Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Weg in die Basis-Absicherung (WiBA)

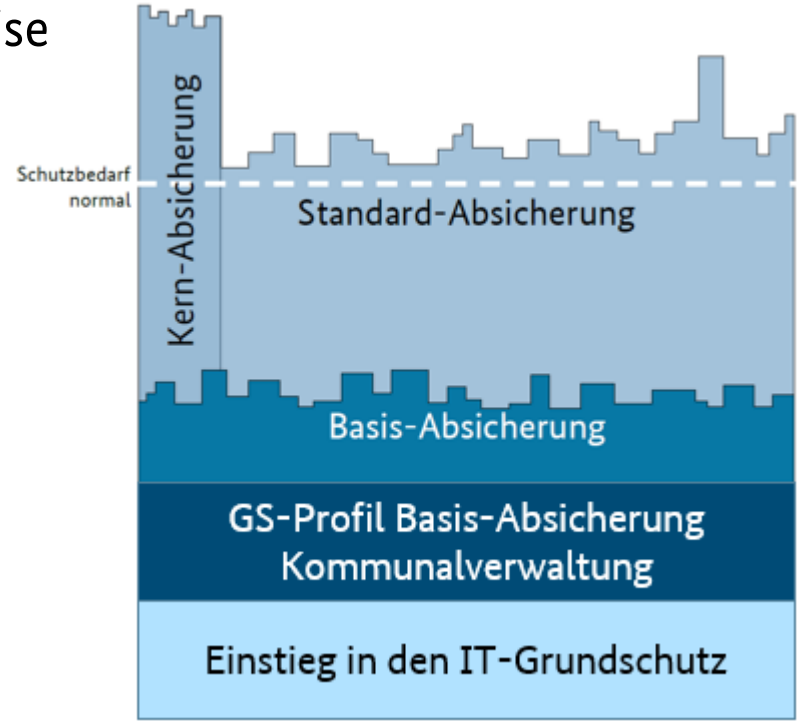
Einstieg in den BSI IT-Grundschutz

Kommunaler IT-Sicherheitskongress (KITS) | 24.04.2023

Michaela Hansert, BSI Referat BL 12 – Informationssicherheitsberatung für Länder und Kommunen

Ausgangslage und Lösungsansatz

- Einstieg in den BSI IT-Grundschutz trotz Basis-Absicherung teilweise zu komplex: vielen kleinen Institutionen fehlen ausreichend Ressourcen und Know-How
- Im Fokus des „Weges in die Basis-Absicherung“: Kommunen
- Ziel: Ohne (tiefere) Kenntnis der Methodik können Sachstände erhoben und umzusetzende Anforderungen mittels Prüffragen und Checklisten mit wenig Aufwänden identifiziert werden.
- Es werden Hilfsmittel bereitgestellt, die bei der Umsetzung unterstützen
- Im Anschluss kann das IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ nahtlos umgesetzt werden.



Vorgehensweise

- Clusterung der **51** relevanten Bausteine in **19** themenspezifischen Checklisten
  - Festlegung eines möglichst praxisnahen Sicherheitsniveaus für den Einstieg (Reduktion auf wesentliche Anforderungen/Maßnahmen)
  - Bereitstellung von Hilfsmitteln / weitergehenden Informationen zur Unterstützung
  - Formulierung von konkreten Fragen
  - Verschmelzung von verschiedenen Bausteinanforderungen zu (thematisch sortierten) Prüffragen
  - Kostenschätzung (Kategorie 1 bis 4) zur Erleichterung der Priorisierung der Maßnahmen
- Erstellung eines „Kennzeichens“ bei Umsetzung der Prüffragen
- Einbindung von Modellkommunen: über kommunale Spitzenverbände

Praxis-Test der Checklisten

- Einbindung der AG koBA
- Einbindung von Modellkommunen
  - Bewerbungs- und Auswahlverfahren über und mit den Kommunalen Spitzenverbänden (DLT, DST, DStGB)
  - über 130 Bewerbungen quer über die Bundesländer verteilt
  - gemeinsame Auswahl auf Basis von z. B. Größe, Kommunalebene, geographische Verteilung, ...
  - zwei sehr kleine Kommunen, zwei mittelgroße Kommunen, eine große Stadt, ein Landkreis
  - jeweils dreitägige Workshops ab Anfang Mai

