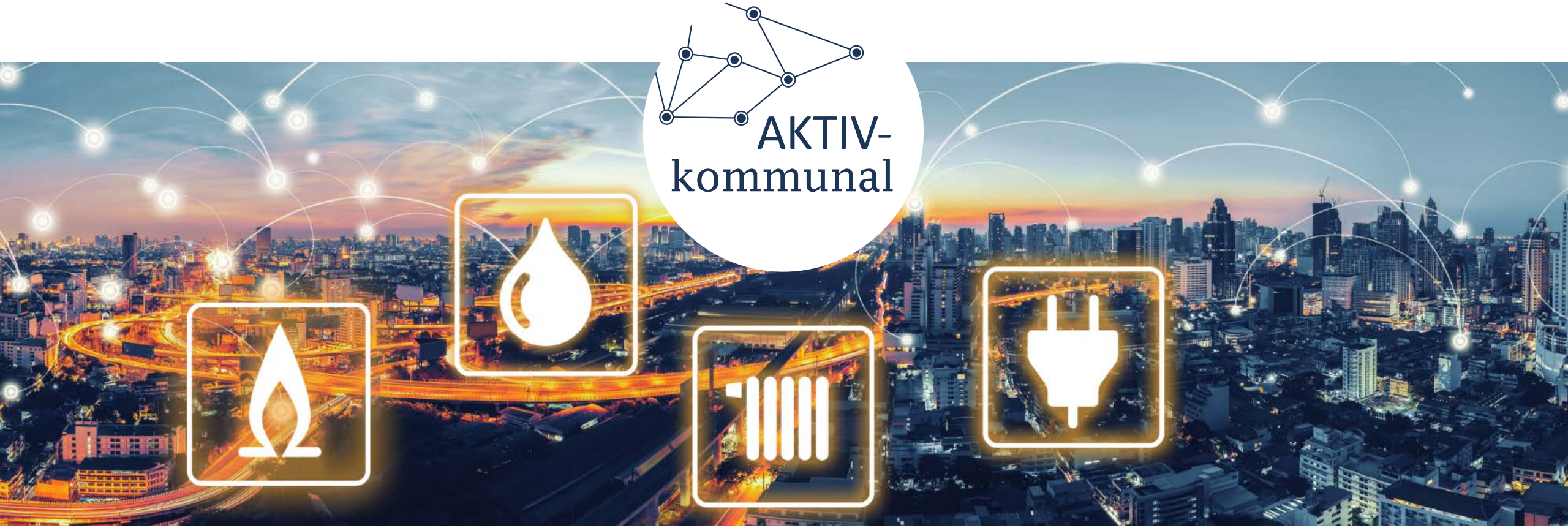
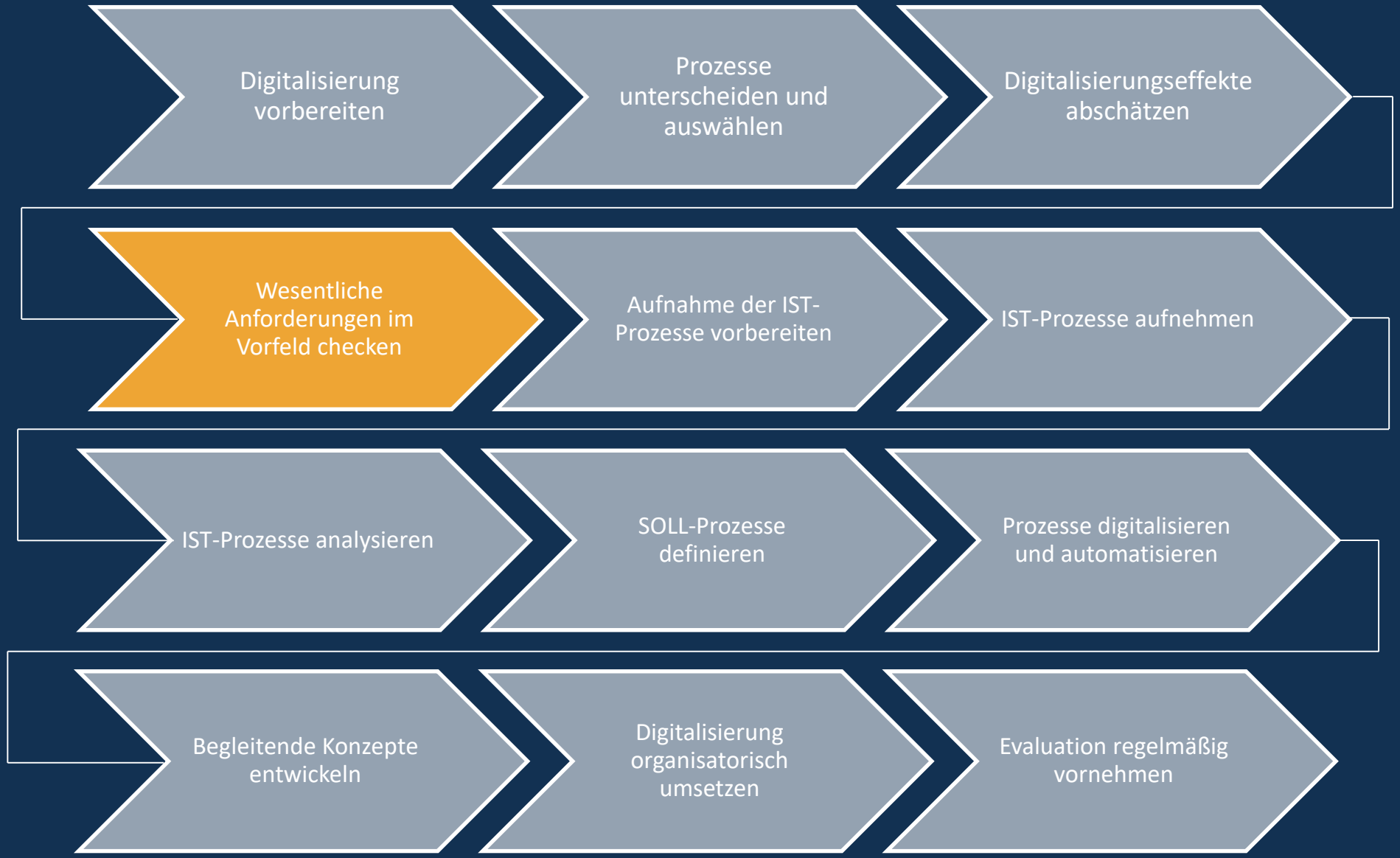
4 Wesentliche Anforderungen im Vorfeld checken
4. 3 Regulative Anforderungen berücksichtigen



