

4. Sicherheitsorganisation

Allgemeine Erläuterung:

Zur Planung und Durchsetzung eines Sicherheitsprozesses gehören die Festlegung von Organisationsstrukturen (z.B. Abteilungen, Gruppen, Kompetenzzentren) und die Definition von Rollen und Aufgaben. In Bezug auf die Aufbauorganisation des Informationssicherheitsmanagements bieten sich verschiedene Möglichkeiten an. Dabei richtet sich die personelle Ausgestaltung nach der Größe der jeweiligen Institution, den vorhandenen Ressourcen und dem angestrebten Sicherheitsniveau

Frage: Wie groß ist Ihre Sicherheitsorganisation und wie ist die organisatorische Ansiedlung des Beauftragten für Informationssicherheit (BfIS)?

1. Angabe der Größe Ihrer Sicherheitsorganisation	Angabe in Vollbeschäftigten-einheit (VBE):	Angabe in Manntage:

2. Wie ist die Tätigkeit Ihres BfIS in die Aufbau- und Ablauforganisation eingeordnet (zutreffendes bitte ankreuzen)**?**	
Bisher kein BfIS benannt	☐
Stabstelle beim Amtsleiter	☐
IT- oder Organisationsdezernat	☐
Extern	☐
eigene Angabe (bitte Anmerkung im nachfolgenden Feld vornehmen)	

5. Maßnahme zur Durchführung von Informations- und Sensibilisierungsveranstaltungen für Mitarbeiter

Allgemeine Erläuterung:

Es ist nur dann möglich, Informationssicherheit innerhalb einer Institution erfolgreich und effizient zu verwirklichen, wenn alle Mitarbeiter erkennen und akzeptieren, dass sie ein bedeutender und notwendiger Faktor für den Erfolg der Institution ist und wenn sie bereit sind, Sicherheitsmaßnahmen wirkungsvoll zu unterstützen. Hierfür müssen eine Sicherheitskultur und ein Sicherheitsbewusstsein (Awareness) aufgebaut und gepflegt werden. Mitarbeiter müssen für relevante Gefährdungen sensibilisiert werden und wissen, wie sich diese auf ihre Institution auswirken können, denn je mehr sie sich damit auskennen, desto eher akzeptieren sie entsprechende Sicherheitsmaßnahmen.

Um den Mitarbeitern das nötige Wissen zu vermitteln, sind gleichermaßen Sensibilisierungs- und Schulungsmaßnahmen erforderlich. Ziel der Sensibilisierung für Informationssicherheit ist es, die Wahrnehmung der Mitarbeiter für sicherheitskritische Situationen und ihre Auswirkungen zu schärfen. Durch Schulungen zur Informationssicherheit sollen die Mitarbeiter die notwendigen Kenntnisse und Kompetenzen für sicherheitsbewusstes Verhalten, für das private und berufliche Umfeld erwerben.

Frage: Werden Maßnahmen in Form von Informations- und Sensibilisierungsveranstaltungen für die Mitarbeiter durchgeführt?
Hinweis: Mehrfachnennungen sind nicht möglich!

keine Angabe	☐
geplant	☐
erfolgt sporadisch oder anlassbezogen	☐
erfolgt regelmäßig (mind. 1x jährlich)	☐
Worin sehen Sie Schwierigkeiten?	
Welchen Unterstützungsbedarf haben Sie?	

Ergänzung:

1.	**Wenn Maßnahmen in Form von Informations- und Sensibilisierungsveranstaltungen durch Sie geplant sind oder durchgeführt wurden, welche Zielgruppe** (z. Bsp. Behördenleitung, Sachbearbeiter oder andere) **soll oder wurde bisher damit angesprochen** (kurze Beschreibung der Zielgruppe dieser Maßnahme)**?**			
2.	**Kennen Sie das E-Learning Angebot „Informationssicherheit am Arbeitsplatz“?**	☐ JA	☐ NEIN	
	Wenn Frage 2 mit "Ja" beantwortet: Nutzen Sie das Angebot?	☐ JA	☐ NEIN	☐ NEIN, aber würde Angebot gern nutzen
3.	**Kennen Sie die Sensibilisierungsveranstaltung „INFOSIC | Die Hacker kommen“?**	☐ JA	☐ NEIN	
	Wenn Frage 3 mit "Ja" beantwortet: Nutzen Sie das Angebot?	☐ JA	☐ NEIN	☐ NEIN, aber würde Angebot gern nutzen
4.	**Kennen Sie die Sensibilisierungsveranstaltung „INFOSIC plus | IT-Sicherheit für Fortgeschrittene“?**	☐ JA	☐ NEIN	
	Wenn Frage 4 mit "Ja" beantwortet: Nutzen Sie das Angebot?	☐ JA	☐ NEIN	☐ NEIN, aber würde Angebot gern nutzen

6. Identifizierung kritischer Anwendungen

Frage: Haben Sie in Ihrer Kommune besonders schützenswerte Anwendungen identifiziert?:
Hinweis: Mehrfachnennungen sind nicht möglich!

keine Angabe	☐
geplant	☐
in Vorbereitung	☐
teilweise erfolgt	☐
vollständig abgeschlossen, aber die Schutzbedarfe wurden noch nicht festgelegt	☐
vollständig abgeschlossen und die Schutzbedarfe hinsichtlich der Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) wurden festgelegt	☐
Worin sehen Sie Schwierigkeiten?	
Welchen Unterstützungsbedarf haben Sie?	

7. Organisatorische Maßnahmen für IT-Sicherheitsvorfälle

Allgemeine Erläuterung:

Neben technischen Sicherheitsmaßnahmen müssen auch organisatorische Abläufe und Prozesse (wie Benutzerrichtlinien, Rechtevergaben, Sicherheitsschulungen, Test- und Freigabeverfahren) eingerichtet werden.

Was ist für Sie ein IT-Sicherheitsvorfall?	

Frage: Wurden organisatorische Maßnahmen für IT-Sicherheitsvorfälle festgelegt?
Hinweis: Mehrfachnennungen sind nicht möglich!

keine Angabe	☐
geplant	☐
in Vorbereitung	☐
festgelegt	☐
Worin sehen Sie Schwierigkeiten?	
Welchen Unterstützungsbedarf haben Sie?	

Ergänzung:

1.	**Gibt es bei Ihnen vorgeschriebene Abläufe bei IT-Sicherheitsvorfällen z. Bsp. durch einen Angriff auf Ihre IT durch Schadsoftware?**	☐ JA	☐ NEIN
2.	**Haben Sie schon einmal einen IT-Sicherheitsvorfall dem "Computer Emergency Response Team" (SAX.CERT) der Landesverwaltung des Freistaates gemeldet?**	☐ JA	☐ NEIN

TEIL B: Gewünschte Unterstützung

In diesem Abschnitt der Umfrage erhalten Sie die Möglichkeit, dem Referat 44 (Informationssicherheit in der Staatsverwaltung, Cybersicherheit) der Sächsischen Staatskanzlei einen Überblick darüber zu geben, welche Unterstützung Sie sich zum Aufbau und zur Weiterentwicklung der Informationssicherheit vorstellen könnten bzw. Ihnen hilfreich wären. Dazu kreuzen Sie bitte die nachfolgend genannten für Sie wichtigsten Unterstützungsmöglichkeiten an.

Mehrfachnennungen sind möglich!

Die folgende Übersicht ist nicht abschließend. Daher nutzen Sie auch gern die Textfelder am Ende dieses Abschnittes der Umfrage und tragen vorhergehend nicht bereits genannte Unterstützungsmöglichkeiten ein.

Es besteht Bedarf an nachfolgend angekreuzten gewünschten Möglichkeiten zur Unterstützung der sächsischen Kommunen durch den Freistaat Sachsen:

1.	**Checklisten**	☐
2.	**Informationsbroschüren**	☐
3.	**Informationen zu IT-Sicherheitsbedrohungen**	☐
4.	**Seminare / Workshops**	☐
5.	**Sensibilisierungsveranstaltungen**	☐
6.	**Allgemeine Informationsveranstaltungen**	☐
7.	**Hilfestellung im Schadensfall durch persönliche Anleitung zur Schadensregulierung**	☐

Weitere Arten von Unterstützungen, die vorhergehend nicht aufgeführt sind, bitte hier eintragen:

8.
9.
10.
11.
12.

Angabe der Themen, wenn Unterstützung gewünscht wird (bitte benennen Sie die jeweilige Unterstützungsart und benennen dann das Thema):

13.
14.
15.
16.
17.

TEIL C: Hemmnisse

In diesem Abschnitt der Umfrage erhalten Sie die Möglichkeit, dem Referat 44 (Informationssicherheit in der Staatsverwaltung, Cybersicherheit) der Sächsischen Staatskanzlei einen Überblick darüber zu geben, welche Hemmnisse Sie für den Aufbau einer systematischen Informationssicherheit in Ihrer Kommune sehen. Dazu kreuzen Sie bitte die nachfolgend genannten für Sie relevantesten Hemmnisse an.

Mehrfachnennungen sind möglich!

Die folgende Übersicht ist nicht abschließend. Daher nutzen Sie auch gern die Textfelder am Ende dieses Abschnittes der Umfrage und tragen vorhergehend nicht bereits genannte Hemmnisse ein.

Folgende Hemmnisse zum Aufbau einer systematischen Informationssicherheit liegen in der an der Umfrage teilnehmenden Kommune vor:

1.	**Interne organisatorische Probleme**	☐
2.	**Unzureichende Unterstützung der Behördenleitung**	☐
3.	**Mangelnde Akzeptanz der Mitarbeiter**	☐
4.	**Probleme der Steuerung von externen Dienstleistern z. Bsp. bei Outsourcing** (Probleme in der Zusammenarbeit mit externen Dienstleistern im Rahmen der Informationssicherheit)	☐
5.	**Fehlendes Personal**	☐
6.	**Geringes Budget**	☐

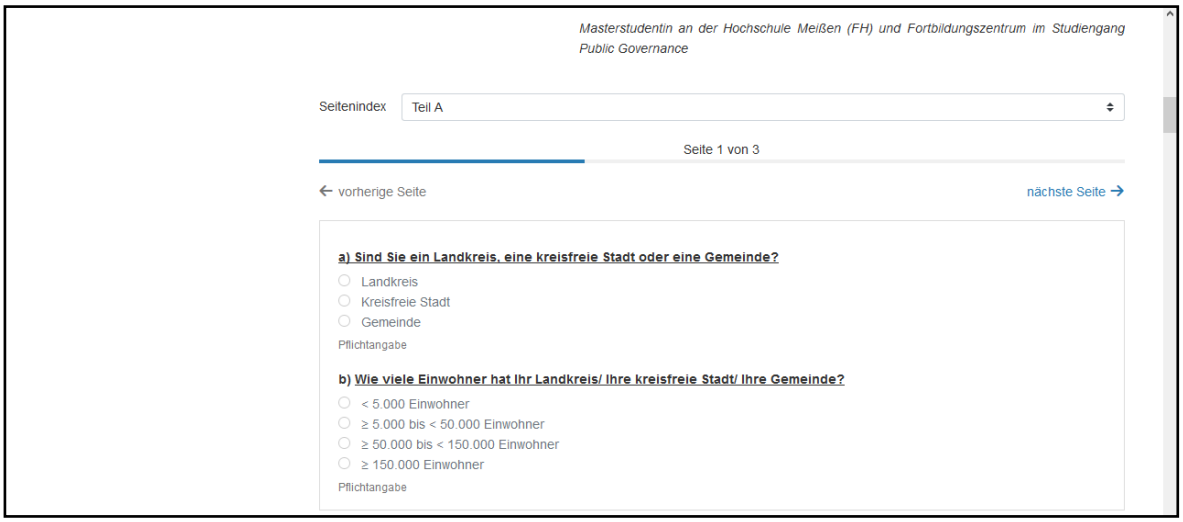
Weitere Hemmnisse, die vorhergehend nicht aufgeführt sind, bitte hier eintragen:

7.	
8.	
9.	

Quellen der allgemeinen Erläuterungen zu den einzelnen Fragen dieser Umfrage sind die Standards des Bundesamt für Sicherheit in der Informationstechnik (Link: www.bsi.bund.de)

ANLAGE 3: DARSTELLUNG FRAGEBOGEN IM BETEILIGUNGSPORTAL

[**Quelle: Eigene Darstellung siehe Quelle www.buergerbeteiligung.sachsen.de (2019)]**



Teil A – Sachstand Informationssicherheit in sächsischen Kommunen

Haben Sie einen Beauftragten für Informationssicherheit benannt (BfIS)?

○ Ja ○ Nein

Pflichtangabe

Wie viel Budget steht Ihnen pro Jahr für die Informationssicherheit zur Verfügung (Schätzung)?

