Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Cyber-Sicherheit in der Smart-City

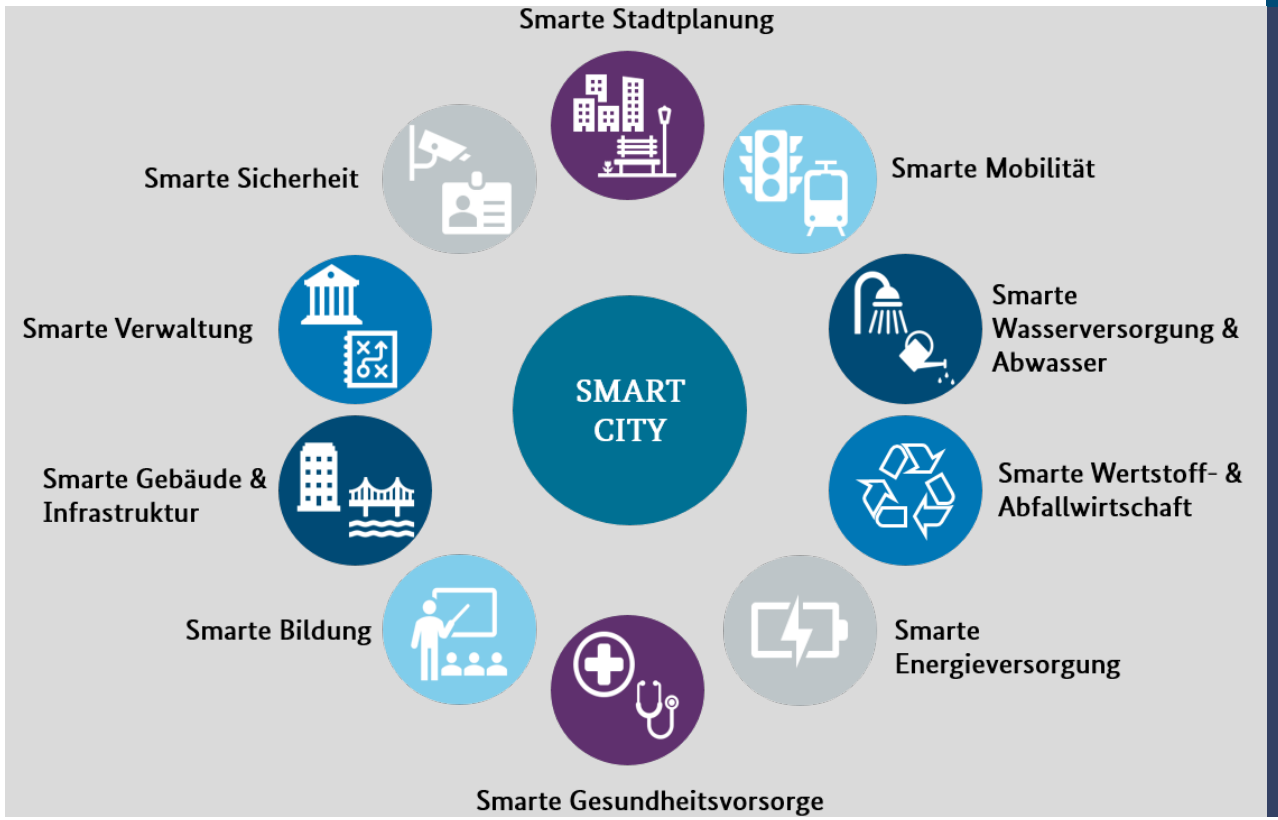
Handlungsempfehlungen zur Informationssicherheit kommunaler IoT-Infrastrukturen –
Dimitri Eichhorn, 8. Kommunaler IT-Sicherheitskongress, 04.05.2022

Herausforderungen für die Cyber-Sicherheit von Smart Cities

Deutschland
Digital•Sicher•BSI•

Digitalisierung der öffentlichen Daseinsvorsorge

- Ziel: Erhöhung der Teilhabe und Lebensqualität und Schaffung einer ökonomisch, ökologisch und sozial nachhaltigen Kommune/Stadt/Region
- Risiken: Ausfall und Missbrauch der dafür notwendigen Infrastrukturen stehen den Zielen entgegen
- Lösung: Prozesse zur Identifizierung und Mitigation von Risiken notwendig
- Herausforderungen:
  - Identifikation von Risiken erfordert ein Verständnis des Anwendungsfalls und der Infrastruktur
  - Mitigation einiger Risiken erfordert Produkte, die entsprechende Cybersicherheitsanforderungen erfüllen