Zeitplan

Gründung Projektgruppe

Entwicklung der „Einstiegsmethodik“

Identifizierung relevanter Bausteine und Anforderungen, Formulierung der Fragen

Erstellung der Dokumentation (Dokumente, Checklisten)

Einbindung der kommunalen Stakeholder (AG KoBa, KSV, ggf. IT-SiBe-Forum)

Pilotierung des finalen Produkts mit Modellkommunen

Veröffentlichung

Einstieg in den IT-Grundschutz

Geplante Checklisten

- „Allgemeine Aspekte“ / Vorgehensweise
- Arbeit außerhalb der Institution
- Arbeit innerhalb der Institution / Haustechnik
- Backup
- Client
- Drucker / Multifunktionsgeräte
- IT-Administration
- Mobile Endgeräte
- Netze
- Organisation und Personal
- Outsourcing
- Bürosoftware
- Rollen und Rechte / Authentisierung
- Serverraum
- Serversysteme
- Sicherheitsmechanismen
- Telefonie und Fax
- Umgang mit Informationen
- Vorbereitung für Sicherheitsvorfälle

Clusterbildung: Beispiele

- „Serversysteme“
  - SYS.1.1 allg. Server, SYS.1.5 Virtualisierung, APP 2.1 allg. Verzeichnisdienst, APP.3.3 Fileserver, APP.5.3 Allg. E-Mail-Client und –Server
- „Umgang mit Informationen“
  - CON.6 Löschen und Vernichten, CON.9 Informationsaustausch
- „Arbeit außerhalb der Institution“
  - OPS.1.2.4 Telearbeit, INF.8 Häuslicher Arbeitsplatz, INF.9 Mobiler Arbeitsplatz, INF.11 Allgemeines Fahrzeug
- „Outsourcing und Cloud“
  - OPS.2.1 Outsourcing für Kunden, OPS.2.2 Cloud-Nutzung

Beispiel Herabsenkung von Anforderungen für Einstieg

ID-Anforderung	Titel	Inhalt	Typ	im GS-Profil	berücksichtigen	Begründung für Nicht-Berücksichtigung	Checkfrage
OPS.2.1.A1	Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben	Alle Sicherheitsanforderungen für ein Outsourcing-Vorhaben MÜSSEN auf Basis einer Strategie zum Outsourcing festgelegt sein und beide Outsourcing-Parteien MÜSSEN sich vertraglich dazu verpflichten, den IT-Grundschutz oder ein vergleichbares Schutzniveau einzuhalten.	Basis	ja	ja		Werden Sicherheitsanforderungen durch den Outsourcing-Dienstleister erfüllt?

Prüffragen

Nr.	Zu prüfende Anforderung	Aufwand	Erfüllt	
			Ja	Nein
1	Werden die Sicherheitsanforderungen der Institution durch den Outsourcing-Dienstleister erfüllt?	-		
	Es sollten mindestens die Anforderungen der Checklisten aus der Einstiegsstufe erfüllt werden. *Die Verpflichtung sollte vertraglich erfolgt sein.*			
	Notizen			

Beispiel Konsolidierung von Anforderungen

ID-Anforderung	Titel	Inhalt	Typ	im GS-Profil	berücksichti	Begründung für Nicht-Berücksichtigung
OPS.1.1.2.A7	Regelung der IT-Administrationstätigkeit	Die Befugnisse, Aufgaben und Pflichten der Administratoren SOLLTEN in einer Arbeitsanweisung oder Richtlinie verbindlich festgeschrieben werden.	Standard	Ja	nein	in Checkliste "Personal und Organisation" in Anforderung 2
OPS.1.1.2.A7	Regelung der IT-Administrationstätigkeit	Die Aufgaben zwischen den einzelnen Administratoren SOLLTEN so verteilt werden, dass einerseits Überschneidungen in den Zuständigkeiten vermieden werden und andererseits keine Administrationslücken entstehen.	Standard	Ja	nein	in Checkliste "Personal und Organisation" in Anforderung 1 (Hilfsmittel) aufgegangen

Nr.	Zu prüfende Anforderung	Aufwand	Erfüllt	
			Ja	Nein
1	Wurde für alle Geschäftsprozesse, Anwendungen, IT-Systeme, Räume und Gebäude sowie Kommunikationsverbindungen festgelegt, wer für diese und deren Sicherheit zuständig ist?	✊✊		
	Die Aufgaben sollten so verteilt werden, dass einerseits Überschneidungen in den Zuständigkeiten vermieden werden und andererseits keine Lücken entstehen. *Die Festlegung kann dabei in verschiedenen Dokumenten bspw. im Geschäftsverteilungsplan oder dem Assetmanagement erfolgen.* *Die Zuständigkeit liegt dabei in der Regel nicht allein beim ISB, sondern je nach Zielobjekt (Anwendung, IT-System…) bei Admins, Fachverfahrensverantwortlichen usw.*			
	Notizen			

