Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Weg in die Basis-Absicherung (WiBA)

Vorgehensweise

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: wiba@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Ausgangslage und Hintergrund

Die Abhängigkeit der Verwaltungen von IT-gestützten Verfahren ist groß, der Grad an digitaler Vernetzung in Städten und Gemeinden wächst stetig. Gleichzeitig verschärfen sich Bedrohungslagen. Cyber-Angriffe nehmen zu und treffen regelmäßig die kommunale Ebene – mit fatalen Folgen.

Umso wichtiger ist die Informationssicherheit für die Kommunen. Informationssicherheit zielt darauf ab, Daten, Informationen und Infrastrukturen angemessen vor allen denkbaren Gefahren zu schützen. Informationssicherheit muss daher ganzheitlich gedacht werden. Neben technischen Aspekten, also klassischer IT-Sicherheit, spielen auch infrastrukturelle, organisatorische und personelle Themen eine wesentliche Rolle.

Ohne Informationssicherheit gibt es kein verlässliches und nachvollziehbares Verwaltungshandeln in Städten und Gemeinden, keine erfolgreiche Digitalisierung und letztendlich keine kommunale Daseinsvorsorge. Denn die Folgen von Angriffen auf die Informationssicherheit der Städte und Gemeinden können immens sein: Handlungsunfähige Behörden, die ihren gesetzlichen Auftrag nicht mehr erfüllen können, enorme wirtschaftliche Schäden, veröffentlichte sensible Datensätze, Desinformation etc. Die Angebote der kommunalen Daseinsvorsorge und die gesamte Arbeitsfähigkeit der Kommunen werden durch Sicherheitsvorfälle so massiv bedroht, dass das Gemeinwesen dadurch stark eingeschränkt werden kann.

Gleichwohl fehlt es insbesondere dem kommunalen Sektor häufig an personellen und finanziellen Ressourcen, um Standards zur Informationssicherheit angemessen umzusetzen. Insbesondere der Einstieg gestaltet sich oft zu komplex. Daher wurde durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Projekt „Weg in die Basis-Absicherung (WiBA)“ initiiert, um den Einstieg in den IT-Grundschutz praxisnäher zu gestalten und initiale Aufwände zu verringern.

Mittels Prüffragen, zusammengefasst in themenspezifischen Checklisten, wurde die Möglichkeit geschaffen, Sachstände zur Informationssicherheit zu erheben und umzusetzende Anforderungen zu identifizieren. Es ist dabei nicht notwendig, Kenntnis der Methodik des IT-Grundschutzes zu besitzen.

