CDPS
TUM CENTER FOR DIGITAL PUBLIC SERVICES

Tabellarische Übersicht der Anforderungen an die IT-Sicherheit der Kommunen nach der ITSiV-PV

Ass. iur. Nicolas Ziegler und Stud. iur. et inform. Julian Hofmann

TUM Center for Digital Public Services
Lehrstuhl für Recht und Sicherheit der Digitalisierung
Technische Universität München

Direktor
Univ.-Prof. Dr. jur.
Dirk Heckmann
dirk.heckmann@tum.de

Geschäftsführerin
Assessorin jur.
Sarah Rachut
sarah.rachut@tum.de

Kontakt
Tel. +49 89 90 77 93 300
www.tum-cdps.de
www.gov.tum.de/elaw

Vorbemerkung

In nachfolgender Tabelle werden die IT-Sicherheitsanforderungen nach ITSiV-PV für Kommunen dargestellt. Die Anforderungen gelten nicht für die gesamte IT der Kommunen, sondern „nur“ für IT-Komponenten, die im Portalverband genutzt werden oder der Anbindung an den Portalverbund dienen.[1] Zentral im Anwendungsbereich der ITSiV-PV ist die **Unterscheidung zwischen § 2 und § 3**: § 2 gilt nur für **unmittelbar** angebundene IT-Komponenten, also für Kommunen, die selbst Verwaltungsportale unterhalten, die unmittelbar an den Portalverbund angeschlossen werden und mittels technischer Schnittstellen Daten mit dem Portalverbund austauschen. Informationsportale, die lediglich auf Informationen innerhalb des Verbunds verlinken fallen nicht unter den Anwendungsbereich. § 3 gilt nur für **mittelbar** angebundene IT-Komponenten, die nach § 1 Abs. 4 ITSiV-PV für die Anbindung an den Portalverbund **auf Portale von Bund und Länder zugreifen**, die wiederum unmittelbar Daten mit dem Portalverbund austauschen. **§ 3 erfordert deutlich weniger Schutzmaßnahmen,** da das Verbundrisiko hier geringer ausfällt. Der weitergehende § 2 ITSiV-PV gilt im Ergebnis daher faktisch nur für größere und leistungsfähigere Kommunen, die eigene Verwaltungsportale unterhalten.

Bis auf die Eigenerklärung nach § 2 Abs. 12 ITSiV-PV sind **sämtliche Arbeitsschritte einem IT-Outsourcing zugänglich**. Die Schranke des Art. 33 Abs. 4 GG verhindert ein IT-Outsourcing selbst bei extensiver Auslegung nicht, wenn es sich lediglich um technische Hilfsfunktionen handelt und diese nicht in den administrativen Entscheidungsprozess eingebunden sind, dass sie inhaltlich auf einen außenwirksamen Akt Einfluss nehmen.[2] Bei der Wahrung von IT-Sicherheit handelt es sich um eine Meta-Aufgabe, die ordnungsgemäßes Verwaltungshandeln im Portalverbund erst ermöglicht. Eine hoheitsrechtliche Befugnis im Sinne des Art. 33 Abs. 4 GG ist hierin nicht zu sehen. Die Kommunen unterliegen dann aber einer sog. Strukturschaffungspflicht. Sie müssen also Anforderungen an Auswahl der externen Dienstleister, Kontrollmöglichkeiten, Weisungsrechte und Rückholoptionen der Aufgaben vertraglich gestalten.[3]

[1] Denkhaus/Richter/Bostelmann § 5 OZG, Rn.5.
[2] Heckmann, in Bräutigam (Hrsg.), IT-Outsourcing und Cloud-Computing, 4. Aufl. 2019, S. 794 f.
[3] aaO. S. 799.