Nr.	Zu prüfende Anforderung	Aufwand	Erfüllt	
			Ja	Nein
2	Wurden die Personen darüber informiert, welche Zuständigkeiten sie haben und welche Aufgaben, Pflichten und Befugnisse sie in diesem Kontext wahrnehmen?	✊		
	Die Information sollte schriftlich erfolgen.			
	Notizen			

Deutschland Digital•Sicher•BSI•

Wir entwickeln eine praxisnahe Einstiegsstufe in die Informationssicherheit, um Sie bedarfsgerecht zu unterstützen!

Vielen Dank für Ihre Aufmerksamkeit!

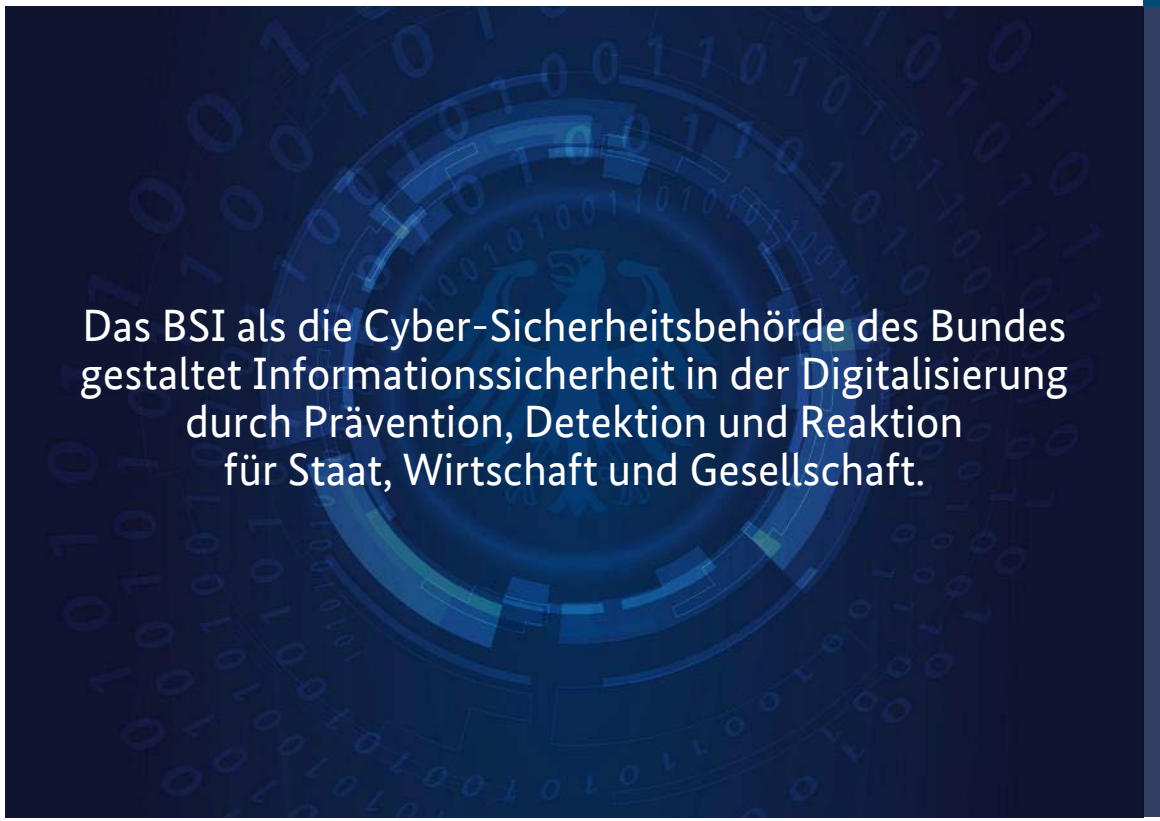
Deutschland
Digital•Sicher•BSI•

Kontakt

Projektgruppe „Weg in die Basis-Absicherung“

Kontakt über:
basisabsicherung@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de



Bundesamt
für Sicherheit in der
Informationstechnik