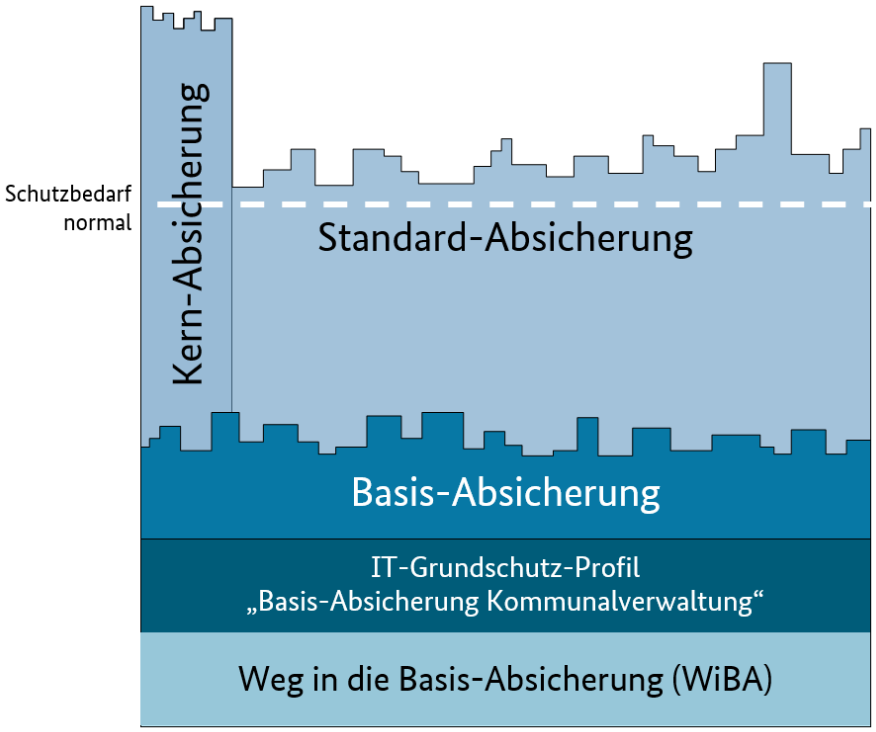

Abbildung 1 Einordnung von WiBA in bisherige Veröffentlichungen zum BSI-IT-Grundschutz

WiBA gliedert sich in die bisherigen Veröffentlichungen zum IT-Grundschutz unterhalb der Basis-Absicherung und des IT-Grundschutz-Profils „Basis-Absicherung Kommunalverwaltung“ ein (Abbildung 1). Die Prüffragen wurden auf Grundlage des IT-Grundschutz-Profils erstellt. Sie bilden die wesentlichen Aspekte ab, die bei einer Absicherung im kommunalen Bereich vorrangig betrachtet und tatsächlich umgesetzt werden müssen.

2 Abgrenzung

WiBA ist als Einstieg in die Informationssicherheit konzipiert, um die Hürde zur Umsetzung von anerkannten Standards der Informationssicherheit zu verringern.

WiBA selbst ist kein Standard für Informationssicherheit. Die Umsetzung von WiBA ist zum Veröffentlichungszeitpunkt nicht verpflichtend, sondern ein Angebot, um niedrigschwellig in die Informationssicherheit einzusteigen. WiBA ersetzt daher auch keine Umsetzung von anerkannten Standards der Informationssicherheit (z. B. BSI IT-Grundschutz oder ISO 27001). Für die erfolgreiche Etablierung eines Managementsystems für Informationssicherheit (ISMS) müssen weitere Maßnahmen über WiBA hinaus ergriffen werden.

WiBA betrachtet aus den genannten Gründen zudem keine Datenschutzanforderungen als solche und auch keine Anforderungen aus dem Geheimschutz. WiBA ist darüber hinaus bspw. nicht für Institutionen geeignet, die gemäß gesetzlicher Regelungen als KRITIS eingestuft werden (vgl. Kapitel 3).

3 WiBA-Checklisten

WiBA 2.0 basiert auf dem IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ in der Version 4.0 vom 23.11.2023 (IT-Grundschutz-Kompendium Edition 2023) und besteht im Kern aus den unten aufgeführten 19 Checklisten. Jede Liste behandelt einen Themenkomplex zur Informationssicherheit. Dabei kann es sich um organisatorische Aspekte (wie „Backup“ oder „Arbeiten außerhalb der Organisation“), technische Zielobjekte (wie „Client“ oder „Mobile Endgeräte“) oder Mischformen aus Organisation und Technik handeln (wie bei „IT-Administration“).

Die Checklisten betrachten als Informationsverbund grundsätzlich die eigentliche Kernverwaltung einer Kommune und berücksichtigen keine spezifischen Anforderungen an Fachverfahren oder evtl. vorhandenen Eigenbetriebe. Theoretisch kann auch eine Erst-Absicherung der Eigenbetriebe mit WiBA vorgenommen werden. Hierfür müssen ggf. Bereiche angepasst, ergänzt oder entfernt werden.

Die Checklisten betrachten zudem keine Kritischen Infrastrukturen. Für diese Bereiche gibt es spezielle gesetzliche Vorgaben, die über WiBA hinausgehen und daher gesondert betrachtet werden müssen.

Grundsätzlich ist jede Checkliste in sich geschlossen, sodass eine unabhängige Bearbeitung möglich ist. Aufgrund von thematischer Nähe oder inhaltlichen Überschneidungen kann es jedoch sinnvoll sein, eine bestimmte Reihenfolge einzuhalten.