Datenformat: Ganzzahl

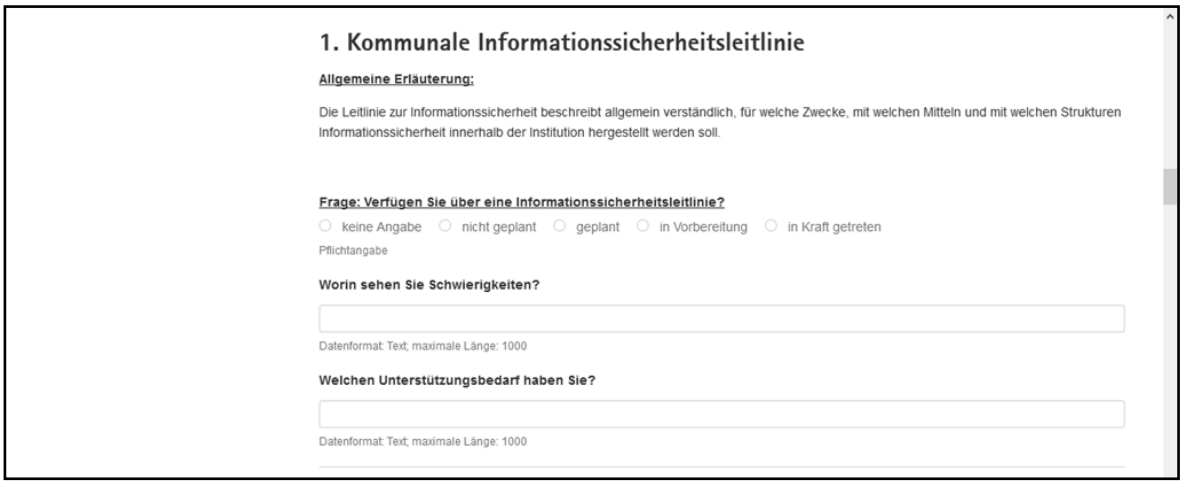
Wie viele Mitarbeiter sind bei Ihnen im Bereich der Informationssicherheit beschäftigt (Angabe Schätzung Stunden pro Jahr)?

Datenformat: Ganzzahl | Angabe Schätzung Stunden pro Jahr

Haben Sie eine Cyberversicherung?

○ Ja ○ Nein ○ keine Angabe

Pflichtangabe



1. Kommunale Informationssicherheitsleitlinie

Allgemeine Erläuterung:

Die Leitlinie zur Informationssicherheit beschreibt allgemein verständlich, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der Institution hergestellt werden soll.

Frage: Verfügen Sie über eine Informationssicherheitsleitlinie?

○ keine Angabe ○ nicht geplant ○ geplant ○ in Vorbereitung ○ in Kraft getreten

Pflichtangabe

Worin sehen Sie Schwierigkeiten?

Datenformat: Text; maximale Länge: 1000

Welchen Unterstützungsbedarf haben Sie?

Datenformat: Text; maximale Länge: 1000

2. IT-Sicherheitskonzept

Allgemeine Erläuterung:

In einem IT-Sicherheitskonzept wird beschrieben, mit welchen Maßnahmen die in der Leitlinie zur Informationssicherheit vorgegebenen Ziele und Strategien verfolgt werden sollen.

Frage: Verfügen Sie über ein IT-Sicherheitskonzept?

○ keine Angabe ○ nicht geplant ○ geplant ○ in Vorbereitung ○ liegt vor

Pflichtangabe

Worin sehen Sie Schwierigkeiten?

Datenformat: Text; maximale Länge: 1000

Welchen Unterstützungsbedarf haben Sie?

Datenformat: Text; maximale Länge: 1000

Halten Sie es für möglich mit einem Muster eines IT-Sicherheitskonzeptes zu arbeiten?

○ Ja ○ Nein ○ keine Angabe

Pflichtangabe

3. Informationssicherheits-Managementsystem (ISMS)

Allgemeine Erläuterung:

Ein Managementsystem umfasst alle Regelungen, die für die Steuerung und Lenkung einer Institution sorgen und letztlich zur Zielerreichung führen sollen. Der Teil des Managementsystems, der sich mit der Informationssicherheit beschäftigt, wird als Informationssicherheitsmanagementsystem (ISMS) bezeichnet.

Das ISMS legt fest, mit welchen Instrumenten und Methoden die Leitungsebene die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt (plant, einsetzt, durchführt, überwacht und verbessert).

Frage: Verfügen Sie über ein ISMS?

○ keine Angabe ○ nicht geplant ○ geplant ○ in Vorbereitung ○ etabliert

Pflichtangabe

Worin sehen Sie Schwierigkeiten?

Datenformat: Text; maximale Länge: 1000

Welchen Unterstützungsbedarf haben Sie?

Datenformat: Text; maximale Länge: 1000

Spezifische Fragestellungen:

	systematisch beteiligt	sporadisch beteiligt	keine Beteiligung	bisher kein BfIS ernannt	keine Angabe
1. Wird bei Ihnen der BfIS an Verwaltungsprojekten und Verwaltungsentscheidungen beteiligt?	○	○	○	○	○

Pflichtangabe

2. Werden bei Ihnen Sicherheitschecks (Bsp.: IT-Sicherheits-Quick-Check für kleine Kommunalverwaltungen) zur Beurteilung der Informationssicherheit durchgeführt?

○ Ja ○ Nein ○ keine Angabe

Pflichtangabe

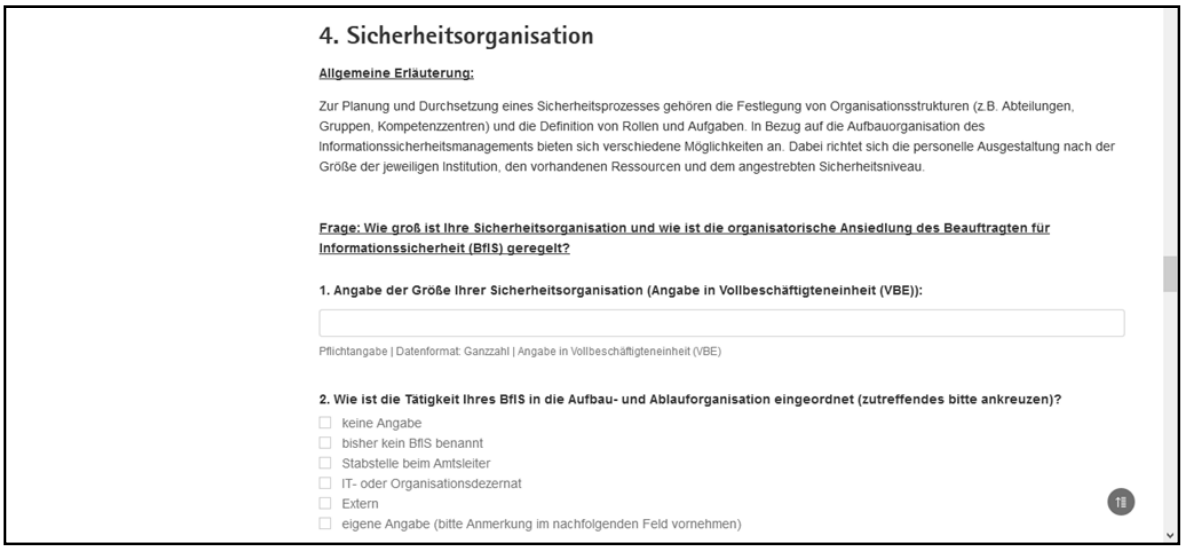
Wenn Sie die Frage 2 mit "Ja" beantwortet haben:

a) In welchem Umfang werden bei Ihnen Sicherheitschecks durchgeführt (kurze Beschreibung der Maßnahme)?

Datenformat: Text; maximale Länge: 2000

b) Mit welcher Häufigkeit/ Regelmäßigkeit werden bei Ihnen Sicherheitschecks durchgeführt?

Datenformat: Text; maximale Länge: 2000



4. Sicherheitsorganisation

Allgemeine Erläuterung:

Zur Planung und Durchsetzung eines Sicherheitsprozesses gehören die Festlegung von Organisationsstrukturen (z.B. Abteilungen, Gruppen, Kompetenzzentren) und die Definition von Rollen und Aufgaben. In Bezug auf die Aufbauorganisation des Informationssicherheitsmanagements bieten sich verschiedene Möglichkeiten an. Dabei richtet sich die personelle Ausgestaltung nach der Größe der jeweiligen Institution, den vorhandenen Ressourcen und dem angestrebten Sicherheitsniveau.

Frage: Wie groß ist Ihre Sicherheitsorganisation und wie ist die organisatorische Ansiedlung des Beauftragten für Informationssicherheit (BfIS) geregelt?

1. Angabe der Größe Ihrer Sicherheitsorganisation (Angabe in Vollbeschäftigteneinheit (VBE)):

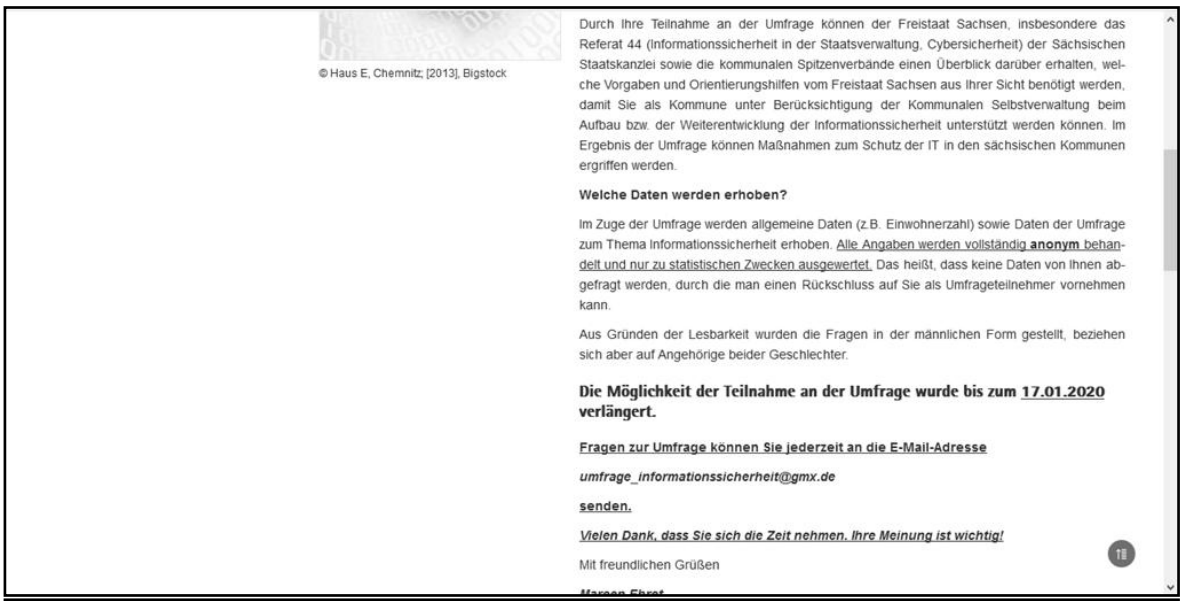
Pflichtangabe | Datenformat: Ganzzahl | Angabe in Vollbeschäftigteneinheit (VBE)

2. Wie ist die Tätigkeit Ihres BfIS in die Aufbau- und Ablauforganisation eingeordnet (zutreffendes bitte ankreuzen)?

- ☐ keine Angabe
- ☐ bisher kein BfIS benannt
- ☐ Stabstelle beim Amtsleiter
- ☐ IT- oder Organisationsdezernat
- ☐ Extern
- ☐ eigene Angabe (bitte Anmerkung im nachfolgenden Feld vornehmen)

Eigene Angabe:

Datenformat: Text; maximale Länge: 1000



© Haus E, Chemnitz; [2013], Bigstock

Durch Ihre Teilnahme an der Umfrage können der Freistaat Sachsen, insbesondere das Referat 44 (Informationssicherheit in der Staatsverwaltung, Cybersicherheit) der Sächsischen Staatskanzlei sowie die kommunalen Spitzenverbände einen Überblick darüber erhalten, welche Vorgaben und Orientierungshilfen vom Freistaat Sachsen aus Ihrer Sicht benötigt werden, damit Sie als Kommune unter Berücksichtigung der Kommunalen Selbstverwaltung beim Aufbau bzw. der Weiterentwicklung der Informationssicherheit unterstützt werden können. Im Ergebnis der Umfrage können Maßnahmen zum Schutz der IT in den sächsischen Kommunen ergriffen werden.

Welche Daten werden erhoben?

Im Zuge der Umfrage werden allgemeine Daten (z.B. Einwohnerzahl) sowie Daten der Umfrage zum Thema Informationssicherheit erhoben. Alle Angaben werden vollständig **anonym** behandelt und nur zu statistischen Zwecken ausgewertet. Das heißt, dass keine Daten von Ihnen abgefragt werden, durch die man einen Rückschluss auf Sie als Umfrageteilnehmer vornehmen kann.

Aus Gründen der Lesbarkeit wurden die Fragen in der männlichen Form gestellt, beziehen sich aber auf Angehörige beider Geschlechter.

Die Möglichkeit der Teilnahme an der Umfrage wurde bis zum 17.01.2020 verlängert.

