Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Weg in die Basis-Absicherung (WiBA)

Empfohlene Bearbeitungsreihenfolge

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

1 Ziel der Priorisierung

Die Prüffragen wurden auf Grundlage des IT-Grundschutz-Profils „Basis-Absicherung Kommunalverwaltung“ erstellt. Sie bilden die wesentlichen Aspekte ab, die bei einer Absicherung im kommunalen Bereich vorrangig betrachtet und tatsächlich umgesetzt werden müssen. Der Weg in die Basis-Absicherung kommt dabei jedoch ohne eine Methodik wie beispielsweise ISO 27001 aus.

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** beginnt mit grundlegenden allgemeinen und organisatorischen Maßnahmen und berücksichtigt speziellere Themen im weiteren Verlauf. Die Reihenfolge ist nicht verbindlich und kann bei Bedarf an die individuellen Gegebenheiten angepasst werden. Auch eine parallele Bearbeitung der Checklisten ist möglich. Insbesondere durch die Zuordnung bestimmter Themen zu unterschiedlichen Rollen in der Institution wird eine parallele Bearbeitung der Checklisten ermöglicht (z. B. zeitgleiche Bearbeitung der Checkliste „Backup“ durch die IT und der Checkliste „Arbeit innerhalb der Institution / Haustechnik“ durch die Haustechnik/Innerer Dienst).

Das BSI empfiehlt die im folgenden Kapitel dargestellte Bearbeitungsreihenfolge. Dabei liegen folgende Kriterien zugrunde:

a) Die Gefährdungslage für kommunale Einrichtungen[1]
b) Zweckdienliche Reihenfolge (allgemein vor konkret)

Mit „Bearbeitungsreihenfolge“ ist NICHT gemeint, dass alle Maßnahmen der Checklisten der Priorität 1 umgesetzt sein müssen, bevor sich den anderen Checklisten gewidmet wird.

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.

Innerhalb der Checklisten beginnen die Prüffragen in der Regel ebenfalls mit grundlegenden, allgemeinen Maßnahmen, die aufeinander aufbauend formuliert sind. Sie führen damit mit einer Art roter Faden durch die Thematik der jeweiligen Checkliste. So ergibt sich innerhalb der jeweiligen Checkliste eine natürliche Priorisierung durch die aufeinander aufbauenden Prüffragen.

Beispiel: Die Checkliste „Backup“ fragt zunächst, ob festgelegt wurde, **welche** Daten gesichert werden sollen und im Anschluss, ob festgelegt wurde, **in welchem zeitlichen Abstand** diese Daten gesichert werden.

Auch innerhalb der Checklisten kann es zweckmäßig sein, von der vorgegebenen Reihenfolge der Prüffragen abzuweichen. Das ist bspw. der Fall, wenn eine Prüffrage schnell und mit wenig Aufwand umgesetzt werden kann (Quick Win, Aufwandskategorie 1).

[1] Vgl. Die Lage der IT-Sicherheit in Deutschland 2023, BSI, 2023, Seite 68.

2 Empfohlene Priorisierung der Checklisten

Aus den in Kapitel 1 genannten Kriterien folgt die folgende Bearbeitungsreihenfolge. Wie beschrieben, ist diese jedoch von den jeweiligen Rahmenbedingungen vor Ort abhängig und damit entsprechend von der Organisation anpassbar.

2.1 Priorität 1

Folgende Checklisten sollten als erstes bearbeitet werden. Diese sind die Grundlage für die weiteren Checklisten und haben entsprechend große Auswirkungen auf diese. Die Maßnahmen dienen zudem dazu die größten Cyberrisiken für Kommunen zu reduzieren.

- Backup
- IT-Administration
- Organisation und Personal
- Rollen / Berechtigungen / Authentisierung
- Vorbereitung für Sicherheitsvorfälle

2.2 Priorität 2

Nachfolgend zu den unter 2.1 genannten Checklisten, wird seitens des BSI empfohlen, danach möglichst diese Checklisten zu bearbeiten, um insbesondere die am meisten sensitiven IT-Systeme, die regelmäßig Ziele von Angriffen sind, zu schützen.

- Bürosoftware
- Client
- Netze
- Serversysteme
- Serverraum und Datenträgerarchiv
- Sicherheitsmechanismen
- Webserver und Webanwendungen

Sinnvollerweise sollten die Checklisten „Client“, „Sicherheitsmechanismen“ und „Bürosoftware“ zusammen bearbeitet werden. Gleiches gilt für „Serversysteme“ und „Serverraum und Datenträgerarchiv“.

2.3 Priorität 3

Nachdem die wichtigsten organisatorischen und technischen Checklisten bearbeitet wurden, sollte sich mit der Absicherung der innerhalb und außerhalb der Organisation bearbeitenden Informationen gewidmet werden:

- Arbeit außerhalb der Institution
- Arbeit innerhalb der Institution / Haustechnik
- Mobile Endgeräte
- Outsourcing und Cloud
- Umgang mit Informationen

Hier sollten sinnvollerweise die Checklisten „Arbeit außerhalb der Institution“ und „Mobile Endgeräte“ zusammen bearbeitet werden.

2.4 Priorität 4

Die Checklisten mit der geringsten Priorität sind:

- Drucker / Multifunktionsgeräte
- Telefonie und Fax

Diese können daher am Ende bearbeitet werden.

2.5 Grafische Übersicht der Bearbeitungsreihenfolge