Die vorgeschlagene Reihenfolge zur Bearbeitung der Checklisten (Abbildung 2) beginnt mit grundlegenden allgemeinen und organisatorischen Maßnahmen und berücksichtigt speziellere Themen im weiteren Verlauf. Checklisten zu verwandten Themen (farblich hinterlegt) sollten idealerweise gemeinsam bearbeitet werden. Die Reihenfolge ist nicht verbindlich und kann bei Bedarf an die individuellen Gegebenheiten angepasst werden. Auch eine parallele Bearbeitung der Checklisten ist möglich. Einen Überblick über eine mögliche Bearbeitungsreihenfolge und Priorisierung der einzelnen Checklisten gibt im Detail auch das Dokument „Weg in die Basis-Absicherung (WiBA) – Empfohlene Bearbeitungsreihenfolge“, das auf der BSI-Webseite zur Verfügung steht.

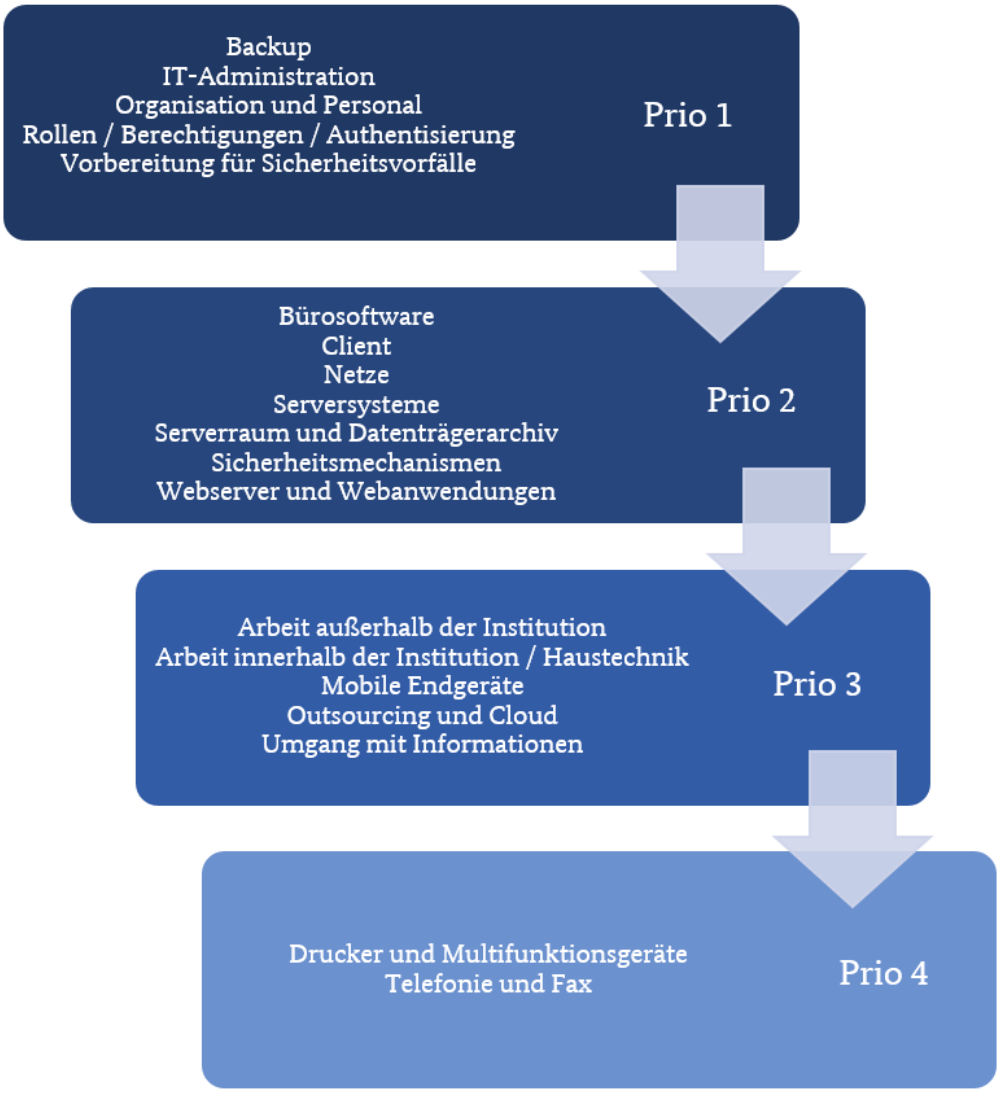

Abbildung 2 vorgeschlagene Reihenfolge zur Bearbeitung der WiBA-Checklisten gemäß IT-Grundschutz-Profil „Basis Absicherung Kommunalverwaltung“ in der Version 4.0 vom 23.11.2023.

Wichtig: Einige Checklisten müssen in der Regel mehrfach angewendet werden, beispielsweise wenn die eigene Institution unterschiedliche Clients verwendet oder mehrere Serverräume betreibt. In solchen Fällen erleichtert die mehrfache Anwendung eine gezielte, differenzierte Erfassung der Objekte und fördert die Übersichtlichkeit.

Checklisten können entfallen, sofern die darin behandelten Themen im eigenen Informationsverbund keine Rolle spielen. Dies gilt nicht für Bereiche, die von externen Dienstleistern übernommen werden (vgl. Kapitel 3.2).

3.1 Grundsätzliche Bearbeitungshinweise

Die Checklisten ermöglichen ein zweistufiges Vorgehen zur Anwendung von WiBA. Es sollte eine Person benannt werden, die die Umsetzung von WiBA federführend begleitet. Sofern ein/eine Informationssicherheitsbeauftragte/r (ISB) benannt wurde, ist es empfehlenswert, dass diese Person die Koordination zu WiBA übernimmt. Weitere Maßnahmen, bspw. die Übernahme der Gesamtverantwortung sowie die Festlegung von Zuständigkeiten und Ressourcen sind im Dokument „Weg in die Basis-Absicherung (WiBA): Management Summary – Aufgaben der Leitungsebene“ zu finden.