Fragen zur Umfrage können Sie jederzeit an die E-Mail-Adresse

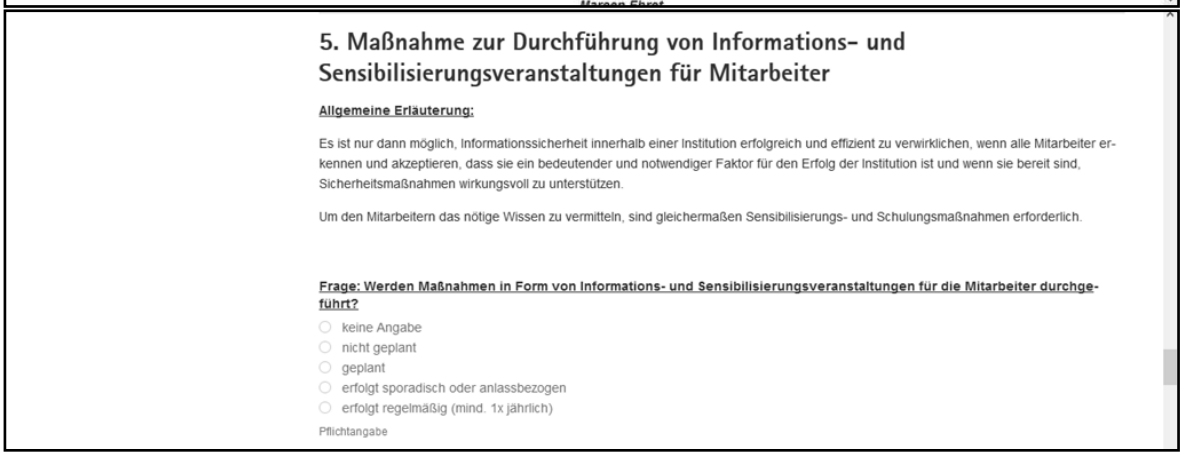
umfrage_informationssicherheit@gmx.de

senden.

Vielen Dank, dass Sie sich die Zeit nehmen. Ihre Meinung ist wichtig!

Mit freundlichen Grüßen

Maren Ehret



5. Maßnahme zur Durchführung von Informations- und Sensibilisierungsveranstaltungen für Mitarbeiter

Allgemeine Erläuterung:

Es ist nur dann möglich, Informationssicherheit innerhalb einer Institution erfolgreich und effizient zu verwirklichen, wenn alle Mitarbeiter erkennen und akzeptieren, dass sie ein bedeutender und notwendiger Faktor für den Erfolg der Institution ist und wenn sie bereit sind, Sicherheitsmaßnahmen wirkungsvoll zu unterstützen.

Um den Mitarbeitern das nötige Wissen zu vermitteln, sind gleichermaßen Sensibilisierungs- und Schulungsmaßnahmen erforderlich.

Frage: Werden Maßnahmen in Form von Informations- und Sensibilisierungsveranstaltungen für die Mitarbeiter durchgeführt?

- ○ keine Angabe
- ○ nicht geplant
- ○ geplant
- ○ erfolgt sporadisch oder anlassbezogen
- ○ erfolgt regelmäßig (mind. 1x jährlich)

Pflichtangabe

Worin sehen Sie Schwierigkeiten?

Datenformat: Text; maximale Länge: 1000

Welchen Unterstützungsbedarf haben Sie?

Datenformat: Text; maximale Länge: 1000

Ergänzung:

1. Wenn Maßnahmen in Form von Informations- und Sensibilisierungsveranstaltungen durch Sie geplant sind oder durchgeführt wurden, welche Zielgruppe (z. Bsp. Behördenleitung, Sachbearbeiter oder andere) soll oder wurde bisher damit angesprochen (kurze Beschreibung der Zielgruppe dieser Maßnahme)?

Datenformat: Text; maximale Länge: 2000

2. Kennen Sie das E-Learning Angebot „Informationssicherheit am Arbeitsplatz“?

○ Ja ○ Nein

Pflichtangabe

2.1 Zusatz Frage 2: Nutzen Sie das Angebot bzw. würden Sie das Angebot gern nutzen?

- ○ Ja
- ○ Nein
- ○ Nein, aber würde Angebot gern nutzen

3. Kennen Sie die Sensibilisierungsveranstaltung „INFOSIC | Die Hacker kommen“?

- ○ Ja ○ Nein

Pflichtangabe

3.1 Zusatz Frage 3: Nutzen Sie das Angebot bzw. würden Sie das Angebot gern nutzen?

- ○ Ja
- ○ Nein
- ○ Nein, aber würde Angebot gern nutzen

4. Kennen Sie die Sensibilisierungsveranstaltung „INFOSIC plus | IT-Sicherheit für Fortgeschrittene“?

- ○ Ja ○ Nein

Pflichtangabe

4.1 Zusatz Frage 4: Nutzen Sie das Angebot bzw. würden Sie das Angebot gern nutzen?

- ○ Ja
- ○ Nein
- ○ Nein, aber würde Angebot gern nutzen

6. Identifizierung schützenswerter Anwendungen

Frage: Haben Sie in Ihrer Kommune besonders schützenswerte Anwendungen identifiziert?

- ○ keine Angabe
- ○ nicht geplant
- ○ ist geplant
- ○ in Vorbereitung
- ○ teilweise erfolgt
- ○ vollständig abgeschlossen, aber die Schutzbedarfe wurden noch nicht festgelegt
- ○ vollständig abgeschlossen und die Schutzbedarfe hinsichtlich der Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) wurden festgelegt

Pflichtangabe

Worin sehen Sie Schwierigkeiten?

Datenformat: Text; maximale Länge: 1000

Welchen Unterstützungsbedarf haben Sie?

Datenformat: Text; maximale Länge: 1000

7. Organisatorische Maßnahmen für IT Sicherheitsvorfälle

Allgemeine Erläuterung:

Neben technischen Sicherheitsmaßnahmen müssen auch organisatorische Abläufe und Prozesse (wie Benutzerrichtlinien, Rechtevergaben, Sicherheitsschulungen, Test- und Freigabeverfahren) eingerichtet werden.

Was ist für Sie ein IT-Sicherheitsvorfall?

Datenformat: Text; maximale Länge: 4000

Frage: Wurden organisatorische Maßnahmen für IT-Sicherheitsvorfälle festgelegt?

- ○ keine Angabe
- ○ nicht geplant
- ○ geplant
- ○ in Vorbereitung
- ○ festgelegt

Pflichtangabe

Worin sehen Sie Schwierigkeiten?

Datenformat: Text; maximale Länge: 1000

Welchen Unterstützungsbedarf haben Sie?

Datenformat: Text; maximale Länge: 1000

Ergänzung:

1. Gibt es bei Ihnen vorgeschriebene Abläufe bei IT-Sicherheitsvorfällen z. Bsp. durch einen Angriff auf Ihre IT durch Schadsoftware?

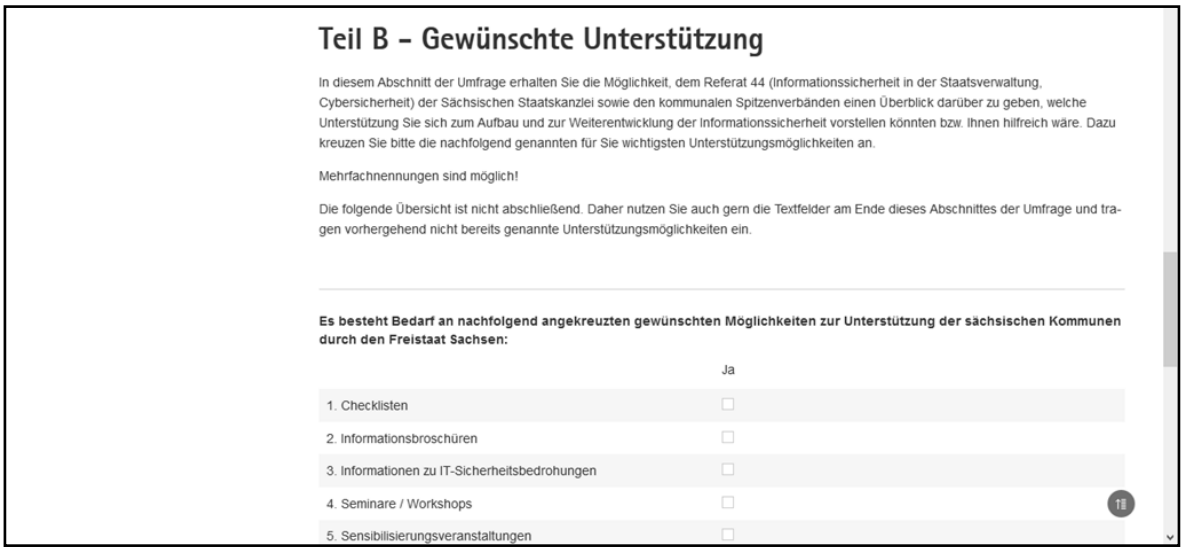
- Ja
- Nein
- keine Angabe

Pflichtangabe

2. Haben Sie schon einmal einen IT-Sicherheitsvorfall dem "Computer Emergency Response Team" (SAX.CERT) der Landesverwaltung des Freistaates gemeldet?

- Ja
- Nein
- keine Angabe

Pflichtangabe



Teil B – Gewünschte Unterstützung

In diesem Abschnitt der Umfrage erhalten Sie die Möglichkeit, dem Referat 44 (Informationssicherheit in der Staatsverwaltung, Cybersicherheit) der Sächsischen Staatskanzlei sowie den kommunalen Spitzenverbänden einen Überblick darüber zu geben, welche Unterstützung Sie sich zum Aufbau und zur Weiterentwicklung der Informationssicherheit vorstellen könnten bzw. Ihnen hilfreich wäre. Dazu kreuzen Sie bitte die nachfolgend genannten für Sie wichtigsten Unterstützungsmöglichkeiten an.

Mehrfachnennungen sind möglich!

Die folgende Übersicht ist nicht abschließend. Daher nutzen Sie auch gern die Textfelder am Ende dieses Abschnittes der Umfrage und tragen vorhergehend nicht bereits genannte Unterstützungsmöglichkeiten ein.

Es besteht Bedarf an nachfolgend angekreuzten gewünschten Möglichkeiten zur Unterstützung der sächsischen Kommunen durch den Freistaat Sachsen:

	Ja
1. Checklisten	☐
2. Informationsbroschüren	☐
3. Informationen zu IT-Sicherheitsbedrohungen	☐
4. Seminare / Workshops	☐
5. Sensibilisierungsveranstaltungen	☐

6. Allgemeine Informationsveranstaltungen	☐
7. Hilfestellung im Schadensfall durch persönliche Anleitung zur Schadensregulierung	☐
8. Keine Unterstützung gewünscht	☐

Weitere Arten von Unterstützungen, die vorhergehend nicht aufgeführt sind, bitte hier eintragen:

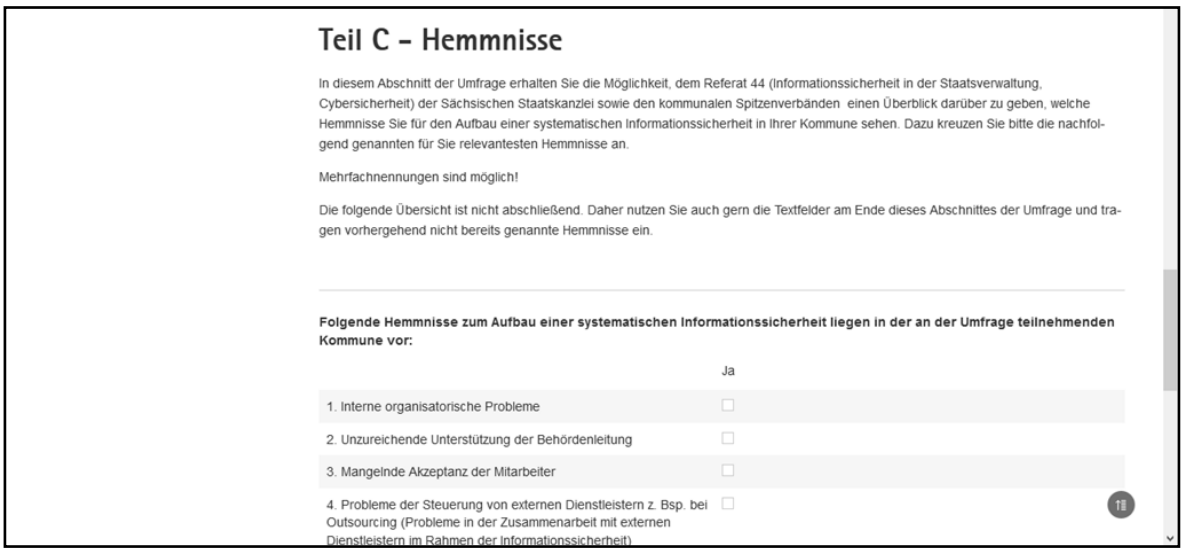
Datenformat: Text; maximale Länge: 4000

Angabe der Themen, wenn Unterstützung gewünscht wird (bitte benennen Sie die jeweilige Unterstützungsart und benennen dann das Thema):

Datenformat: Text; maximale Länge: 4000

← vorherige Seite

nächste Seite →



Teil C – Hemmnisse

In diesem Abschnitt der Umfrage erhalten Sie die Möglichkeit, dem Referat 44 (Informationssicherheit in der Staatsverwaltung, Cybersicherheit) der Sächsischen Staatskanzlei sowie den kommunalen Spitzenverbänden einen Überblick darüber zu geben, welche Hemmnisse Sie für den Aufbau einer systematischen Informationssicherheit in Ihrer Kommune sehen. Dazu kreuzen Sie bitte die nachfolgend genannten für Sie relevantesten Hemmnisse an.