TUM Center for Digital Public Services
Lehrstuhl für Recht und Sicherheit der Digitalisierung
Technische Universität München

Direktor
Univ.-Prof. Dr. jur.
Dirk Heckmann
dirk.heckmann@tum.de

Geschäftsführerin
Assessorin jur.
Sarah Rachut
sarah.rachut@tum.de

Kontakt
Tel. +49 89 90 77 93 300
www.tum-cdps.de
www.gov.tum.de/elaw

Anwendungs-bereich	Vor-schrift(en)	Thematische Beschreibung	Handlungsbedarf	Aufgabenwahrneh-mung (wer?)	sonstiges
§ 2 ITSiV-PV: IT-Sicherheits-anforderungen für **unmittel-bar** an den Por-talverbund an-gebundene IT-Komponenten	§ 2 Abs. 1	Maßnahmen sind nach dem Stand der Technik zu treffen *(siehe zum Begriff § 8a BSIG)*	keiner – lediglich unbestimmter Rechtsbegriff, der mit den konkreten Anforderungen in § 2 aus-gefüllt wird		
	§ 2 Abs. 2	Vermutungswirkung, dass Stand der Technik eingehal-ten wird, wenn technische Richtlinien des BSI im Anhang zu § 2 Abs. 2 eingehalten wer-den	Umsetzung der BSI-TR	Outsourcing möglich	Hiervon kann nach § 4 Abs. 1 Nr. 2 ITSiV-PV bis zu zwei Jahre nach Inkrafttreten der Verordnung ab-gewichen werden. Der Grundschutz ist davon nicht erfasst.

			Umsetzung BSI-TR-03160: Servicekonten Unterteilt in BSI-TR-03160-1 Identifizierung und Authentisierung BSI-TR-03160-2: Interoperables Identitätsmanagment für Bürgerkonten & BSI-TR-03160-3 Interoperabilität von Postfächern & BSI-TR-03160-4 Interoperabilität von Organisationskonten *Befasst sich mit der Identifikation von Nutzern, der Verifikation von Nutzerdaten und der Authentisierung der nachfolgenden Nutzungen sowie der Interoperabilität zwischen den einzelnen Servicekonten im Portalverbund.*	Outsourcing möglich	
			Umsetzung BSI-TR-03107-1: Elektronische Identitäten und Vertrauensdienste im EGovernment Teil 1 *Bewertung verschiedener Verfahren zu elektronischen Identitäten und Vertrauensdienste im Bereich des E-Government hinsichtlich ihres Vertrauensniveaus.*	Outsourcing möglich	

			Umsetzung BSI-TR-03147: Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen *Analyse der Bedrohungen und Anforderungen für Verfahren zum Identitätsnachweis und zur Identitätsprüfung und Bewertung ihres Vertrauensniveaus.*	Outsourcing möglich	
			Umsetzung BSI-TR03116-4: Kryptographische Vorgaben für Projekte der Bundesregierung Teil 4 *Vorgaben zur Verschlüsselung elektronischer Kommunikation und der damit zusammenhängenden Verwendung kryptografischer Verfahren.*	Outsourcing möglich	
	§ 2 Abs. 4	IT-Komponenten müssen einem Informationssicherheitsmanagement unterliegen nach gültiger Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung des IT-Planungsrates		Outsourcing möglich	

	§ 2 Abs. 5	IT-Komponenten müssen die IT-Sicherheitskonzepte nach Standard BSI 200-1, BSI 200-2 und BSI 200-3 erfüllen, oder ISO/IEC 27001 Mindestanforderung ist BSI 200-2 (mit Niveau der **Standard-Absicherung**)	**Siehe die Ausführungen zu § 3 ITSiV-PV** (dort jedoch nur Basis-Schutzniveau, hier höheres Standard-Schutzniveau)	Die verantwortliche Stelle kann nach eigenem Ermessen externe Dienstleister mit der Erstellung des IT-Sicherheitskonzeptes beauftragen *(BAnz AT 04.05.2022 B2, S. 5)*	
	§ 2 Abs. 6	IT-Komponenten die unmittelbar mit dem Internet verbunden sind oder einen hohen oder sehr hohen Schutzbedarf nach BSI-Grundschutz haben sind vor der Anbindung an den Portalverbund einem Webcheck und einem Penetrationstest nach Vorgaben des BSI zu unterziehen.	Die Kommune bestimmt nach BSI-Grundschutz die IT-Komponenten, die dem besonderen Schutz unterliegen und für die daher Penetrationstest und Webchecks durchgeführt werden müssen. (Nutzerkonto, elektronischer Bezahldienst, Postfach und Datensafe gehören auf jeden Fall zu den Komponenten, die den Tests unterzogen werden müssen)	**siehe zum Outsourcing bei § 2 Abs. 8 und 9 ITSiV-PV**	
	§ 2 Abs. 7		Wiederholung der Penetrationstests und Webchecks alle 3 Jahre, oder bei größeren Änderungen der IT-Komponenten in § 2 Abs. 6		