Toolbox zur Digitalisierung interner Arbeits- und Leistungsprozesse



AKTIV-kommunal

4. 3 Regulative Anforderungen berücksichtigen

Leitfragen

Warum ist der Teilschritt wichtig?

Digitalisierte Prozesse unterliegen immer der potenziellen Gefahr eines Cyber-Angriffes. Der Gesetzgeber hat darauf in den vergangenen Jahren mit entsprechenden Richtlinien reagiert. Für Unternehmen stellt sich nun die Frage, ob und wie die Anforderungen der Bundesnetzagentur bzw. der DIN 27001 auf das eigene Digitalisierungsvorhaben angewendet werden müssen.

Was ist im Teilschritt konkret zu tun?

Dieser Schritt dient der Vermittlung des Wissens über die gesetzlichen Rahmenbedingungen von Informationssicherheit. Kommunale Unternehmen sollen darüber hinaus angeregt werden, die gesetzlichen Forderungen auf ihre Digitalisierungsprojekte zu reflektieren.

Welche Instrumente/Methoden helfen mir bei der Umsetzung?

Neben einer kurzen *thematischen Einführung* und einer Darstellung der regulativen Anforderungen in einem *Schaubild*, wird eine *Checkliste* zur IT-Sicherheit in Unternehmen geboten.

Wo finde ich weiterführende Informationen?

Ein *Praxisleitfaden des Bitkom* zum IT-Sicherheitskatalog bietet umfassendes Wissen und Handlungsempfehlungen für Betreiber kritischer Infrastrukturen an. Für weitere Details zum IT-Sicherheits- bzw. dem Energiewirtschaftsgesetz kann ebenfalls auf die entsprechende Seite der *Bundesnetzagentur* zum Thema verwiesen werden.

Wie geht es weiter?

Im nächsten Schritt werden *IT-technische Anforderungen* an die Prozessdigitalisierung beleuchtet.

AKTIV-kommunal

4. 3 Regulative Anforderungen berücksichtigen

Eckdaten aus dem IT-Sicherheitskatalog

Um die Anforderungen des Sicherheitskatalogs der Bundesnetzagentur zu erfüllen, müssen alle Netzbetreiber ein sogenanntes Informationssicherheits-Managementsystem (ISMS) einrichten. Dieses legt fest, mit welchen Instrumenten und Methoden die gesamte Informationssicherheit innerhalb eines Unternehmens – in diesem Fall des Netzbetreibers – realisiert wird.