Mehrfachnennungen sind möglich!

Die folgende Übersicht ist nicht abschließend. Daher nutzen Sie auch gern die Textfelder am Ende dieses Abschnittes der Umfrage und tragen vorhergehend nicht bereits genannte Hemmnisse ein.

Folgende Hemmnisse zum Aufbau einer systematischen Informationssicherheit liegen in der an der Umfrage teilnehmenden Kommune vor:

	Ja
1. Interne organisatorische Probleme	☐
2. Unzureichende Unterstützung der Behördenleitung	☐
3. Mangelnde Akzeptanz der Mitarbeiter	☐
4. Probleme der Steuerung von externen Dienstleistern z. Bsp. bei Outsourcing (Probleme in der Zusammenarbeit mit externen Dienstleistern im Rahmen der Informationssicherheit)	☐

5. Fehlendes Personal	☐
6. Geringes Budget	☐
7. Es bestehen keine Hemnisse	☐

Weitere Hemmnisse, die vorhergehend nicht aufgeführt sind, bitte hier eintragen:

Datenformat: Text; maximale Länge: 4000

← vorherige Seite

nächste Seite →

ANLAGE 4: UMFRAGEERGEBNISSE

[**Quelle: Eigene Darstellung siehe Quelle www.buergerbeteiligung.sachsen.de (2019)]**

Einleitende Fragen:

Teil A								
ID	Ersteller	Eingegangen am	a) Sind Sie ein Landkreis, eine kreisfreie Stadt oder eine Gemeinde? (Einfachauswahl)	b) Wie viele Einwohner hat Ihr Landkreis/ Ihre kreisfreie Stadt/ Ihre Gemeinde? (Einfachauswahl)	Haben Sie einen Beauftragten für Informationssicherheit benannt (BfIS)? (Einfachauswahl)	Wie viel Budget steht Ihnen pro Jahr für die Informationssicherheit zur Verfügung (Schätzung)? (Offene Frage)	Wie viele Mitarbeiter sind bei Ihnen im Bereich der Informationssicherheit beschäftigt (Angabe Schätzung Stunden pro Jahr)? (Offene Frage)	Haben Sie eine Cyberversicherung? (Einfachauswahl)
1248349	Anonym	17.12.2019 10:48	Gemeinde	≥ 5.000 bis < 50.000 Einwohner	Nein	2000	3	Nein
1248913	Anonym	19.12.2019 09:01	Gemeinde	≥ 5.000 bis < 50.000 Einwohner	Nein	0	110	Nein
1248961	Anonym	19.12.2019 11:51	Landkreis	≥ 150.000 Einwohner	Ja			Nein
1248972	Anonym	19.12.2019 12:53	Landkreis	≥ 150.000 Einwohner	Ja		2000	Nein
1251675	Anonym	02.01.2020 22:53	Landkreis	≥ 150.000 Einwohner	Ja	25000	200	Nein
1252728	Anonym	06.01.2020 13:17	Gemeinde	< 5.000 Einwohner	Ja	2500	0	Nein
1252802	Anonym	06.01.2020 15:10	Landkreis	≥ 150.000 Einwohner	Ja	20000	3000	Nein
1253140	Anonym	07.01.2020 17:07	Gemeinde	≥ 50.000 bis < 150.000 Einwohner	Nein	0	0	Nein
1253319	Anonym	08.01.2020 09:32	Gemeinde	≥ 5.000 bis < 50.000 Einwohner	Nein			Nein
1253382	Anonym	08.01.2020 11:56	Landkreis	≥ 150.000 Einwohner	Ja		1	Nein
1253688	Anonym	09.01.2020 08:11	Gemeinde	< 5.000 Einwohner	Ja	6000	40	Nein
1253700	Anonym	09.01.2020 08:28	Gemeinde	≥ 5.000 bis < 50.000 Einwohner	Nein	0	50	Nein
1253702	Anonym	09.01.2020 08:48	Gemeinde	< 5.000 Einwohner	Nein	500	20	Nein
1253720	Anonym	09.01.2020 08:35	Gemeinde	≥ 5.000 bis < 50.000 Einwohner	Ja	10000	80	Ja
1253737	Anonym	09.01.2020 10:10	Gemeinde	< 5.000 Einwohner	Ja	5000	50	Nein
1253770	Anonym	09.01.2020 11:07	Gemeinde	< 5.000 Einwohner	Nein	100	20	Nein
1253772	Anonym	09.01.2020 11:34	Gemeinde	≥ 5.000 bis < 50.000 Einwohner	Ja	10000	120	Ja
1253793	Anonym	09.01.2020 11:33	Gemeinde	< 5.000 Einwohner	Nein	0	0	Nein
1253818	Anonym	09.01.2020 14:14	Gemeinde	≥ 5.000 bis < 50.000 Einwohner	Nein			Nein
1253824	Anonym	09.01.2020 14:30	Gemeinde	< 5.000 Einwohner	Nein	1500	24	Nein
1254058	Anonym	10.01.2020 08:32	Gemeinde	≥ 5.000 bis < 50.000 Einwohner	Ja	10000	300	Nein
1254067	Anonym	10.01.2020 10:22	Gemeinde	< 5.000 Einwohner	Nein	0	0	Nein
1254079	Anonym	10.01.2020 08:51	Gemeinde	≥ 5.000 bis < 50.000 Einwohner	Ja	500	20	Ja
1254144	Anonym	10.01.2020 12:33	Landkreis	≥ 150.000 Einwohner	Ja	1000	800	Nein
1254815	Anonym	13.01.2020 09:14	Gemeinde	≥ 5.000 bis < 50.000 Einwohner	Ja	10000	416	Ja
1254840	Anonym	13.01.2020 10:53	Gemeinde	< 5.000 Einwohner	Nein			Ja
1254898	Anonym	13.01.2020 13:41	Gemeinde	< 5.000 Einwohner	Nein	5000	50	Ja
1254905	Anonym	13.01.2020 14:01	Gemeinde	≥ 5.000 bis < 50.000 Einwohner	Nein			Ja
1255026	Anonym	13.01.2020 22:58	Gemeinde	≥ 5.000 bis < 50.000 Einwohner	Ja	7000	10	Nein
1255110	Anonym	14.01.2020 10:39	Gemeinde	≥ 5.000 bis < 50.000 Einwohner	Nein	0	0	Ja
1255149	Anonym	14.01.2020 14:12	Gemeinde	< 5.000 Einwohner	Nein	3000	1	Ja
1256539	Anonym	20.01.2020 17:01	Landkreis	≥ 150.000 Einwohner	Ja		1500	keine Angabe

Frage 1: Kommunale Informationssicherheitsleitlinie

Teil A					
ID	Ersteller	Eingegangen am	Frage: Verfügen Sie über eine Informationssicherheitsleitlinie? (Einfachauswahl)	Worin sehen Sie Schwierigkeiten? (Offene Frage)	Welchen Unterstützungsbedarf haben Sie? (Offene Frage)
1248349	Anonym	17.12.2019 10:48	geplant		
1248913	Anonym	19.12.2019 09:01	in Vorbereitung	Zu wenig Knowhow vor Ort, zu wenig finanzielle Mittel, zu wenig Informationsfluss von oben nach unten, Am Beispiel der DSGVO des Landes Hessen orientieren	Grundkonzepte, konkrete Ansprechpartner beim Land, welche Informationen bzw. Inhalte sind wichtig, Information der Bürgermeister für besseres Verständnis und dadurch größere Unterstützung
1248961	Anonym	19.12.2019 11:51	in Kraft getreten		
1248972	Anonym	19.12.2019 12:53	in Kraft getreten		
1251675	Anonym	02.01.2020 22:53	in Kraft getreten		
1252728	Anonym	06.01.2020 13:17	in Kraft getreten		
1252802	Anonym	06.01.2020 15:10	in Kraft getreten	keine Angabe	z.B. Sensibilisierung der Führungskräfte
1253140	Anonym	07.01.2020 17:07	in Kraft getreten	wird von den wenigsten gelesen, verstanden oder gar in Handeln umgesetzt, denken, das ist nur was für´s FG IT	Dienststellenleiter, externen Sicherheitsbeauftragen, z.B. neue Funktion in RPA der Landkreise
1253319	Anonym	08.01.2020 09:32	nicht geplant	Versändnis für das Gesetz und die Umsetzung dessen, Fachpersonal wird benötigt	
1253382	Anonym	08.01.2020 11:56	in Kraft getreten		
1253688	Anonym	09.01.2020 08:11	in Vorbereitung	Zeitfaktor	ext. DSB=IT-Sicherheitsbeauftrtagter ist tätig, aber Abstimmungsprozesse IN der Verwaltung kann dieser nicht lösen - somit das eigene Zeitbudget
1253700	Anonym	09.01.2020 08:28	geplant	notwendiges Fachwissen, zeitliche Einordnung	Checkliste, Vorbereitung zur Aufgabenerfüllung
1253702	Anonym	09.01.2020 08:48	keine Angabe	finanzielle Ausstattung	ausreichende Finanzausstattung der Kommune
1253720	Anonym	09.01.2020 08:35	in Kraft getreten		
1253737	Anonym	09.01.2020 10:10	geplant	Umfang und Detailgrad / Tiefe der Regelung	Mustertexte bzw. Handreichung soweit möglich
1253770	Anonym	09.01.2020 11:07	in Kraft getreten	muss überarbeitet werden	Musterrichtlinie
1253772	Anonym	09.01.2020 11:34	in Kraft getreten	Bürokratische Hürden	
1253793	Anonym	09.01.2020 11:33	geplant	Neben all den anderen Herausforderungen Datenschutz, Umsatzsteuer für Kommunen, E-Rechnung mit gleichem Personalbestand diese Aufgaben zu bewältigen	Vor allem fachlicher Art, aber auch monetärer Art um Dienstleister für die Aufgaben hinzuziehen zu können.
1253818	Anonym	09.01.2020 14:14	keine Angabe		
1253824	Anonym	09.01.2020 14:30	geplant	fehlendes Rundumwissen	kommunale Schulung
1254058	Anonym	10.01.2020 08:32	in Kraft getreten	kurzfristige Reaktion auf Entwicklung und Umsetzung der Richtlinien und gesetzl. Anforderungen (kleine Kommune mit wenig Personal und Budget)	KISA und privater Dienstleister
1254067	Anonym	10.01.2020 10:22	keine Angabe	keine Finanzen, kein Personal	Finanzen, Stellenplan oder finanzierbarer Dienstleister
1254079	Anonym	10.01.2020 08:51	geplant	Abstimmungsprobleme	
1254144	Anonym	10.01.2020 12:33	in Kraft getreten		
1254815	Anonym	13.01.2020 09:14	in Kraft getreten	Anpassung der Compliance an DSGVO	Beadrf an Mustern / Vorlagen angepasst an DSGVO
1254840	Anonym	13.01.2020 10:53	geplant		
1254898	Anonym	13.01.2020 13:41	in Vorbereitung	fachliche Formulierungen	externen Beratungsbedarf
1254905	Anonym	13.01.2020 14:01	geplant		
1255026	Anonym	13.01.2020 22:58	in Kraft getreten	Keine	Keinen
1255110	Anonym	14.01.2020 10:39	geplant	keine Mitarbeiter verfügbar, entsprechende Qualifikationen fehlen	Vermittlung Knowhow / Finanzierung externer Leistungen
1255149	Anonym	14.01.2020 14:12	keine Angabe	Wussten bis eben nicht, dass es eine Informationssicherheitsleitlinie gibt; werden uns damit beschäftigen, aber das Budget ist gering und personell haben wir nur begrenzte Möglichkeiten	Beratung, Unterstützung, was alles gebraucht wird, aber nicht von teuren Beratungsunternehmen, die sich eine goldene Nase daran verdienen, da nach oben hin keine Grenzen sind
1256539	Anonym	20.01.2020 17:01	in Kraft getreten	Durchsetzung - Zeitbudget	