Zunächst wird ggf. unter Beteiligung von weiteren Fachkräften der Institution der Umsetzungsstatus geprüft, indem die Fragen gemäß der Checklisten mit „Ja“, „Nein“ oder „Nicht relevant“ beantwortet werden. Dabei werden bereits umgesetzte Anforderungen und damit ein Sachstand der Informationssicherheit ermittelt.

Wichtig: Bitte lesen Sie vor Beantwortung der Frage sorgfältig die Hinweise, die im Hilfsmittel angegeben sind. Sie konkretisieren häufig die Frage und geben Anhaltspunkte, wie die Anforderung umgesetzt werden könnte.

Die nicht umgesetzten Anforderungen sollten gesammelt und im Anschluss bezüglich der Umsetzungsreihenfolge priorisiert werden. Anhaltspunkte für eine Priorisierung können dabei die Aufwandsschätzung (siehe Kapitel 3.3.6.3 bzw. Abbildung 3) oder die vorgeschlagene Reihenfolge zur Bearbeitung der Checklisten (Abbildung 2) bieten. Hierauf geht das Dokument „Weg in die Basis-Absicherung – Empfohlene Bearbeitungsreihenfolge“ detaillierter ein. Es kann auch sinnvoll sein, zunächst Anforderungen aus eigentlich niedriger priorisierten Checklisten umzusetzen, wenn sie bspw. einen Quick Win darstellen oder offensichtliche, gravierende Schwachstellen schließen. Nach der Priorisierung sollten die Anforderungen sukzessive umgesetzt werden.

Für die Umsetzung gibt es keine „richtige“ oder „falsche“ Zeitspanne, innerhalb derer die Umsetzung erfolgen muss, da dies individuell von unterschiedlichsten Faktoren abhängig sein kann.

3.2 Externe Dienstleister

Sofern es einen bzw. mehrere externe Dienstleister gibt, die bestimmte Services übernehmen, sollten die Dienstleister die Checklisten ausfüllen, die deren jeweiligen Servicebereich betreffen. Insbesondere bei externen IT-Dienstleistungen ist zu erwarten, dass die Checklisten seitens der Dienstleister übererfüllt werden. Es empfiehlt sich dennoch, die Berücksichtigung und Umsetzung der Checklisten durch den IT-Dienstleister im Vertrag aufzunehmen.