- ISMS muss der DIN ISO/IEC 27001, 27001 und IEC TR 27019 entsprechen
- Wesentliche Anforderung: IT-Sicherheit ist ein stetiger Prozess bei dem Strukturen stetig aktualisiert und abgesichert werden müssen
- Grundlage ist die Risikoeinschätzung auf Basis derer Schutzmaßnahmen umgesetzt werden

Quelle: Bitkom, VKU 2015: Praxisleitfaden IT-Sicherheitskatalog, S. 10f. Zuletzt aufgerufen am 22.05.19

AKTIV-kommunal

4. 3 Regulative Anforderungen berücksichtigen

Schaubild: Bereiche und gesetzliche Grundlagen zur IT-Sicherheit

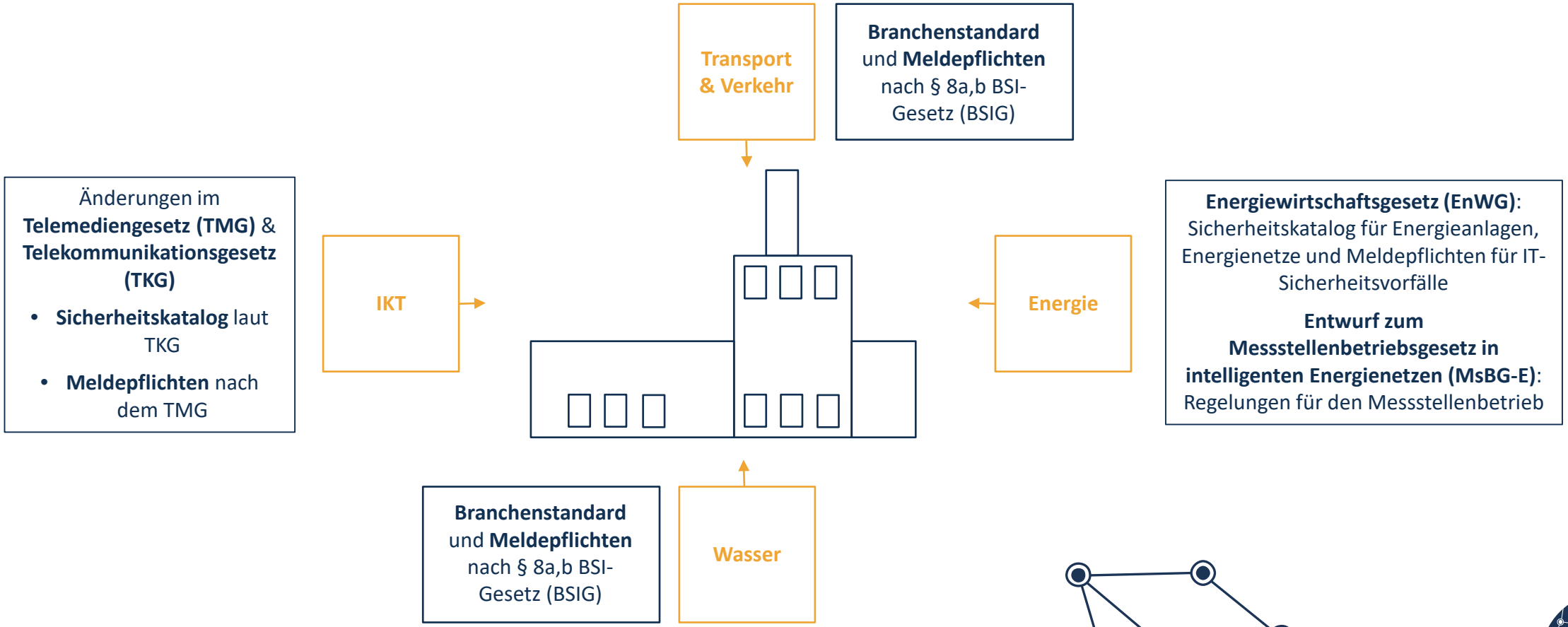


Abbildung: gesetzliche Anforderungen an (kommunale) Energieversorger

Quelle: eigene Darstellung in Anlehnung an Bundesverband der Energie- und Wasserwirtschaft (BDEW) 2016: Die digitale Energiewirtschaft, S. 72. Zuletzt aufgerufen am 22.05.19