Frage 2: IT-Sicherheitskonzept

Teil A						
ID	Ersteller	Eingegangen am	Frage: Verfügen Sie über ein IT-Sicherheitskonzept? (Einfachauswahl)	Worin sehen Sie Schwierigkeiten? (Offene Frage)	Welchen Unterstützungsbedarf haben Sie? (Offene Frage)	Halten Sie es für möglich mit einem Muster eines IT-Sicherheitskonzeptes zu arbeiten? (Einfachauswahl)
1248349	Anonym	17.12.2019 10:48	nicht geplant			Nein
1248913	Anonym	19.12.2019 09:01	in Vorbereitung	Zu wenig Knowhow vor Ort, zu wenig finanzielle Mittel, zu wenig Informationsfluss von oben nach unten, Am Beispiel der DSGVO des Landes Hessen orientieren	Grundkonzepte, konkrete Ansprechpartner beim Land, welche Informationen bzw. Inhalte sind wichtig, Information der Bürgermeister für besseres Verständnis und dadurch größere Unterstützung	Ja
1248961	Anonym	19.12.2019 11:51	liegt vor	unvollständig		keine Angabe
1248972	Anonym	19.12.2019 12:53	liegt vor			Nein
1251675	Anonym	02.01.2020 22:53	liegt vor			keine Angabe
1252728	Anonym	06.01.2020 13:17	geplant	Ermittlung der Schutzbedarfe		Ja
1252802	Anonym	06.01.2020 15:10	liegt vor	keine Vollständigkeit erreicht	begrenzte Beteiligungen am Sicherheitskonzept durch starke Belastung der Fachabteilungen	Ja
1253140	Anonym	07.01.2020 17:07	nicht geplant	internes Wissen in Organistaion und Leitungsebene liegt nicht vor, personelle Kapazitäten in Qualität und Quantität nicht ausreichend	Dientstellenleiter, externe Begleitung, Kooperation innerhalb der kommunalen Familie	Ja
1253319	Anonym	08.01.2020 09:32	in Vorbereitung			Ja
1253382	Anonym	08.01.2020 11:56	liegt vor			Ja
1253688	Anonym	09.01.2020 08:11	in Vorbereitung	Zeitbudget	ext. DSB=IT-Sicherheitsbeauftrtagter ist tätig, aber Abstimmungsprozesse IN der Verwaltung kann dieser nicht lösen - somit das eigene Zeitbudget	Nein
1253700	Anonym	09.01.2020 08:28	geplant	Umsetzung, Fachwissen, zeitl. Einordnung	Erstellung eines Musterkonzeptes	Ja
1253702	Anonym	09.01.2020 08:48	keine Angabe			Ja
1253720	Anonym	09.01.2020 08:35	liegt vor			Ja
1253737	Anonym	09.01.2020 10:10	geplant			Ja
1253770	Anonym	09.01.2020 11:07	in Vorbereitung	Kosten eines externen Dienstleisters	externe Erarbeitung notwendig	Ja
1253772	Anonym	09.01.2020 11:34	geplant			Ja
1253793	Anonym	09.01.2020 11:33	geplant	siehe 1.	siehe 1.	Nein
1253818	Anonym	09.01.2020 14:14	keine Angabe			Ja
1253824	Anonym	09.01.2020 14:30	geplant	Erstellung und Umsetzung	großen	keine Angabe
1254058	Anonym	10.01.2020 08:32	liegt vor	s. oben	KISA und privater Dienstleister	Ja
1254067	Anonym	10.01.2020 10:22	keine Angabe	großes Aufgabenfeld und keine Zeit	Vorlagen	Ja
1254079	Anonym	10.01.2020 08:51	geplant	Abstimmungsschwierigkeiten und Erfassung der vorhandenen TOM aufgrund der unterschiedlichsten Einrichtungen (Kita, Schulen Verwaltung ect.		Ja
1254144	Anonym	10.01.2020 12:33	geplant	personelle und finanzielle Ressourcen	personelle und finanzielle Ressourcen	Ja

Frage 2: IT-Sicherheitskonzept

Teil A						
ID	Ersteller	Eingegangen am	Frage: Verfügen Sie über ein IT-Sicherheitskonzept? (Einfachauswahl)	Worin sehen Sie Schwierigkeiten? (Offene Frage)	Welchen Unterstützungsbedarf haben Sie? (Offene Frage)	Halten Sie es für möglich mit einem Muster eines IT-Sicherheitskonzeptes zu arbeiten? (Einfachauswahl)
1254815	Anonym	13.01.2020 09:14	in Vorbereitung	zeitliche Bearbeitung aus Kapazitätsgründen / Personalmangel unmöglich		Ja
1254840	Anonym	13.01.2020 10:53	geplant			Ja
1254898	Anonym	13.01.2020 13:41	liegt vor	Konzept von 2008	externen Beratungsbedarf	Nein
1254905	Anonym	13.01.2020 14:01	geplant			Ja
1255026	Anonym	13.01.2020 22:58	in Vorbereitung	Zu wenig Ressourcen bereitgestellt	Ausreichend vorhanden	Ja
1255110	Anonym	14.01.2020 10:39	geplant	Es gibt kein Personal, das dieses Thema "nebenbei" bearbeiten kann, da da Knowhow fehlt. Zusätzliches oder externes Personal kostet Geld, das mit den zur Verfügung stehenden Mitteln nur schwer umzusetzen ist.	Vermittlung von Knowhow, Muster-Vorlagen, vor-Ort-Unterstützung durch Experten	Ja
1255149	Anonym	14.01.2020 14:12	keine Angabe	Wir gehen bereits sehr sensibel und bewusst vertraulich mit den Daten unserer Bürger um. Durch diese Gesetze und Vorkehrungen, die derzeit mehr und mehr zunehmen wird ein riesiger Aufwand betrieben. Wir beschäftigen uns mehr mit der Datensicherung, als andere wichtige Dinge für die Bürger auf den Weg zu bringen. Nicht wir sind die Täter der Cyberkriminalität, müssen aber so einen enormen Aufwand betreiben. Ich sehe dies sehr kritisch.	in allen Belangen. Jede Kommune, gerade die kleinen müssen eigentlich das gleiche machen. Wir haben schon darüber gesprochen, dass wir uns gern zusammenlegen würden. Einen verantwortlichen einsetzen, der die Richtlinie erstellt, die Sicherheit in der Kommune überprüft und das nötigste veranlasst. spricht man aber mit derartigen Firmen, bieten die Beratung an. Keiner übernimmt die Gewährleistung, dass man dann abgesichert und fertig ist. In meinen Augen muss es aber irgendwann gut sein. Wir haben keine Zeit, uns zusätzlich damit zu beschäftigen. Das ist das traurige daran. Wir müssen uns mit Dingen beschäftigen, die in meinen Augen nebensächlich sind, nicht wichtig, da wir eh schon sensibel mit allen Daten umgeben	Ja
1256539	Anonym	20.01.2020 17:01	keine Angabe	Kontrolle der Umsetzung, Befugnis zur Ko.	andere Bez., aber ähnl. Inhalte -> in Dienstanweisung	Ja

Frage 3: Informationssicherheits-Managementsystem (ISMS)

Teil A										
ID	Ersteller	Eingegangen am	Frage: Verfügen Sie über ein ISMS? (Einfachauswahl)	Worin sehen Sie Schwierigkeiten? (Offene Frage)	Welchen Unterstützungsbedarf haben Sie? (Offene Frage)	Spezifische Fragestellungen: (Matrix mit Einfachauswahl)	2. Werden bei Ihnen Sicherheitschecks (Bsp.: IT-Sicherheits-Quick-Check für kleine Kommunalverwaltungen) zur Beurteilung der Informationssicherheit durchgeführt? (Einfachauswahl)	a) In welchem Umfang werden bei Ihnen Sicherheitschecks durchgeführt (kurze Beschreibung der Maßnahme)? (Offene Frage)	b) Mit welcher Häufigkeit/ Regelmäßigkeit werden bei Ihnen Sicherheitschecks durchgeführt? (Offene Frage)
						1. Wird bei Ihnen der BfIS an Verwaltungsprojekten und Verwaltungsentscheidungen beteiligt?			
1248349	Anonym	17.12.2019 10:48	nicht geplant			bisher kein BfIS ernannt	Nein		
1248913	Anonym	19.12.2019 09:01	nicht geplant	Zu wenig Knowhow vor Ort, zu wenig finanzielle Mittel, wodurch externe Firmen nicht beauftragt werden können, externe Firmen tun sich auch schwer, da die Struktur in der öffentlichen Verwaltung anders gelagert sind, als in der freien Wirtschaft, zu wenig Informationsfluss von oben nach unten, Am Beispiel der DSGVO des Landes Hessen orientieren	Grundkonzepte, konkrete Ansprechpartner beim Land, welche Informationen bzw. Inhalte sind wichtig, Information der Bürgermeister für besseres Verständnis und dadurch größere Unterstützung	bisher kein BfIS ernannt	Nein		
1248961	Anonym	19.12.2019 11:51	etabliert			sporadisch beteiligt	Ja	Interne Revisionen zur Prüfung der Umsetzung des IT-Grundschutz	nicht regelmäßig, sondern Fallabhängig
1248972	Anonym	19.12.2019 12:53	etabliert			sporadisch beteiligt	Ja	Im Rahmen der BSI-IT-Grundschutz-Umsetzung MÜSSEN solche Checks umgesetzt werden!	bei Verfahrensänderungen, zyklisch, bei Veränderungen des Standes der Technik, etc.
1251675	Anonym	02.01.2020 22:53	etabliert			sporadisch beteiligt	Ja	Grundschutz-Check	
1252728	Anonym	06.01.2020 13:17	nicht geplant			systematisch beteiligt	Nein		
1252802	Anonym	06.01.2020 15:10	etabliert	Sensibilisierung der Führungskräfte erforderlich, fehlende Beteiligung des BfIS bei neuen Projekten	Hilfe bei der Sensibilisierung der Führungskräfte	sporadisch beteiligt	Ja	IS-Kurzrevision/Zertifizierungsaudit im Fachbereich ELER	jeweils ca. alle 3 Jahre
1253140	Anonym	07.01.2020 17:07	nicht geplant	internes Wissen in Organistaion und Leitungsebene liegt nicht vor, Aufgabe als Führungsaufgabe nicht erkannt	Dienstellenleiter, externe Begleitung, Kooperation innerhalb der kommunalen Familie	bisher kein BfIS ernannt	Nein	für KDN Audit wird Beratung in Anspruch genommen und die geforderte Dokumentation erstellt	0
1253319	Anonym	08.01.2020 09:32	nicht geplant			bisher kein BfIS ernannt	Nein		
1253382	Anonym	08.01.2020 11:56	etabliert			systematisch beteiligt	Ja	Kurzaudits im Rahmen EU-Zahlstellentätigkeit, beschränkt auf ausgewählte Bausteine	Abstand 3-4 Jahre
1253688	Anonym	09.01.2020 08:11	geplant	Zeitbudget	ext. DSB=IT-Sicherheitsbeauftrtagter ist tätig, aber Abstimmungsprozesse IN der Verwaltung kann dieser nicht lösen - somit das eigene Zeitbudget	keine Angabe	Ja	sind damit erst ganz am Anfang, Ziel: vollumfängliche Checks	sind damit erst ganz am Anfang, Ziel: vollumfängliche Checks
1253700	Anonym	09.01.2020 08:28	nicht geplant	Fachwissen, Umsetzung	Muster, Checkliste	bisher kein BfIS ernannt	Nein		
1253702	Anonym	09.01.2020 08:48	nicht geplant			bisher kein BfIS ernannt	Nein		
1253720	Anonym	09.01.2020 08:35	etabliert			systematisch beteiligt	keine Angabe		
1253737	Anonym	09.01.2020 10:10	geplant			sporadisch beteiligt	Ja	geplant, in 2020	noch festzulegen
1253770	Anonym	09.01.2020 11:07	nicht geplant			bisher kein BfIS ernannt	Nein		
1253772	Anonym	09.01.2020 11:34	geplant			sporadisch beteiligt	Ja	sporadisch und nach Neuerungen	sporadisch
1253793	Anonym	09.01.2020 11:33	nicht geplant	Erst die anderen Schritte abarbeiten	siehe andere Themengebiete	bisher kein BfIS ernannt	Nein		
1253818	Anonym	09.01.2020 14:14	keine Angabe			keine Angabe	Nein		
1253824	Anonym	09.01.2020 14:30	geplant	Aufbau und Betreibung	großen	bisher kein BfIS ernannt	Nein		
1254058	Anonym	10.01.2020 08:32	etabliert		KISA und privater Dienstleister	systematisch beteiligt	keine Angabe		
1254067	Anonym	10.01.2020 10:22	keine Angabe	kein Personal, keine Zeit, keine Finanzen für Drittbeauftragung	Vorlagen	keine Angabe	Ja	Computerfirma (Dritter) prüft aktuelle Software	ca. aller 3-4 Monate
1254079	Anonym	10.01.2020 08:51	nicht geplant			sporadisch beteiligt	Nein		
1254144	Anonym	10.01.2020 12:33	etabliert			sporadisch beteiligt	Ja	z.B. Basis-Sicherheitscheck, externe Audits EU-Zahlstelle	aller 2 Jahre
1254815	Anonym	13.01.2020 09:14	geplant	zeitliche Bearbeitung aus Kapazitätsgründen / Personalmangel unmöglich		systematisch beteiligt	Ja	durch den IT-Sicherheitsbeauftragten mittels Kontrollsoftware	bisher einmalig
1254840	Anonym	13.01.2020 10:53	keine Angabe			keine Angabe	Nein		
1254898	Anonym	13.01.2020 13:41	nicht geplant	fachliches Know How und Umsetzungsschwierigkeiten	externen Beratungsbedarf	keine Angabe	Nein		
1254905	Anonym	13.01.2020 14:01	keine Angabe			keine Angabe	Ja		
1255026	Anonym	13.01.2020 22:58	in Vorbereitung		Ausreichend vorhanden	sporadisch beteiligt	Nein		
1255110	Anonym	14.01.2020 10:39	nicht geplant	Personal und Geld fehlt	Vermittlung von Knowhow, vor-Ort-Unterstützung durch Experten	keine Angabe	Nein		
1255149	Anonym	14.01.2020 14:12	nicht geplant	Personal, Kosten, Wissen darüber, Umsetzung, Zeit	in all den oben genannten Belangen: Personal, Kosten, Wissen darüber, Umsetzung, Zeit	keine Beteiligung	Nein		
1256539	Anonym	20.01.2020 17:01	keine Angabe	Durchsetzung/Realisierung, Revision	fachlich, zeitlich	sporadisch beteiligt	Ja	regelm. in BEreichen mit BSI-Zert.	sporadisch geplant in and. Bereichen,

