Verordnung zur Gewährleistung der IT-Sicherheit der im Portalverbund und zur Anbindung an den Portalverbund genutzten IT-Komponenten (IT-Sicherheitsverordnung Portalverbund - ITSiV-PV)

ITSiV-PV

Ausfertigungsdatum: 06.01.2022

Vollzitat:

"IT-Sicherheitsverordnung Portalverbund vom 6. Januar 2022 (BGBl. I S. 18)"

Fußnote

(+++ Textnachweis ab: 20.1.2022 +++)

Eingangsformel

Auf Grund des § 5 Satz 1 des Onlinezugangsgesetzes vom 14. August 2017 (BGBl. I S. 3122, 3138), der zuletzt durch Artikel 77 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist, in Verbindung mit § 1 Absatz 2 des Zuständigkeitsanpassungsgesetzes vom 16. August 2002 (BGBl. I S. 3165) und dem Organisationserlass vom 8. Dezember 2021 (BGBl. I S. 5176) verordnet das Bundesministerium des Innern und für Heimat:

§ 1 Begriffsbestimmungen

(1) Soweit in dieser Verordnung Begriffe Verwendung finden, die in § 2 des Onlinezugangsgesetzes definiert werden, finden die dortigen Begriffsbestimmungen auch für den Geltungsbereich dieser Verordnung Anwendung.

(2) Soweit in dieser Verordnung Begriffe Verwendung finden, die in § 2 des BSI-Gesetzes definiert werden, finden die dortigen Begriffsbestimmungen auch für den Geltungsbereich dieser Verordnung Anwendung.

(3) IT-Sicherheit der IT-Komponenten im Sinne dieser Verordnung bezeichnet die Einhaltung bestimmter Sicherheitsstandards, welche die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen sicherstellen, die durch IT-Komponenten im Portalverbund und in IT-Komponenten zur Anbindung an den Portalverbund verarbeitet werden.

(4) IT-Komponenten zur Anbindung an den Portalverbund im Sinne dieser Verordnung sind

1. die von Bund und Ländern betriebenen informationstechnischen Systeme, die unmittelbar Daten mit dem Portalverbund austauschen, und
2. mittelbar an den Portalverbund angebundene informationstechnische Systeme öffentlicher Stellen, die sich für die Anbindung der Dienste der in Nummer 1 genannten Stellen bedienen.

§ 2 Portalverbund und unmittelbar angebundene IT-Komponenten

(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.

§ 3 Mittelbar angebundene IT-Komponenten

Stellen nach § 1 Absatz 4 Nummer 2 sind auf der Grundlage angemessener Nutzungsbedingungen anzubinden. Sie erstellen und setzen für die zum Datenaustausch mit dem Portalverbund eingesetzten IT-Komponenten ein Sicherheitskonzept um, das den Standards 200-1, 200-2 und 200-3 des Bundesamtes für Sicherheit in der Informationstechnik in der jeweils geltenden Fassung oder einem vergleichbaren vom Land anerkannten Standard entspricht. Mindestanforderung ist die Umsetzung der Basis-Absicherung nach BSI Standard 200-2.

§ 4 Übergangsregelung

(1) Für IT-Komponenten im Portalverbund und für IT-Komponenten zur unmittelbaren Anbindung an den Portalverbund nach § 1 Absatz 4 Nummer 1, die zum Zeitpunkt des Inkrafttretens dieser Verordnung in Betrieb sind oder bis zum 30. Juni 2022 in Betrieb genommen werden,

1. kann bis zum 31. Dezember 2022 von den Vorgaben des § 2 Absatz 6 abgewichen werden,
2. kann in begründeten Fällen bis zu zwei Jahre nach Inkrafttreten dieser Verordnung von den Regelungen der in der Anlage zu dieser Verordnung genannten Technischen Richtlinien abgewichen werden.

(2) Die Abweichungen sind zu dokumentieren.

§ 5 Inkrafttreten

Diese Verordnung tritt am Tag nach der Verkündung in Kraft.

Anlage (zu § 2 Absatz 2)

(Fundstelle: BGBl. I 2022, 20)

1. BSI TR-03160 Servicekonten
2. BSI TR-03107-1 Elektronische Identitäten und Vertrauensdienste im E-Government Teil 1
3. BSI TR-03147 Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen
4. BSI TR-03116-4 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 4