	§ 2 Abs. 8 S. 1	Zuständigkeit der Penetrationstests und Webchecks für IT-Systeme der **Bundesverwaltung**		BSI selbst, oder vom BSI zertifizierter IT-Sicherheitsdienstleister	
	§ 2 Abs. 8 S. 2	Zuständigkeit der Penetrationstests und Webchecks für IT-Systeme der **Länder** *(nach Auslegung des OZG und Art. 91c Abs. 5 GG Kommunen wohl miterfasst)*	Treffen einer entsprechenden Auswahl	Fachbehörden für Informationssicherheit der Länder oder vom BSI zertifizierte IT-Sicherheitsdienstleister	
	§ 2 Abs. 9	Durchführung der Webchecks und Penetrationstests von **nicht** durch das BSI zertifizierte IT-Sicherheitsdienstleister	Treffen einer entsprechenden Auswahl	Zulässig nur, wenn zertifizierte IT-Sicherheitsdienstleister nicht zur Verfügung stehen und die Maßnahmen nach Vorgaben des BSI durchgeführt werden (müssen hierzu Fachkunde als „Penetrationstester“ nachweisen können)	

	§ 2 Abs. 10	Bericht über die Ergebnisse der Penetrationstests und Webchecks durch die Prüfer	Gefundene Mängel sind zu beseitigen und die Beseitigung ist zu dokumentieren	Outsourcing möglich	
	§ 2 Abs. 11	Die genutzten IT-Komponenten müssen einem IT-Notfallmanagement unterliegen (Anforderungen nach der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung des IT-Planungsrates)	Implementierung Notfallmanagement	Outsourcing möglich	
	§ 2 Abs. 12	Verantwortlichkeit für die Umsetzung der Anforderungen nach § 2 Abs. 1 bis 11 Verantwortliche Stelle = die für den Betrieb verantwortliche Institution	Jährliche Abgabe einer **Eigenerklärung**, dass die Maßnahmen umgesetzt/überwacht werden	Der für die IT-Komponente verantwortliche Stelle obliegt die Erfüllung der Anforderungen (also jeweilige Kommune) Wenn IT-Komponenten von Dienstleistern betrieben werden, **bleibt die auslagernde Stelle für die Erfüllung der**	

				Anforderungen verantwortlich (muss sie also nicht selbst ausführen, sondern nur überwachen) Eigenerklärung muss also selbst abgegeben werden! BAnz AT 04.05.2022 B“ S. 6: die Einbindung von Dienstleistern entbindet nicht von der Pflicht zur Einhaltung der Verordnung. Die Einhaltung der Vorgaben der ITSiV-PV durch beauftragte Dienstleister ist daher	