Frage 4: Sicherheitsorganisation

Teil A											
ID	Ersteller	Eingegangen am	1. Angabe der Größe Ihrer Sicherheitsorganisation (Angabe in Vollbeschäftigteneinheit (VBE)): (Offene Frage)	2. Wie ist die Tätigkeit Ihres BfIS in die Aufbau- und Ablauforganisation eingeordnet (zutreffendes bitte ankreuzen)? (Mehrfachauswahl)							Eigene Angabe: (Offene Frage)
1248349	Anonym	17.12.2019 10:48	0		bisher kein BfIS benannt						
1248913	Anonym	19.12.2019 09:01	21		bisher kein BfIS benannt						
1248961	Anonym	19.12.2019 11:51	1						eigene Angabe (bitte Anmerkung im nachfolgenden Feld vornehmen)	Beauftragter - direkt dem Landrat zugeordnet	
1248972	Anonym	19.12.2019 12:53	1						eigene Angabe (bitte Anmerkung im nachfolgenden Feld vornehmen)	Als Stabsstelle beim Beigeordneten	
1251675	Anonym	02.01.2020 22:53	200					Extern			
1252728	Anonym	06.01.2020 13:17	46					Extern			
1252802	Anonym	06.01.2020 15:10	2						eigene Angabe (bitte Anmerkung im nachfolgenden Feld vornehmen)	Stabstelle beim Landrat	
1253140	Anonym	07.01.2020 17:07	0						eigene Angabe (bitte Anmerkung im nachfolgenden Feld vornehmen)	SB im FG IT	
1253319	Anonym	08.01.2020 09:32	0		bisher kein BfIS benannt						
1253382	Anonym	08.01.2020 11:56	5						eigene Angabe (bitte Anmerkung im nachfolgenden Feld vornehmen)	Stabstelle beim Landrat	
1253688	Anonym	09.01.2020 08:11	0					Extern			ext. DSB = IT-Sicherheitsbeauftragter
1253700	Anonym	09.01.2020 08:28	0		bisher kein BfIS benannt						
1253702	Anonym	09.01.2020 08:48	0		bisher kein BfIS benannt						
1253720	Anonym	09.01.2020 08:35	220					Extern			
1253737	Anonym	09.01.2020 10:10	38					Extern			
1253770	Anonym	09.01.2020 11:07	0		bisher kein BfIS benannt						keine Stelle vorhanden und auch keine Stelle finanzierbar
1253772	Anonym	09.01.2020 11:34	1					Extern			
1253793	Anonym	09.01.2020 11:33	15		bisher kein BfIS benannt						
1253818	Anonym	09.01.2020 14:14	1	keine Angabe							
1253824	Anonym	09.01.2020 14:30	2		bisher kein BfIS benannt						
1254058	Anonym	10.01.2020 08:32	0					Extern			
1254067	Anonym	10.01.2020 10:22	7	keine Angabe							
1254079	Anonym	10.01.2020 08:51	162				IT- oder Organisationsdezernat				
1254144	Anonym	10.01.2020 12:33	0						eigene Angabe (bitte Anmerkung im nachfolgenden Feld vornehmen)	Zuordnung zum Bereich Landrat	
1254815	Anonym	13.01.2020 09:14	140					Extern			
1254840	Anonym	13.01.2020 10:53	1					Extern			
1254898	Anonym	13.01.2020 13:41	10	keine Angabe							
1254905	Anonym	13.01.2020 14:01	5		bisher kein BfIS benannt						
1255026	Anonym	13.01.2020 22:58	0					Extern			Zu 1. - Weit unter 0,05 (Zahl kann leider so nicht eingegeben werden)
1255110	Anonym	14.01.2020 10:39	0	keine Angabe							
1255149	Anonym	14.01.2020 14:12	7		bisher kein BfIS benannt						
1256539	Anonym	20.01.2020 17:01	1						eigene Angabe (bitte Anmerkung im nachfolgenden Feld vornehmen)	direkte Zuordnung zur Behördenleitung	

Frage 5: Maßnahme zur Durchführung von Informations- und Sensibilisierungsveranstaltungen für Mitarbeiter

Teil A												
ID	Ersteller	Eingegangen am	Frage: Werden Maßnahmen in Form von Informations- und Sensibilisierungsveranstaltungen für die Mitarbeiter durchgeführt? (Einfachauswahl)	Worin sehen Sie Schwierigkeiten? (Offene Frage)	Welchen Unterstützungsbedarf haben Sie? (Offene Frage)	1. Wenn Maßnahmen in Form von Informations- und Sensibilisierungsveranstaltungen durch Sie geplant sind oder durchgeführt wurden, welche Zielgruppe (z. Bsp. Behördenleitung, Sachbearbeiter oder andere) soll oder wurde bisher damit angesprochen (kurze Beschreibung der Zielgruppe dieser Maßnahme)? (Offene Frage)	2. Kennen Sie das E-Learning Angebot „Informationssicherheit am Arbeitsplatz"? (Einfachauswahl)	2.1 Zusatz Frage 2: Nutzen Sie das Angebot bzw. würden Sie das Angebot gern nutzen? (Einfachauswahl)	3. Kennen Sie die Sensibilisierungsveranstaltung „INFOSIC | Die Hacker kommen"? (Einfachauswahl)	3.1 Zusatz Frage 3: Nutzen Sie das Angebot bzw. würden Sie das Angebot gern nutzen? (Einfachauswahl)	4. Kennen Sie die Sensibilisierungsveranstaltung „INFOSIC plus | IT-Sicherheit für Fortgeschrittene"? (Einfachauswahl)	4.1 Zusatz Frage 4: Nutzen Sie das Angebot bzw. würden Sie das Angebot gern nutzen? (Einfachauswahl)
1248349	Anonym	17.12.2019 10:48	erfolgt regelmäßig (mind. 1x jährlich)			alle Mitarbeiter, die Zugang zu Bildschirmarbeitsplätzen mit Netzwerkzugang haben	Nein	Nein, aber würde Angebot gern nutzen	Ja	Ja	Nein	
1248913	Anonym	19.12.2019 09:01	erfolgt sporadisch oder anlassbezogen	zu wenig Verständnis der Mitarbeiter		Alle Mitarbeiter der Verwaltung und Außenstellen, die mit Daten arbeiten	Nein	Nein, aber würde Angebot gern nutzen	Nein	Nein, aber würde Angebot gern nutzen	Nein	Nein, aber würde Angebot gern nutzen
1248961	Anonym	19.12.2019 11:51	erfolgt sporadisch oder anlassbezogen	verschiedener Wissens- und Motivationsstand der Mitarbeiter	externe e-learning Angebote und Möglichkeiten der "Flächensensibilisierung"		Ja	Ja	Ja	Ja	Nein	Nein, aber würde Angebot gern nutzen
1248972	Anonym	19.12.2019 12:53	erfolgt regelmäßig (mind. 1x jährlich)	große Verwaltung daher hoher Aufwand		Intranet, Rundschreiben (anlassbezogen), Zielgruppenorientierte Einzelmaßnahmen, Flyer, etc.	Ja	Nein	Ja	Ja	Ja	Ja
1251675	Anonym	02.01.2020 22:53	erfolgt regelmäßig (mind. 1x jährlich)				Ja	Nein	Ja	Nein	Ja	Nein
1252728	Anonym	06.01.2020 13:17	erfolgt regelmäßig (mind. 1x jährlich)			Behördenleitung und Sachbearbeiter	Ja	Nein, aber würde Angebot gern nutzen	Ja	Nein, aber würde Angebot gern nutzen	Nein	Nein
1252802	Anonym	06.01.2020 15:10	erfolgt regelmäßig (mind. 1x jährlich)	Teilnahmeprobleme wegen Arbeitsbelastung in den Fachbereichen	mangelnde Vorbildwirkung durch Führungskräfte	alle Beschäftigten	Ja	Ja	Ja	Ja	Ja	Ja
1253140	Anonym	07.01.2020 17:07	nicht geplant	Erfordernis wird so nicht gesehen und dahinter liegender Aufwand wird gescheut, personelle geeignete Kapazitäten nicht vorhanden	Dientstellenleiter, externe Begleitung		Ja	Ja	Ja	Nein	Nein	Nein
1253319	Anonym	08.01.2020 09:32	nicht geplant				Nein	Nein, aber würde Angebot gern nutzen	Nein	Nein, aber würde Angebot gern nutzen	Nein	Nein, aber würde Angebot gern nutzen
1253382	Anonym	08.01.2020 11:56	erfolgt regelmäßig (mind. 1x jährlich)			Schulung aller Mitarbeiter, Intranet-Artikel, Informationen per E-Mail an ausgewählte Zielgruppen, Veranstaltung der Infosic im Haus durchgeführt, E-Learning Sachsen im Intranet publiziert	Ja	Ja	Ja	Ja	Ja	Ja
1253688	Anonym	09.01.2020 08:11	erfolgt regelmäßig (mind. 1x jährlich)	Zeitfaktor NEBEN allen anderen Themen der Verwaltung	keinen	ALLE	Nein	Nein, aber würde Angebot gern nutzen	Nein	Nein, aber würde Angebot gern nutzen	Nein	Nein, aber würde Angebot gern nutzen
1253700	Anonym	09.01.2020 08:28	geplant	Vermittlung der entsprechenden Gesetzlichkeiten	Muster, Checkliste	gesamte Belegschaft, Behördenleitung, Beschäftigte	Nein	Nein, aber würde Angebot gern nutzen	Ja	Nein, aber würde Angebot gern nutzen	Nein	Nein
1253702	Anonym	09.01.2020 08:48	erfolgt regelmäßig (mind. 1x jährlich)	teilweise fehlende IT-Grundkenntnisse der Mitarbeiter		alle Verwaltungsmitarbeiter mit Zugang zum Datenverarbeitungssystem	Ja	Nein, aber würde Angebot gern nutzen	Nein	Nein, aber würde Angebot gern nutzen	Nein	Nein, aber würde Angebot gern nutzen
1253720	Anonym	09.01.2020 08:35	erfolgt regelmäßig (mind. 1x jährlich)			Alle Mitarbeiter	Ja	Ja	Ja	Ja	Ja	Ja
1253737	Anonym	09.01.2020 10:10	geplant	keine	derzeit keine, externe Fachkraft	gesamte Mitarbeiterschaft	Ja	Nein, aber würde Angebot gern nutzen	Ja	Ja	Nein	Nein, aber würde Angebot gern nutzen
1253770	Anonym	09.01.2020 11:07	erfolgt sporadisch oder anlassbezogen	Aufwand für Informationseinholung	Muster	Belegschaft	Nein	Nein, aber würde Angebot gern nutzen	Nein	Nein, aber würde Angebot gern nutzen	Ja	Nein, aber würde Angebot gern nutzen
1253772	Anonym	09.01.2020 11:34	erfolgt sporadisch oder anlassbezogen				Nein	Nein, aber würde Angebot gern nutzen	Nein	Nein, aber würde Angebot gern nutzen	Nein	Nein
1253793	Anonym	09.01.2020 11:33	erfolgt sporadisch oder anlassbezogen	Es fehlt bisher ein BfIS	Einen BfIS zu benennen und fachlich fit zu machen und die entsprechenden Konzepte etc. zu bearbeiten	Aufgrund unserer überschaubaren Größe werden meist alle Mitarbeiter geschult	Nein	Nein, aber würde Angebot gern nutzen	Ja	Nein, aber würde Angebot gern nutzen	Nein	Nein, aber würde Angebot gern nutzen
1253818	Anonym	09.01.2020 14:14	keine Angabe				Ja	Ja	Ja	Nein, aber würde Angebot gern nutzen	Nein	Nein, aber würde Angebot gern nutzen
1253824	Anonym	09.01.2020 14:30	geplant	zu kleine Verwaltung	großen	noch keine	Nein	Nein, aber würde Angebot gern nutzen	Nein	Nein, aber würde Angebot gern nutzen	Nein	Nein, aber würde Angebot gern nutzen
1254058	Anonym	10.01.2020 08:32	erfolgt regelmäßig (mind. 1x jährlich)	Vermittlung der gesetzlichen Anforderungen und Pflichten/Auswirkungen an jeden einzelnen Mitarbeiter	KISA und privaten Dienstleister	Schulung zum Datenschutz und IT-Sicherheit für jeden Mitarbeiter	Nein	Nein, aber würde Angebot gern nutzen	Nein	Nein, aber würde Angebot gern nutzen	Nein	Nein, aber würde Angebot gern nutzen
1254067	Anonym	10.01.2020 10:22	nicht geplant	keine Finanzen, kein Personal, keine Zeit	mehr Finanzen, mehr Personal, mehr Zeit	Verwaltungsmanagement, Regiebetriebsleiter/-mitarbeiter	Nein	Nein, aber würde Angebot gern nutzen	Nein	Nein, aber würde Angebot gern nutzen	Nein	Nein, aber würde Angebot gern nutzen
1254079	Anonym	10.01.2020 08:51	erfolgt sporadisch oder anlassbezogen				Nein	Ja	Nein	Ja	Nein	Ja
1254144	Anonym	10.01.2020 12:33	erfolgt regelmäßig (mind. 1x jährlich)		zentrale Angebote für Behörden	Leitungspersonal, Sachbearbeiter	Ja	Nein, aber würde Angebot gern nutzen	Ja	Ja	Ja	Ja
1254815	Anonym	13.01.2020 09:14	erfolgt regelmäßig (mind. 1x jährlich)			Behördenleitung / Sachbearbeiter / technisches Personal	Nein	Nein	Ja	Nein, aber würde Angebot gern nutzen	Nein	Nein, aber würde Angebot gern nutzen
1254840	Anonym	13.01.2020 10:53	geplant				Nein	Nein, aber würde Angebot gern nutzen	Ja	Ja	Nein	Ja
1254898	Anonym	13.01.2020 13:41	erfolgt sporadisch oder anlassbezogen		externen Beratungsbedarf		Nein	Ja	Nein	Ja	Nein	Ja
1254905	Anonym	13.01.2020 14:01	erfolgt sporadisch oder anlassbezogen				Nein	Nein, aber würde Angebot gern nutzen	Ja	Nein, aber würde Angebot gern nutzen	Nein	Nein, aber würde Angebot gern nutzen
1255026	Anonym	13.01.2020 22:58	erfolgt sporadisch oder anlassbezogen	Muss regelmäßig erfolgen, kann mit externem ISB und derzeitigem Budget schwer realisiert werden. Intern zu wenig Ressourcen.		Alle Mitarbeiter	Ja	Nein, aber würde Angebot gern nutzen	Ja	Nein	Ja	Nein, aber würde Angebot gern nutzen
1255110	Anonym	14.01.2020 10:39	nicht geplant	fehlende Strukturen (BfIS)	-		Nein	Nein, aber würde Angebot gern nutzen	Ja	Ja	Nein	Nein, aber würde Angebot gern nutzen
1255149	Anonym	14.01.2020 14:12	nicht geplant	Zeit, Kosten	das richtige zu finden, das zeitlich einzuordnen, das ganze personell umzusetzen und zu finanieren	keine	Nein	Nein	Nein	Nein	Nein	Nein
1256539	Anonym	20.01.2020 17:01	geplant	zeitlich in der Umsetzung durch die Mitarb. des Fachbereichs, sonst keine	Angebot Sensibil. In-House / "Die Hacker kommen" u. a. / Aufbauveranst.	alle MA	Ja	Ja	Ja	Ja	Ja	Ja