3.3 Aufbau der WiBA-Checklisten

Jede WiBA-Checkliste ist gleich aufgebaut:

- Zugrundeliegende Bausteine des IT-Grundschutz-Kompendiums (Abschnitt 3.3.1)
- Bearbeitungsinformationen (Abschnitt 3.3.2)
- Ziel (Abschnitt 3.3.3)
- Allgemeiner Hinweis (Abschnitt 3.3.4)
- Ggf. weiterführende Informationen (Abschnitt 3.3.5)
- Prüffragen (Abschnitt 3.3.6)

Die einzelnen Bereiche werden in den folgenden Unterkapiteln im Detail beschrieben.

3.3.1 Zugrundeliegende Bausteine des IT-Grundschutz-Kompendiums

Als Referenz werden zu Beginn jeder Checkliste die IT-Grundschutz-Bausteine genannt, auf denen die Checkliste basiert. Dies dient einer transparenten Information und unterstützt auch bei der weiterführenden Bearbeitung.

3.3.2 Bearbeitungsinformationen

Die Bearbeitungsinformationen bestehen aus einer tabellarischen Übersicht mit insgesamt fünf Zellen.

Zelle 1 bietet die Möglichkeit, ein betrachtetes Zielobjekt zu nennen. Das jeweils zu betrachtende Zielobjekt (bspw. Mail-Server, File-Server etc.) ist hier einzutragen. Dies dient der Transparenz und

Nachvollziehbarkeit und ist zudem relevant, wenn bspw. verschiedene Clients verwendet oder unterschiedliche Serverräume betrachtet werden sollen, deren Absicherungsniveau unterschiedlich ausgestaltet ist.

Zelle 2 nennt die Anzahl der Prüffragen in der jeweiligen Checkliste.

In **Zelle 3** kann eingetragen werden, wie viele davon bereits umgesetzt sind (Umsetzungsstatus).

In **Zelle 4** ist das jeweilige Bearbeitungsdatum einzutragen.

In **Zelle 5** soll eine Person und/oder Rolle benannt werden, welche die Checkliste bearbeitet hat. Dabei kann es sich um unterschiedliche Personen bzw. Rollen handeln, je nach Checkliste und Zielobjekt.

In Kombination können die Zellen 2 bis 5 daher als interne Revisionsmöglichkeit dienen, um einen Überblick zu behalten, welche Checklisten bereits wann bearbeitet wurden und ob sich aus den Checklisten Handlungsbedarf ergibt (Delta zwischen Zelle 2 und 3).

3.3.3 Ziel

Im Abschnitt „Ziel“ wird der jeweils in der Checkliste betrachtete Themenkomplex kurz beschrieben und abgegrenzt. In der Regel finden sich Beispiele und allgemeine Gefährdungen in diesem Abschnitt.

3.3.4 Allgemeiner Hinweis

Der allgemeine Hinweis ist in jeder Checkliste wortgleich gehalten. Er dient insbesondere dazu, nochmals kurz die Ziele und Hintergründe, aber auch Grenzen von WiBA zu beschreiben. Dadurch können die Checklisten auch unabhängig voneinander genutzt und durch verschiedene Stellen bzw. Mitarbeitende bearbeitet werden.

3.3.5 Ggf. weiterführende Informationen

In einzelnen Checklisten ist zusätzlich ein Abschnitt mit weiterführenden Informationen hinterlegt. Dies ist dann der Fall, wenn es überblicksartige Veröffentlichungen gibt, die das Thema der Checkliste vertiefen.

3.3.6 Prüffragen

Die Prüffragen in den Checklisten sind ebenfalls immer gleich aufgebaut und bestehen neben der eigentlichen Prüffrage bzw. Anforderung aus folgenden Elementen:

- Antwortmöglichkeiten Ja / Nein / Nicht relevant (Abschnitt 3.3.6.1)
- Hilfsmittel (Abschnitt 3.3.6.2
- Aufwandsschätzung (Abschnitt 3.3.6.3)
- Notizen (Abschnitt 3.3.6.4)

Die einzelnen Bereiche werden in den folgenden Unterkapiteln im Detail beschrieben.