				vertraglich sicherzustellen	
§ 3 ITSiV-PV: IT-Sicherheitsanforderungen für **mittelbar** angebundene IT-Komponenten	§ 3 S. 1	IT-Sicherheitskonzept nach BSI Standard 200-1 *definiert allgemeine Anforderungen an ein Managementsystem für Informationssicherheit (ISMS)*	Definiert allgemeine Anforderungen für die Erstellung eines Managementsystems für Informationssicherheit (ISMS) Hier müssen zunächst **organisatorische Maßnahmen** (etwa die Benennung eines IT-Sicherheitsbeauftragten) getroffen werden, um im Folgenden den Schutzbedarf zu identifizieren und geeignete Maßnahmen zu treffen. Grundsätzlich definiert der BSI-Standard 200-1 dabei den Rahmen für ein ISMS mit einem großen Gestaltungsspielraum. Dieser kann durch die Methodik des BSI-Standards 200-2 gestaltet werden.	Erst-Recht Schluss zu § 2 Abs. 5: auch hier kann ein externer Dienstleister mit der Erstellung eines IT-Sicherheitskonzeptes beauftragt werden	Im Gegensatz zu § 2 Abs. 5 wird hier nicht auf den Standard ISO/IEC 27001 verwiesen, zwingend ist der BSI-Standard jedoch nicht, da § 3 S. 1 auch auf einen vergleichbaren, vom Land anerkannten Standard verweist

	§ 3 S. 1, **S. 2**	IT-Sicherheitskonzept nach BSI Standard 200-2	IT-Grundschutz-Methodik, beschreibt das grundlegende Vorgehen zum effektiven Management von IT-Sicherheit. Demnach muss zunächst ein Sicherheitsprozess initialisiert und entsprechend organisiert und dokumentiert werden. Innerhalb des Prozesses wird dann je nach angestrebtem Schutzniveau ein Sicherheitskonzept erstellt, umgesetzt und im Folgendem aufrechterhalten. Konkrete technisch-organisatorische Maßnahmen sind dabei im sog. IT-Grundschutzkompendium aufgeführt (siehe dazu unten).	Erst-Recht Schluss zu § 2 Abs. 5: auch hier kann ein externer Dienstleister mit der Erstellung eines IT-Sicherheitskonzeptes beauftragt werden	

			BSI-Standard 200-2 beschreibt die Methodik zur Umsetzung des IT-Grundschutzes (Kapitel 7 konkret die Umsetzung einer Basis-Absicherung) Die **konkreten Maßnahmen** finden sich dabei im **IT-Grundschutz-Kompendium** und bestehen aus zwei Bausteinschichten mit jeweils fünf Bausteinen. Jeder davon umfasst Sicherheitsanforderungen, die für den Schutz des zu betrachtenden Aspekts relevant sind und die zum Schutz umzusetzen sind. Kommunen können sich bei der Umsetzung am IT-Grundschutz-Profil **Basis-Absicherung-Kommunalverwaltung** orientieren (laut Begründung Bundesanzeiger, S. 6). Entspricht größtenteils Basis-Anforderungen, ergänzt durch Standard-Anforderungen aufgrund Verpflichtungen aus der DS-GVO, aber umfasst nicht alle Basis-Anforderungen gem. BSI (siehe hierzu Punkt 6.4 des Profils).		Das IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung **umfasst nicht alle Basis-Anforderungen nach den BSI-Standard 200-2** (siehe unter 6.4., S. 5) Unklar daher, ob das Grundschutz-Profil ausreichend ist, oder ob sämtliche Basis-Anforderungen umgesetzt werden müssen. Die Begründung bleibt hier hinter den Anforderungen des **VO-Textes** zurück, der bei der Auslegung jedoch **Vorrang** hat.

			Beispiele für die geforderten Maßnahmen zur **Basis-Absicherung aus dem IT-Grundschutz-Profil Kommunalverwaltung**: **Prozessorientierte Bausteinschicht** • **ISMS (Managementsysteme für Informationssicherheit)** Erstellen einer Leitlinie zur Informationssicherheit (ISMS.1.A2); Benennung eines Informationssicherheitsbeauftragten (ISMS.1.A4) Festlegung von Sicherheitsmaßnahmen (ISMS.1.A7) • **ORP (Organisation und Planung)** Zuweisung von Zuständigkeiten (ORP.1.A2) Geregelte Einarbeitung neuer Mitarbeiter (ORP.2.A1) Einrichtung, Änderung und Entzug von Berechtigungen (ORP.4.A2) • **CON (Konzepte)** Erstellung von Datensicherungsplänen (CON.3.A4)	Outsourcing möglich (s.o.)	