Frage 6: Identifizierung schützenswerter Anwendungen

Teil A					
ID	Ersteller	Eingegangen am	Frage: Haben Sie in Ihrer Kommune besonders schützenswerte Anwendungen identifiziert? (Einfachauswahl)	Worin sehen Sie Schwierigkeiten? (Offene Frage)	Welchen Unterstützungsbedarf haben Sie? (Offene Frage)
1248349	Anonym	17.12.2019 10:48	nicht geplant		
1248913	Anonym	19.12.2019 09:01	teilweise erfolgt	Komplexität der Aufgabe mit zu wenig zeitlichen Ressourcen	konkretten Ansprechpartner bei dem man Fragen stellen kann und am Ende auch beantwortet kommt. Mehrere Mails an das Land blieben unbeantwortet.
1248961	Anonym	19.12.2019 11:51	vollständig abgeschlossen und die Schutzbedarfe hinsichtlich der Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) wurden festgelegt	Verständnis der Fachbereiche in Schutzbedarf umzusetzen	klare Vorgaben an die Einstufung der Vertraulichkeit von Daten (ab wann erhöhter Schutzbedarf)
1248972	Anonym	19.12.2019 12:53	teilweise erfolgt		
1251675	Anonym	02.01.2020 22:53	vollständig abgeschlossen und die Schutzbedarfe hinsichtlich der Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) wurden festgelegt		
1252728	Anonym	06.01.2020 13:17	ist geplant	siehe 2.	
1252802	Anonym	06.01.2020 15:10	teilweise erfolgt	zu viele unterschiedliche Fachverfahren	wünschenswerte vermehrte Zentralisierung der Anwendungen z.B. in Form der Nutzung von Basiskomponenten
1253140	Anonym	07.01.2020 17:07	nicht geplant	Fast alle Programme arbeiten mit personenbezogenen DAten, sind für die Dienstleistung der Verwaltung erforderlich, alle schützenswert	Dienststellenleitung, Organisation, externe Begleitung
1253319	Anonym	08.01.2020 09:32	teilweise erfolgt		
1253382	Anonym	08.01.2020 11:56	teilweise erfolgt	Identifikation und zeitlicher Aufwand	
1253688	Anonym	09.01.2020 08:11	teilweise erfolgt		
1253700	Anonym	09.01.2020 08:28	keine Angabe		
1253702	Anonym	09.01.2020 08:48	keine Angabe	die Frage ist unklar formuliert, da nicht klar ist, auf welche besonders schützenswerte Anwendungen abgestellt wird	
1253720	Anonym	09.01.2020 08:35	keine Angabe		
1253737	Anonym	09.01.2020 10:10	ist geplant		
1253770	Anonym	09.01.2020 11:07	teilweise erfolgt	Personalaufwand	
1253772	Anonym	09.01.2020 11:34	vollständig abgeschlossen, aber die Schutzbedarfe wurden noch nicht festgelegt		
1253793	Anonym	09.01.2020 11:33	ist geplant	Überblick über alle Anwendungen und deren Schutzbedarfe verschaffen (zeitaufwendig und muss immer "nebenher" erledigt werden)	Personell bzw. monetär um die personelle Schiene über Dienstleister abzudecken
1253818	Anonym	09.01.2020 14:14	keine Angabe		
1253824	Anonym	09.01.2020 14:30	ist geplant	Sensibiliserung, Know how	großen
1254058	Anonym	10.01.2020 08:32	vollständig abgeschlossen und die Schutzbedarfe hinsichtlich der Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) wurden festgelegt	Reaktionszeit auf gesetzliche Änderungen neben den eigentlichen Arbeitsaufgaben	KISA, privater Dienstleister
1254067	Anonym	10.01.2020 10:22	teilweise erfolgt		
1254079	Anonym	10.01.2020 08:51	ist geplant		
1254144	Anonym	10.01.2020 12:33	teilweise erfolgt	hoher personeller Aufwand, Vielzahl der Fachanwendungen	personelle und finanzielle Ressourcen
1254815	Anonym	13.01.2020 09:14	teilweise erfolgt	zeitliche Bearbeitung aus Kapazitätsgründen / Personalmangel unmöglich	Vorhaltung von ausreichend Personalstellen
1254840	Anonym	13.01.2020 10:53	ist geplant		
1254898	Anonym	13.01.2020 13:41	teilweise erfolgt	organisatorische Umsetzung	Schulungsbedarf der Mitarbeiter
1254905	Anonym	13.01.2020 14:01	keine Angabe		
1255026	Anonym	13.01.2020 22:58	in Vorbereitung	Ressourcen, kommen nicht voran wie gewünscht	
1255110	Anonym	14.01.2020 10:39	nicht geplant	s.o.	-
1255149	Anonym	14.01.2020 14:12	nicht geplant	das richtige zu finden, das zeitlich einzuordnen, das ganze personell umzusetzen und zu finanieren	in allen oben genannten Belangen: Personal, Finanzierung, Zeitaufwand
1256539	Anonym	20.01.2020 17:01	vollständig abgeschlossen und die Schutzbedarfe hinsichtlich der Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) wurden festgelegt	ZEitaufw., Überprüfung, Einord. in eine systemat. Übersciht der GEschäftsprozesse	

Frage 7: Organisatorische Maßnahmen für IT Sicherheitsvorfälle

Teil A								
ID	Ersteller	Eingegangen am	Was ist für Sie ein IT-Sicherheitsvorfall? (Offene Frage)	Frage: Wurden organisatorische Maßnahmen für IT-Sicherheitsvorfälle festgelegt? (Einfachauswahl)	Worin sehen Sie Schwierigkeiten? (Offene Frage)	Welchen Unterstützungsbedarf haben Sie? (Offene Frage)	1. Gibt es bei Ihnen vorgeschriebene Abläufe bei IT-Sicherheitsvorfällen z. Bsp. durch einen Angriff auf Ihre IT durch Schadsoftware? (Einfachauswahl)	2. Haben Sie schon einmal einen IT-Sicherheitsvorfall dem "Computer Emergency Response Team" (SAX.CERT) der Landesverwaltung des Freistaates gemeldet? (Einfachauswahl)
1248349	Anonym	17.12.2019 10:48		keine Angabe			keine Angabe	Nein
1248913	Anonym	19.12.2019 09:01	Teil- oder Totalausfall der IT und der Telefone aufgrund größerer Schadensereignisse (Stromausfall, Brand, Erdbeben, Hochwasser, Schadsoftware u. ä.)	festgelegt		Vorlage des Sicherheitskonzept zur Prüfung und evtl. Anregungen zur Verbesserung	Ja	Nein
1248961	Anonym	19.12.2019 11:51	Verletzung der Schutzziele CIA	geplant	Vorgaben nach Sanktionen fehlen		Ja	Ja
1248972	Anonym	19.12.2019 12:53	§ 3 SächsISichG: Abs. 5: Ein Sicherheitsvorfall ist ein Ereignis, das tatsächlich nachteilige Auswirkungen auf die Informationssicherheit hat.	festgelegt	Prozessabstimmung, Paktikabilität und Umsetzbarkeit im Verwlatungsalltag, Akzeptanz für Prozesse,		Ja	Ja
1251675	Anonym	02.01.2020 22:53		geplant			Ja	Nein
1252728	Anonym	06.01.2020 13:17	z.B. Hackerangriff	geplant			Nein	Nein
1252802	Anonym	06.01.2020 15:10	ist ein Ereignis, dass nachteilige Auswirkungen auf die Informationssicherheit hat	festgelegt	bei der Umsetzung	regelmäßige Information der entsprechenden Mitarbeiter durch die Vorgesetzten	keine Angabe	Nein
1253140	Anonym	07.01.2020 17:07	ist nicht definiert in der Sicherheitsrichtlinie	nicht geplant	Dienststellenleitung, Organisation sehen dies nicht als Führungsaufgabe, lediglich Aufgabe des FG IT	Dienststellenleitung, Organisation, externe Begleitung	Nein	Nein
1253319	Anonym	08.01.2020 09:32		nicht geplant			Nein	Nein
1253382	Anonym	08.01.2020 11:56	ein Ereignis, welches die Vertraulichkeit, Verfügbarkeit und Integrität beliebiger Informationen, Geschäftsprozesse, IT-Dienste, IT-Systeme oder IT-Anwendungen beeinträchtigen kann. und bei dem durch die Auswirkungen ein Schaden für den Landkreis, seine Kunden und Geschäftspartner entstehen kann.	in Vorbereitung			Ja	Ja
1253688	Anonym	09.01.2020 08:11		in Vorbereitung	Zeitfaktor		keine Angabe	Nein
1253700	Anonym	09.01.2020 08:28		in Vorbereitung			Ja	Nein
1253702	Anonym	09.01.2020 08:48	Hardwareschaden, Datenverlust, nicht autorisierter Systemzugriff von außen und intern,	in Vorbereitung			keine Angabe	Ja
1253720	Anonym	09.01.2020 08:35		festgelegt			Ja	keine Angabe
1253737	Anonym	09.01.2020 10:10	Hackerangriff, Offenlegen von Daten durch Konfigurationsfehler	festgelegt			Ja	Nein
1253770	Anonym	09.01.2020 11:07	Schadsoftware, unerlaubte Datenlöschung, externe Angriff (Mail)	geplant	Aufwand	Muster	Nein	Nein
1253772	Anonym	09.01.2020 11:34	Angriffe, Datenlecks etc.	keine Angabe			Ja	Nein
1253793	Anonym	09.01.2020 11:33	Beispielsweise wenn ein Mitarbeiter einen unbekannten Anhang öffnet und sich bzw. der Verwaltung somit Schadsoftware herunterlädt, die dann das Netzwerk befällt.	geplant	Sensibilisierung und Prävention für IT-Sicherheitsvorfälle	siehe andere Antworten	Nein	Nein
1253818	Anonym	09.01.2020 14:14		keine Angabe			keine Angabe	Nein
1253824	Anonym	09.01.2020 14:30	Hackerangriff	geplant	Kompetenz, Know how	großen	Nein	Nein
1254058	Anonym	10.01.2020 08:32	Missbrauch Datenschutzrichtlinien, Hackerangriff, SPAM-Mails geöffnet	festgelegt	Umsetzugn bei den einzelnen Mitarbeitern beim Sicherheitsvorfall	KISA und privaten Dienstleister	Ja	Nein
1254067	Anonym	10.01.2020 10:22	Darüber nachzudenken, fehlt es an Zeit	keine Angabe			Nein	Nein
1254079	Anonym	10.01.2020 08:51	Angriff auf das Netz der Kommune	geplant			Nein	Nein
1254144	Anonym	10.01.2020 12:33	Definition im Sächsischen Informationssicherheitsgesetz	festgelegt			Ja	Nein
1254815	Anonym	13.01.2020 09:14		festgelegt			Ja	Nein
1254840	Anonym	13.01.2020 10:53	Virenbefall	geplant			Ja	Nein
1254898	Anonym	13.01.2020 13:41	Hackerangriff mittels Schadensoftware	festgelegt			Ja	Nein
1254905	Anonym	13.01.2020 14:01		geplant			keine Angabe	Nein
1255026	Anonym	13.01.2020 22:58	Ein Ereignis, das die Vertraulichkeit, Verfügbarkeit und Integrität unserer IT-Systeme oder IT-Anwendungen (IT-Services) mit hohem oder sehr hohem Schutzbedarf derart beeinträchtigt, dass ein großer Schaden für unsere Verwaltung bzw. die Bürger (unsere "Kunden") entstehen kann.	in Vorbereitung			Nein	Nein
1255110	Anonym	14.01.2020 10:39	-	nicht geplant	s.o.	-	keine Angabe	Nein
1255149	Anonym	14.01.2020 14:12	wenn sich jemand in unsere Daten einhackt.	nicht geplant	Zeit, Personal, Finanzierung	in allen oben genannten Belangen: Personal, Finanzierung, Zeitaufwand	Nein	Nein
1256539	Anonym	20.01.2020 17:01		festgelegt	Zeitl., Übung, Revision/PRüf. a. Anwendbarkeit/Aktualität		Ja	keine Angabe