3.3.6.1 Antwortmöglichkeiten Ja / Nein / Nicht relevant

Jede Checkliste enthält eine Reihe von geschlossenen Fragen (Ja/Nein-Fragen), die essentielle Maßnahmen zur Informationssicherheit bzw. deren Umsetzungsstatus abfragen. Für eine erfolgreiche Umsetzung sollte jede Frage mit „Ja“ beantwortet werden können. Wird eine Frage mit „Nein“ beantwortet, so sind entsprechende Maßnahmen zur Erfüllung umzusetzen. Die Checklisten können somit auch zur Planung von notwendigen Maßnahmen genutzt werden.

Sofern abgefragte Bereiche für die Institution nicht zutreffen, kann die Antwort „nicht relevant“ gewählt werden. „Nicht relevant“ bedeutet, dass die Frage nicht beantwortet werden muss, weil bspw. die in der Frage erwähnten Produkte nicht eingesetzt werden. Es sollte in jedem Fall im Feld „Notizen“ kurz

dokumentiert werden, weshalb „nicht relevant“ ausgewählt wurde. „Nicht relevant“ darf nicht dazu verwendet werden, eine valide Prüffrage als unnötig zu deklarieren.

Beispiel:

Frage: Sind Faxgeräte so aufgestellt, dass eingehende Dokumente nicht von unberechtigten Personen eingesehen oder entnommen werden können?

Eine mögliche Begründung für die Auswahl von „nicht relevant“ wäre bspw., dass die Institution nur noch digitale Fax-Funktionen benutzt. Ein physisches Faxgerät ist nicht vorhanden, daher kann das Gerät unmöglich so aufgestellt werden, dass die eingehenden Dokumente nicht von unberechtigten Personen eingesehen oder entnommen werden können.

Ein gutes Hilfsmittel für die Entscheidung, ob „nicht relevant“ zutreffend ist, ist häufig die Frage, ob die Anforderung objektiv erfüllt werden könnte oder deren Umsetzung für jeden unmöglich wäre.

3.3.6.2 Hilfsmittel

Viele Fragen enthalten ein Hilfsmittel. Dieses dient u. a. dazu, die Frage näher zu erläutern und Begriffe zu definieren. Zudem werden praxisbewährte Hinweise gegeben, wie eine Anforderung konkret erfüllt werden kann und worauf dabei besonders zu achten ist. Hilfsmittel enthalten teilweise auch Verweise auf externe Dokumente, die zur einfacheren Umsetzung der Anforderungen herangezogen werden können. Einige der Verweise führen zu Dokumenten, die sich im internen Bereich der Sicherheitsberatung befinden.[1] Die Hilfsmittel sind zwar nicht verbindlich, aber in der Regel praxisbewährt, empfehlenswert und sinnvoll. Wo Hilfsmittel fehlen, freut sich das BSI über Ergänzungen aus der Praxis.

[1] https://www.bsi.bund.de/dok/SicherheitsberatungLK-Intern

3.3.6.3 Aufwandsschätzung

Jede Prüffrage enthält zudem eine Aufwandsschätzung in Form von vier Aufwandskategorien, die einen ersten Hinweis geben, wie komplex die Erfüllung bzw. Umsetzung der jeweiligen Frage ist. Die Definition „Aufwand“ gliedert sich dabei sowohl in zeitliche als auch finanzielle Aufwände.