			Regelmäßige Datensicherung (CON.3.A5) Ordnungsgemäßes Löschen von schützenswerten Informationen (CON.6.A2) • **OPS (Betrieb)** Vertretungsregelung und Notfallvorsorge (OPS.1.1.2.A2) Regelmäßige Aktualisierung von IT-Systemen und Software (OPS.1.1.3.A15) Auswahl eines Virenschutzprogramms (OPS.1.1.4.A3) • **DER (Detektion und Reaktion)** Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen (DER.2.A2) Behebung von Sicherheitsvorfällen (DER.2.A5)		

			Systemorientierte Bausteinschicht • **SYS (IT-Systeme)** Einsatz von Virenschutz-Programmen auf Servern (SYS 1.1.A9) Sichere Benutzerauthentisierung (SYS.2.1.A.1) Datenträgerverschlüsselung (SYS.4.5.A10) • **NET (Netze und Kommunikation)** Grundlegende Absicherung des Internetzugangs (NET.1.1.A8) Auswahl geeigneter Kryptoverfahren für WLAN (NET.2.1.A3) • **INF (Infrastruktur)** Zugangsregelung und -kontrolle (INF.1.A7) Regelung für mobile Arbeitsplätze (INF.9.A2) • **APP (Anwendungen)** Sicheres Öffnen von Dokumenten aus externen Quellen (APP.1.1.A3) Verwendung von vertrauenswürdigen Zertifikaten (APP.1.2.A3) Sichere Beschaffung von Software (APP.6.A3)		

			• **IND (Industrielle IT)** Nicht im IT-Grundschutz-Profil aufgeführt, da typischerweise nicht Teil der Kommunalverwaltung		
			Folgende Bausteine sind im IT-Grundschutz-Profil nicht ausgeführt, jedoch für eine Basis-Absicherung erforderlich (siehe dazu Punkt 6.4 des Profils): • ORP.5 Compliance Management (Anforderungsmanagement) • CON.1 Kryptokonzept (Auswahl, Einsatz und Pflege von Verschlüsselungssoftware) • CON.2 Datenschutz (geht hier nicht nur um personenbezogene Daten) • OPS.1.1.6 Software-Tests und -Freigaben • DER.1 Detektion von sicherheitsrelevanten Ereignissen • DER.2.2 Vorsorge für die IT-Forensik (rechtliche und technische Vorbereitungen zur Beweissicherung bei Vorfällen) • DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle		

			• DER.3.1 Audits und Revisionen (regelmäßige Überprüfung der Einhaltung von Vorschriften und Vorgaben) • DER.4 Notfallmanagement (geht über die Anforderungen des Grundschutzprofils hinaus, steht aber im Kompendium als Umsetzungsmaßnahme) • APP.1.4 Mobile Anwendung (Apps) (Kontrolle des Einsatzes von Apps) • APP.2.1 Allgemeiner Verzeichnisdienst (Verwaltung von Ressourcen und Benutzern) • Ggf. spezifische Server-Bausteine • Ggf. spezifische Client-Bausteine		
	§ 3 S. 1	IT-Sicherheitskonzept nach BSI Standard 200-3	BSI-Standard 200-3 beschreibt die Risikoanalyse auf Basis des IT-Grundschutzes. Diese umfasst die **Gefahrenerkennung**, die Einschätzung der damit verbundenen Risiken und eine entsprechende Behandlung der Risken durch Anpassung des IT-Sicherheitskonzepts. Eine solche Risikoanalyse ermöglicht eine an die konkrete Situation angepasstes Schutzniveau.	Erst-Recht Schluss zu § 2 Abs. 5: auch hier kann ein externer Dienstleister mit der Erstellung eines IT-Sicherheitskonzeptes beauftragt werden	