Teil B: Gewünschte Unterstützung

Teil B													
ID	Ersteller	Eingegangen am	Es besteht Bedarf an nachfolgend angekreuzten gewünschten Möglichkeiten zur Unterstützung der sächsischen Kommunen durch den Freistaat Sachsen. (Mehrfach möglich)									Weitere Arten von Unterstützungen, die vorhergehend nicht aufgeführt sind, bitte hier eintragen. (Offene Frage)	Angabe der Themen, wenn Unterstützung gewünscht wird (bitte benennen Sie die jeweilige Unterstützungsart und benennen dann das Thema). (Offene Frage)
			1. Checklisten	2. Informationsbroschüren	3. Informationen zu IT-Sicherheitsbedrohungen	4. Seminare / Workshops	5. Sensibilisierungsveranstaltungen	6. Allgemeine Informationsveranstaltungen	7. Hilfestellung im Schadensfall durch persönliche Anleitung zur Schadensregulierung	8. Keine Unterstützung gewünscht			
1248349	Anonym	17.12.2019 10:48				Ja	Ja		Ja				
1248513	Anonym	19.12.2019 09:01	Ja		Ja		Ja					Finanzielle Unterstützung durch das Land, gesetzliche Vorgaben mit Angabe der erforderlichen MA, Einstellung von Fachkräften beim Land, die für die Kleinen Kommunen zuständig sind und auch vor Ort kommen	Technische Gestaltung zu allem derzeitigen Jahren vorgegeben und durch Gesetz außerhalb Aufgaben. In kleineren Kommunen wird DSKMO, IT-Sicherheitsbeauftragter usw. dem Mitarbeiter übergeben, der mit einer geringen Stundenzahl für das gesamte System verantwortlich ist. Die Mitarbeiter und damit die Arbeitsplätze sind geringer, jedoch ist die Komplexität der Aufgaben nicht geringer. Auch Server, USV usw. und die damit verbunden Sicherheitsmaßnahmen sind weder finanziell noch personell bei einer 7000 EWO Gemeinde geringer als bei einer 100000 EWO Stadt. Auch darüber sollte sich das Land über Stand
1248581	Anonym	19.12.2019 11:51	Ja	Ja	Ja	Ja	Ja	Ja	Ja			zentrale Vorgaben und Möglichkeit wie die IT-Sicherheit zu erhöhen (zentrale technische Lösungen)	
1248972	Anonym	19.12.2019 12:53			Ja	Ja	Ja		Ja			Standardverfahren (Fachanwendungen) die im Freistaat gehostet werden. Möglichkeit, technische Sicherheit für den ganzen Freistaat, Arbeitsmarkt Basiskomponente, Einteilung von Betrieb möglichkeiten in der Fachanwendung. (Einkommensende Beispiele: ELA/Arbeitslos, Wohngeld, etc.)	
1251675	Anonym	02.01.2020 22:33			Ja		Ja	Ja	Ja				
1252726	Anonym	06.01.2020 13:17	Ja	Ja	Ja	Ja	Ja	Ja	Ja				
1252932	Anonym	06.01.2020 15:10			Ja	Ja	Ja		Ja			Sensibilisierung einer zentralen Gemeinschaftsstelle	Sensibilisierung der Führungsebene
1253140	Anonym	07.01.2020 17:07	Ja	Ja	Ja		Ja	Ja				Einstellung einer Übersicht der Aufgabenverantwortung der Dienstleistung für die Thematik Informationssicherheit), sichere Verarbeitung der (SB) bei den Landkreisen z.B. bei den RPA	
1253319	Anonym	08.01.2020 09:32	Ja	Ja	Ja	Ja	Ja	Ja	Ja				
1253352	Anonym	08.01.2020 11:06	Ja	Ja	Ja	Ja	Ja	Ja	Ja				
1253695	Anonym	08.01.2020 06:11							Ja				
1253700	Anonym	08.01.2020 06:28	Ja	Ja	Ja			Ja					
1253702	Anonym	08.01.2020 06:46	Ja			Ja	Ja		Ja				
1253720	Anonym	08.01.2020 08:35											
1253737	Anonym	09.01.2020 10:10	Ja	Ja	Ja	Ja	Ja	Ja	Ja				Sicherheitsbedrohungen - Newsletter, Grundinformationen im Broschürenform als Unterweisungsmöglichkeit, Sensibilisierung als kurze Dienstbesprechung / Filmclip
1253770	Anonym	09.01.2020 11:07	Ja		Ja	Ja	Ja		Ja			Einfache und kostenlose Bereitstellung von allgemeinen Materialien	
1253772	Anonym	09.01.2020 11:34	Ja	Ja	Ja				Ja				
1253793	Anonym	09.01.2020 11:33	Ja		Ja	Ja	Ja		Ja				
1253815	Anonym	09.01.2020 14:14	Ja	Ja	Ja	Ja	Ja	Ja	Ja				
1253824	Anonym	09.01.2020 14:30	Ja	Ja	Ja	Ja	Ja	Ja	Ja				
1254056	Anonym	10.01.2020 06:32	Ja						Ja				
1254087	Anonym	10.01.2020 10:22	Ja	Ja	Ja		Ja					besseres Finanzbudget besseres Zeitbudget besseres Personalbudget	
1254170	Anonym	10.01.2020 08:51	Ja	Ja	Ja	Ja	Ja	Ja	Ja				
1254744	Anonym	10.01.2020 12:33	Ja	Ja	Ja	Ja	Ja	Ja	Ja				
1254815	Anonym	13.01.2020 09:14	Ja	Ja	Ja	Ja			Ja				Kennzahlen für Stellen im IT-Sicherheitsbereich für Kommunalverwaltungen - Vorgaben durch die Landesregierung (auch bei externen Beauftragen bleibt die Kommune für die IT-Sicherheit verantwortlich)
1254840	Anonym	13.01.2020 10:53	Ja	Ja	Ja			Ja	Ja				
1254846	Anonym	13.01.2020 13:41	Ja		Ja	Ja	Ja	Ja	Ja				
1254935	Anonym	13.01.2020 14:01	Ja			Ja	Ja		Ja				
1255026	Anonym	13.01.2020 22:56	Ja		Ja	Ja			Ja			Technische Schutzprogramme (IPS / IDS) zur Minderung durch Kommunen	
1255170	Anonym	14.01.2020 10:39			Ja	Ja	Ja		Ja				
1255749	Anonym	14.01.2020 14:12	Ja		Ja	Ja	Ja						
1256039	Anonym	20.01.2020 17:01	Ja		Ja	Ja	Ja	Ja	Ja			E-Recht, Überprüfung/ Hinweise zur Nutzung von seitens des FS Sachs. empfohlen, oder verpflichtend einzuführenden, jedoch von der Kommunen als Verantwortlichem betriebenen Systemen/Software, nachhaltige Information bei geplanten Umsetzungen/	

Teil C: Hemmnisse

Teil C										
ID	Ersteller	Eingegangen am	Folgende Hemmnisse zum Aufbau einer systematischen Informationssicherheit liegen in der an der Umfrage teilnehmenden Kommune vor: (Matrix mit Mehrfachauswahl)							Weitere Hemmnisse, die vorhergehend nicht aufgeführt sind, bitte hier eintragen: (Offene Frage)
			1. Interne organisatorische Probleme	2. Unzureichende Unterstützung der Behördenleitung	3. Mangelnde Akzeptanz der Mitarbeiter	4. Probleme der Steuerung von externen Dienstleistern z. B.sp. bei Outsourcing (Probleme in der Zusammenarbeit mit externen Dienstleistern im Rahmen der Informationssicherheit)	5. Fehlendes Personal	6. Geringes Budget	7. Es bestehen keine Hemnisse	
1248849	Anonym	17.12.2019 10:48					Ja	Ja		Fachwissen
1248913	Anonym	19.12.2019 09:01	Ja	Ja	Ja	Ja	Ja	Ja		
1248961	Anonym	19.12.2019 11:51	Ja		Ja	Ja	Ja	Ja		
1248972	Anonym	19.12.2019 12:53	Ja	Ja	Ja	Ja	Ja	Ja		
1251575	Anonym	02.01.2020 22:53						Ja		
1252728	Anonym	06.01.2020 13:17					Ja	Ja		
1252802	Anonym	06.01.2020 15:19	Ja	Ja	Ja	Ja	Ja	Ja		keine Angabe
1253140	Anonym	07.01.2020 17:07	Ja	Ja						Ist die Produktion von IT immer noch der effektivste Weg für die Kommunalverwaltung, wäre regionale Kooperation in einem RZ Verbund nicht ein systematischer Ansatz für mehr Informationssicherheit?
1253319	Anonym	08.01.2020 09:32		Ja			Ja			
1253382	Anonym	08.01.2020 11:56							Ja	
1253688	Anonym	09.01.2020 08:11					Ja	Ja		
1253700	Anonym	09.01.2020 08:28					Ja			
1253702	Anonym	09.01.2020 08:48	Ja			Ja	Ja	Ja		
1253720	Anonym	09.01.2020 08:35								
1253737	Anonym	09.01.2020 10:10			Ja		Ja	Ja		
1253770	Anonym	09.01.2020 11:07					Ja	Ja		
1253772	Anonym	09.01.2020 11:34					Ja			
1253793	Anonym	09.01.2020 11:33	Ja		Ja		Ja	Ja		
1253818	Anonym	09.01.2020 14:14	Ja		Ja		Ja	Ja		
1253824	Anonym	09.01.2020 14:30	Ja			Ja	Ja	Ja		
1254058	Anonym	10.01.2020 08:32	Ja				Ja	Ja		
1254067	Anonym	10.01.2020 10:22		Ja		Ja	Ja	Ja		
1254079	Anonym	10.01.2020 08:51	Ja		Ja		Ja	Ja		
1254144	Anonym	10.01.2020 12:33					Ja	Ja		
1254815	Anonym	13.01.2020 09:14	Ja				Ja			Die Zahl der Vollbeschäftigten zur Bewertung einer Sicherheitsorganisation ist nicht ausreichend, besser ist die Zahl der peripheren computer- und mobil unterstützten Arbeitsplätze insgesamt.
1254840	Anonym	13.01.2020 10:53					Ja			
1254898	Anonym	13.01.2020 13:41	Ja		Ja		Ja	Ja		
1254905	Anonym	13.01.2020 14:01	Ja				Ja	Ja		
1255028	Anonym	13.01.2020 22:58	Ja	Ja			Ja	Ja		
1255110	Anonym	14.01.2020 10:39					Ja	Ja		
1255149	Anonym	14.01.2020 14:12	Ja	Ja			Ja	Ja		
1255639	Anonym	20.01.2020 17:01					Ja			

Eidesstattliche Erklärung

Ich versichere hiermit an Eides Statt, dass ich die vorgelegte Masterarbeit mit dem Titel

Bedarfsanalyse und Konzeptentwicklung zum Aufbau und zur Weiterentwicklung der Informationssicherheit in sächsischen Kommunen

selbständig verfasst, nur die angegebenen Quelle und Hilfsmittel benutzt sowie alle Stellen der Arbeit, die wörtlich oder sinngemäß aus anderen Quellen übernommen wurden, als solche kenntlich gemacht habe und die Masterarbeit in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegt wurde.

Die gedruckte und digitalisierte Version der Masterarbeit sind identisch.

Dresden, 19. Februar 2020

Ort, Datum	Unterschrift Student/Studentin