Aufwands-kategorie	*Erläuterung*
1	Bei Maßnahmen der Kategorie 1 handelt es sich um sogenannte Quick Wins, welche i. d. R. im Zeitraum von einem Tag und/oder mit wenig Aufwand erreichbar sind. *Beispiel: Information an eine bestimmte Personengruppe.*
2	Maßnahmen der Kategorie 2 lassen sich mit geringem Aufwand üblicherweise in einem kurzen Zeitraum (max. einige Wochen) umsetzen. Die Umsetzung erfolgt dabei grds. in Eigenregie (kein externer Dienstleister erforderlich). *Beispiel: Erstellung einer Kontaktübersicht, die mit mehreren Fachbereichen abgestimmt werden muss.*
3	Die Umsetzung von Maßnahmen der Kategorie 3 sind etwas aufwendiger. Die Umsetzung benötigt in der Regel einige Monate Umsetzungszeit und kann eine externe Beteiligung erfordern. *Beispiel: Überprüfung von Konfigurationen in Software und ggf. Korrektur.*
4	Maßnahmen der Kategorie 4 sind aufwendig und häufig mit einer längerfristigen Umsetzung verbunden. Es wird Expertenwissen und oftmals auch eine Unterstützung von Dritten benötigt. *Beispiel: Initiierung und Umsetzung von Baumaßnahmen.*

Abbildung 3 Erläuterung der Kategorien für die Aufwandsschätzung.

3.3.6.4 Notizen

Das BSI empfiehlt, eine grundsätzliche und nachvollziehbare Dokumentation der internen Umsetzung von WiBA zu erstellen. Das Feld „Notizen“ bietet hierfür die Möglichkeit, die ausgewählte Antwort („Ja“, „Nein“, „Nicht relevant“) zu konkretisieren und damit eine kurze Dokumentation anzulegen.

Die Dokumentation dient u. a. der Nachvollziehbarkeit für Dritte in der Institution (z. B. Leitungsebene). So können bspw. nicht vollständig umgesetzte Anforderungen im Notizfeld beschrieben werden, sodass sich auch für Dritte erkennen lässt, welcher Teilbereich noch fehlt, bis die Anforderung mit „Ja“ beantwortet werden kann. Wenn Fragen bereits bejaht werden können, kann mit einer Dokumentation im Notizfeld die Umsetzungsart nachvollzogen werden.

4 Tipps und Tricks

Im Nachfolgenden haben wir einige Tipps und Tricks zusammengestellt, die bei der Umsetzung von WiBA unterstützen können.

4.1 Über den Tellerrand hinausblicken

Häufig sind Maßnahmen im Bereich der Informationssicherheit bereits gelebte Praxis und/oder werden in Bereichen ebenfalls geprüft, die nicht originär der Informationssicherheit zuzuordnen sind. Hier helfen die Anforderungen, einen besseren Überblick über den Sachstand zu erhalten. Zudem können Maßnahmen durch die Hilfsmittel oft noch verbessert werden. Wichtig ist nicht, woher die Anforderungen kommen, wichtig ist, dass diese umgesetzt sind!

Beispiel: Eine jährliche Datenschutzschulung behandelt bereits u. a., dass Mitarbeitende ihren Bildschirm sperren müssen, wenn sie den Arbeitsplatz verlassen, damit Unbefugte keinen Zugriff auf vertrauliche Informationen erhalten. Dadurch kann bspw. die entsprechende Prüffrage 2 der Checkliste „Client" bejaht werden, ohne neue Maßnahmen ergreifen zu müssen.

4.2 Austausch pflegen

Selten sind Probleme so speziell, dass sie nicht schon in einer anderen Institution genauso aufgetreten wären. Eine Vernetzung mit anderen Fachkräften aus benachbarten Kommunen kann helfen, um sich gegenseitig zu unterstützen.

Eine weitere Möglichkeit zur Vernetzung ist das IT-SiBe-Forum[2]. Das Forum als nichtöffentliches Netzwerk dient dem Informations- und Erfahrungsaustausch zwischen Beschäftigten der Kommunal- und Landesverwaltung im Kontext Informationssicherheit. Der Betrieb wird vom Deutschen Landkreistag getragen. Der Deutsche Städtetag, der Deutsche Städte- und Gemeindebund und das Bundesamt für Sicherheit in der Informationstechnik unterstützen die Initiative.