4. 3 Regulative Anforderungen berücksichtigen

Checkliste: IT-Sicherheit für Unternehmen

Themengebiet	Handlungsempfehlung	geprüft/trifft zu
IT-Sicherheits-management	Zuständigkeiten und Verfahren auf Informationssicherheit abstimmen	
	Zulässigen Gebrauch von Informationen und Firmeneigentum festlegen	
	Verfahren für den Umgang mit klassifizierten Informationen festlegen	
Mitarbeiter	Mitarbeiter schulen und durch Aus- bzw. Weiterbildungsmaßnahmen für IT-Sicherheit sensibilisieren	
	Vertraulichkeits- und Geheimhaltungsvereinbarungen abschließen	
	Schwachstellen durch funktionierenden Berichterstattungs-mechanismus erkennen	
	IT-Sicherheitsmängel werden an bekanntgegebene Adressaten gemeldet	
Zugang und Zugriff	Zugriffsrechte durch Authentifizierung regeln	
	Kennwortschutz sicherstellen	
	unbeaufsichtigte Endgeräte durch automatische bzw. manuelle Sperrung schützen	

Tabelle 1: eigene Darstellung in Anlehnung an Kompetenzzentrum Kritische Infrastrukturen (KKI) 2015: Handlungsempfehlungen – Zur Verbesserung der IT- und Informationssicherheit für Betreiber kritischer Infrastrukturen, S. 11f. Zuletzt aufgerufen am 22.05.19

4. 3 Regulative Anforderungen berücksichtigen

Checkliste: IT-Sicherheit für Unternehmen

Themengebiet	Handlungsempfehlung	geprüft/trifft zu
IT-Betrieb	Verfahren des IT-Betriebs (Systeminstallation, -wartung und -löschung) dokumentieren	
	Beschränkung der Installation auf betrieblichen Anwendungssystemen	
	Beschränkung der Softwareinstallation auf Clients und Mobilgeräten	
	Management von Mobilgeräten (die Bewertung der Nutzung von Mobilgeräten wurde im Hinblick auf IT-Sicherheit vorgenommen)	
	Wechseldatenträgernutzung kontrollieren	
	Schutz der IT-Systeme (Malwareschutz auf Client-, Server- und Netzwerkseite)	
	Systemwiederherstellung wird durch regelmäßige Datensicherungen trainiert	
	Administratoren- und Betreiberprotokolle pflegen	
Beziehung zu externen Akteuren	gegenüber Informationssicherheit in Lieferantenbeziehungen sensibilisieren	
	Behördenkontakte festlegen und pflegen	

Tabelle 2: eigene Darstellung in Anlehnung an Kompetenzzentrum Kritische Infrastrukturen (KKI) 2015: Handlungsempfehlungen – Zur Verbesserung der IT- und Informationssicherheit für Betreiber kritischer Infrastrukturen, S. 12f.

AKTIV-kommunal

„Wir brauchen bei der IT-Sicherheit mindestens das gleiche Sicherheitsbewusstsein wie bei der Verkehrssicherheit.“

Quelle: Dr. Thomas de Maizière zitiert nach Bundesministerium des Innern, für Bau und Heimat: Mehr digitale Sorgfalt statt digitaler Sorglosigkeit notwendig, zuletzt aufgerufen am 22.05.19

AKTIV-kommunal

Förderhinweise

Dieses Forschungs- und Entwicklungsprojekt „AKTIV-kommunal - Arbeitsgestaltung für kommunale Unternehmen in digitalen Innovations- und Veränderungsprozessen“ wird im Rahmen des Programms „Zukunft der Arbeit“ (FKZ 02L15A100) vom Bundesministerium für Bildung und Forschung (BMBF) und dem Europäischen Sozialfonds (ESF) gefördert und vom Projektträger Karlsruhe (PTKA) betreut. Die AKTIV-kommunal Toolbox zur Digitalisierung interner Arbeits- und Leistungsprozesse wurde im Rahmen des Teilprojektes „Ansatz zur Digitalisierung von Arbeitsprozessen unter Bedingungen gesellschaftlich notwendiger Dienstleistungen“ (FKZ 02L15A105) erstellt. Diese Toolbox wurde von den Projektpartnern Fraunhofer IAO sowie den Stadtwerken Konstanz federführend realisiert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

ESF
Europäischer Sozialfonds
für Deutschland

EUROPÄISCHE UNION

Zusammen.
Zukunft.
Gestalten.

AKTIV-
kommunal