§ 2 ITSiV-PV — Portalverbund und unmittelbar angebundene IT-Komponenten

IT-Sicherheitsverordnung Portalverbund
Stand: 20.01.2022 (konsolidierte Textfassung, kein amtliches Inkrafttretensdatum)

(1) Für den Portalverbund und für IT-Komponenten nach § 1 Absatz 4 Nummer 1 sind zur Gewährleistung der IT-Sicherheit Maßnahmen nach dem Stand der Technik zu treffen.

(2) Die Einhaltung des Standes der Technik im Sinne von Absatz 1 wird vermutet, wenn die in der Anlage aufgeführten Standards in Form von Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik in der jeweils geltenden Fassung eingehalten werden. Die jeweils geltende Fassung der Anlage wird im Bundesanzeiger durch Verweis auf die Internetseite des Bundesamtes für Sicherheit in der Informationstechnik bekanntgegeben. Bei Fortschreibung einer Technischen Richtlinie gilt die Vermutung nach Satz 1 für zwei Jahre ab Bekanntgabe der Fortschreibung im Bundesanzeiger fort, soweit durch das Bundesministerium des Innern und für Heimat keine andere Umsetzungsfrist vorgegeben wird.

(3) Weitere Technische Richtlinien sowie neuere Versionen von Technischen Richtlinien nach Absatz 2 werden durch das Bundesamt für Sicherheit in der Informationstechnik im Benehmen mit den Ländern erarbeitet. Die erarbeiteten Technischen Richtlinien sind dem Bundesministerium des Innern und für Heimat zur Zustimmung vorzulegen. Nach der Zustimmung durch das Bundesministerium des Innern und für Heimat erfolgt eine Bekanntgabe der Technischen Richtlinien durch das Bundesamt für Sicherheit in der Informationstechnik nach Absatz 2 Satz 2.

(4) Die genutzten IT-Komponenten müssen einem Informationssicherheitsmanagementsystem unterliegen, welches die Vorgaben der aktuell gültigen Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung des IT-Planungsrates umsetzt.

(5) Die für die genutzten IT-Komponenten verantwortlichen Stellen erstellen und setzen ein IT-Sicherheitskonzept um, das den Standards 200-1, 200-2 und 200-3 des Bundesamtes für Sicherheit in der Informationstechnik oder den Vorgaben der ISO/IEC 27001 in der jeweils geltenden Fassung entspricht. Mindestanforderung ist die Umsetzung der Standard-Absicherung nach BSI Standard 200-2.

(6) IT-Komponenten, die über eine technische Schnittstelle unmittelbar mit dem Internet verbunden sind, und alle sonstigen IT-Komponenten mit einem nach BSI IT-Grundschutz hohen oder sehr hohen Schutzbedarf in mindestens einem der Schutzziele Vertraulichkeit, Integrität oder Verfügbarkeit sind vor Anbindung an den Portalverbund einem Penetrationstest und einem Webcheck nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik zu unterziehen. Zu den IT-Komponenten nach Satz 1 zählen insbesondere Nutzerkonto, elektronischer Bezahldienst, Postfach und Datensafe.

(7) Penetrationstests und Webchecks sind spätestens nach drei Jahren oder bei größeren Änderungen der in Absatz 6 genannten IT-Komponenten zu wiederholen.

(8) Penetrationstests und Webchecks für IT-Systeme der Bundesverwaltung werden vom Bundesamt für Sicherheit in der Informationstechnik oder durch vom Bundesamt für Sicherheit in der Informationstechnik zertifizierte IT-Sicherheitsdienstleister durchgeführt. IT-Systeme der Länder werden durch Fachbehörden für Informationssicherheit der Länder oder durch vom Bundesamt für Sicherheit in der Informationstechnik zertifizierte IT-Sicherheitsdienstleister einem Penetrationstest und einem Webcheck unterzogen.

(9) IT-Sicherheitsdienstleister, die über keine Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik verfügen, können von der für die IT-Komponente verantwortlichen Stelle ersatzweise mit der Prüfung beauftragt werden, sofern zertifizierte IT-Sicherheitsdienstleister nicht zur Verfügung stehen und der Penetrationstest und der Webcheck nach den Vorgaben des Bundesamtes für Sicherheit

in der Informationstechnik durchgeführt werden.

(10) Das Bundesamt für Sicherheit in der Informationstechnik, die Fachbehörden für Informationssicherheit der Länder oder die beauftragten IT-Sicherheitsdienstleister haben die Prüfberichte spätestens sechs Wochen nach Durchführung des Penetrationstests oder Webchecks der jeweiligen verantwortlichen Stelle zur Kenntnis zu bringen.

(11) Die genutzten IT-Komponenten müssen einem IT-Notfallmanagement unterliegen, das die Anforderungen der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung des IT-Planungsrates in der jeweils geltenden Fassung erfüllt.

(12) Die Umsetzung der Vorgaben der Absätze 1 bis 11 obliegt der für die jeweilige IT-Komponente verantwortlichen Stelle. Werden IT-Komponenten von Dienstleistern betrieben, bleibt die auslagernde Stelle verantwortlich für die Erfüllung der Anforderungen dieser Verordnung. Die Umsetzung der Maßnahmen ist für die IT-Komponenten im Portalverbund durch eine jährliche Eigenerklärung der für die jeweilige IT-Komponente verantwortlichen Stelle zu dokumentieren. Ein verbindliches Erklärungsmuster wird durch das Bundesministerium des Innern und für Heimat bereitgestellt. Die jeweils geltende Fassung des Erklärungsmusters wird im Bundesanzeiger durch Verweis auf die Internetseite des Bundesamtes für Sicherheit in der Informationstechnik bekanntgegeben.

(13) Verantwortliche Stellen des Bundes übermitteln die Eigenerklärung bis zum 1. Januar eines Kalenderjahres der zentralen Stelle des Bundes. Verantwortliche Stellen in den Ländern hinterlegen die Erklärung bis zum 1. Januar eines Kalenderjahres bei der jeweiligen zentralen Stelle des Landes. Die zentrale Stelle für den Bund und das Verfahren zur Abgabe der Erklärungen im Bund werden durch das Bundesministerium des Innern und für Heimat bestimmt. Die Länder legen die für ihren jeweiligen Zuständigkeitsbereich zentrale Stelle und das Verfahren zur Abgabe der Erklärungen fest.