[2] https://info.it-sibe-forum.de/it-sibe-forum-de/kurzinformation

5 Ausblick – Was kommt nach WiBA?

Bei WiBA handelt es sich um die wesentlichen Aspekte, die bei der Absicherung vorrangig betrachtet werden müssen. Es ist ein Teilbereich des IT-Grundschutzes, der als Grundlage für den Aufbau einer Basis-Absicherung dienen kann. WiBA orientiert sich am IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ und ermöglicht mit wenig Aufwand einen ersten wichtigen Schritt in die Informationssicherheit. Dennoch handelt es sich nicht um ein vollumfängliches Managementsystem für Informationssicherheit (ISMS). Daher empfehlen wir in einem Folgeschritt die Umsetzung des IT-Grundschutz-Profils „Basis-Absicherung Kommunalverwaltung“.

6 Mapping WiBA – IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“

Um nach WiBA nahtlos das IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ umsetzen zu können, stellt das BSI eine Mappingtabelle[3] zur Verfügung. Wir empfehlen ein Mapping auf das aktuelle IT-Grundschutz-Profil 4.0 aufgrund der relevanten Erweiterung des Profils um mehrere Bausteine.

Die Mappingtabelle stellt den Zusammenhang zwischen den Prüffragen der WiBA-Checklisten und den Anforderungen des IT-Grundschutz-Profils dar. So kann einfach abgeglichen werden, welche Anforderungen aus dem IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ bereits durch WiBA erfüllt werden und welche noch bearbeitet werden müssen.

Die Mappingtabelle beschreibt für jede Anforderung aus dem IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“, welche Prüffrage den entsprechenden Aspekt behandelt. Mit Blick auf den Umfang der Tabelle ist es ratsam, bei der Bearbeitung die Sortierfunktion bzw. einen Filter zu nutzen. Wenn die Prüffrage mit „Ja“ beantwortet wurde, ist auch die entsprechende Anforderung erfüllt. In einigen Fällen sind Anforderungen aus dem Profil nicht unmittelbar in eine Prüffrage eingeflossen, sondern wurden als Hilfsmittel zu einer Prüffrage aufgenommen. Dann muss im Einzelfall geprüft werden, ob die Anforderung durch die Umsetzung der Empfehlungen im Hilfsmittel entsprechend erfüllt wurde, oder ob noch weitere Maßnahmen notwendig sind. Darüber hinaus sind Anforderungen teilweise auch in mehreren Prüffragen oder Hilfsmitteln aufgegangen. In diesem Fall ist die Anforderung in der Mappingtabelle mehrfach aufgeführt und gilt erfüllt, wenn alle zugeordneten Prüffragen bzw. Empfehlungen aus den Hilfsmitteln umgesetzt wurden.

Die Anforderungen des Bausteins ISMS.1 *Sicherheitsmanagement* sind im Dokument „Management Summary – Aufgaben der Leitungsebene“ aufgegangen. Hier muss ebenfalls geprüft werden, ob die Anforderungen durch entsprechende Maßnahmen erfüllt wurde, oder ob noch weitere Maßnahmen notwendig sind.

Für detailliertere Informationen zur Verwendung der Mappingtabelle ist im entsprechenden Dokument das Tabellenblatt „Anleitung“ enthalten.

Sofern bereits WiBA in der Version 1.0 umgesetzt wurde, empfehlen wir, dass zunächst mit Hilfe des „Änderungsdokument WiBA“ auf WiBA 2.0 gewechselt wird, d. h. dass geprüft wird, welche Fragen zwischen WiBA 1.0 und WiBA 2.0 eine Änderung erfahren haben bzw. neu hinzugekommen sind. Mit dem Stand von WiBA 2.0 kann dann auf das aktuelle IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ Version 4.0 gemappt werden.

Neben der Mappingtabelle steht auf der BSI-Webseite auch ein Tool für die Umsetzung von WiBA zur Verfügung. Zudem werden im internen Bereich der BSI-Sicherheitsberatung für Länder und Kommunen[4] weitere Arbeitshilfen für die Umsetzung der Basis-Absicherung und Informationen über aktuelle Schwachstellen und Bedrohungen angeboten.

[3] https://www.bsi.bund.de/dok/wiba
[4] https://www.bsi.bund.de/dok/SicherheitsberatungLK-Intern