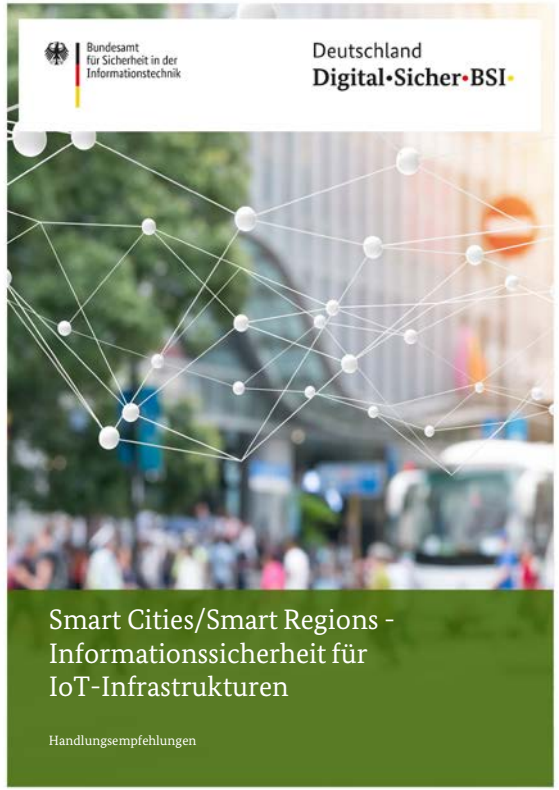


Handlungsempfehlungen: Cyber-Sicherheit in der Smart City von Anfang an mitdenken

Deutschland
Digital•Sicher•BSI•

BSI Veröffentlichung

- Adressat: Entscheider und operativ Verantwortliche für IoT-Projekte im kommunalen Umfeld
- Ziele:
  - Einstieg in strukturierte IT-Sicherheitsbetrachtung
    - Reduktion der Komplexität durch Strukturierung
    - Kann als Checkliste verwendet werden
    - Verweise auf weiterführende Konzepte
  - Darstellung wesentlicher IT-Sicherheitsaspekte
  - Motivation zur Etablierung kontinuierlicher Prozesse um Risiken zu erkennen und adäquat zu behandeln

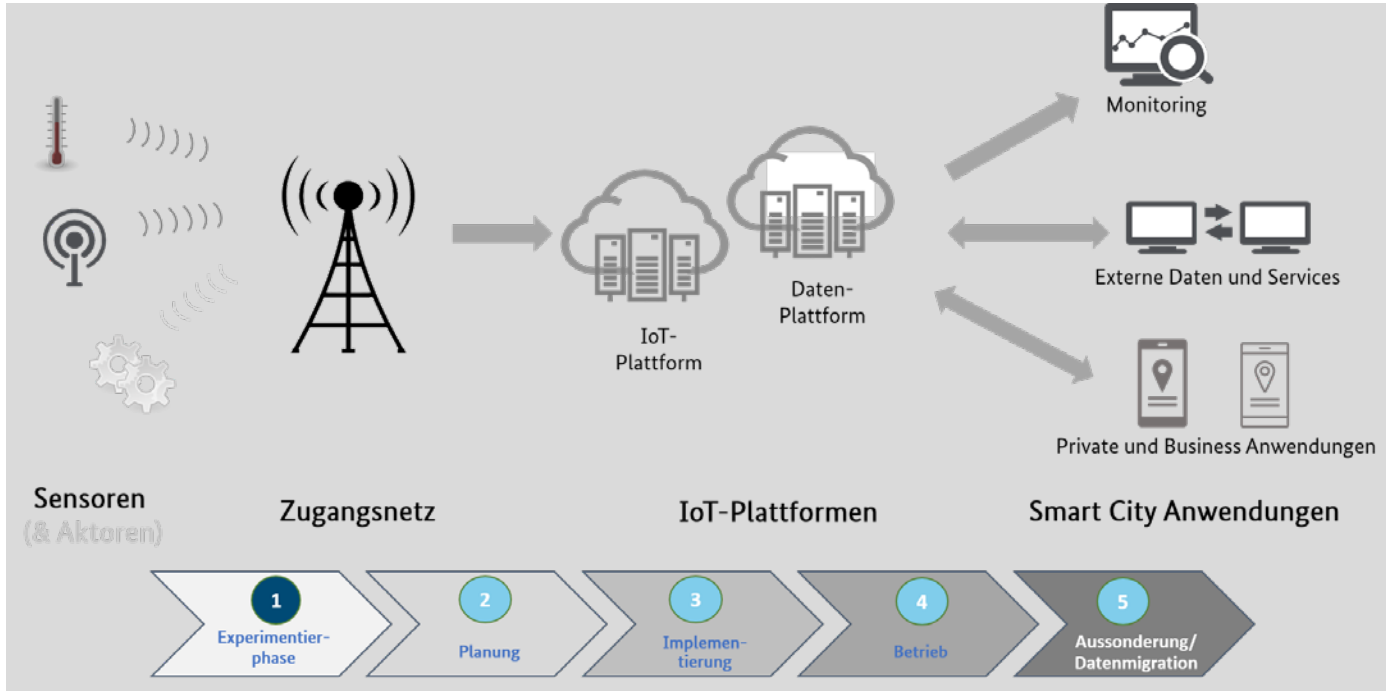


Handlungsempfehlungen: Cyber-Sicherheit in der Smart City von Anfang an mitdenken

Deutschland Digital•Sicher•BSI•

Experimentierphase – ggf. nicht erforderlich

- Grobe konzeptionelle Überlegungen bzgl. IT-Sicherheit initiieren:
  - Schutzbedarfsfeststellung
  - Dokumentation der IoT-Infrastruktur
    - Architektur
    - Komponenten
    - Schnittstellen
- Schlüssel für Erfolg:
  - Anwendungsfall und technische Infrastruktur verstehen
  - relevante Stakeholder identifizieren

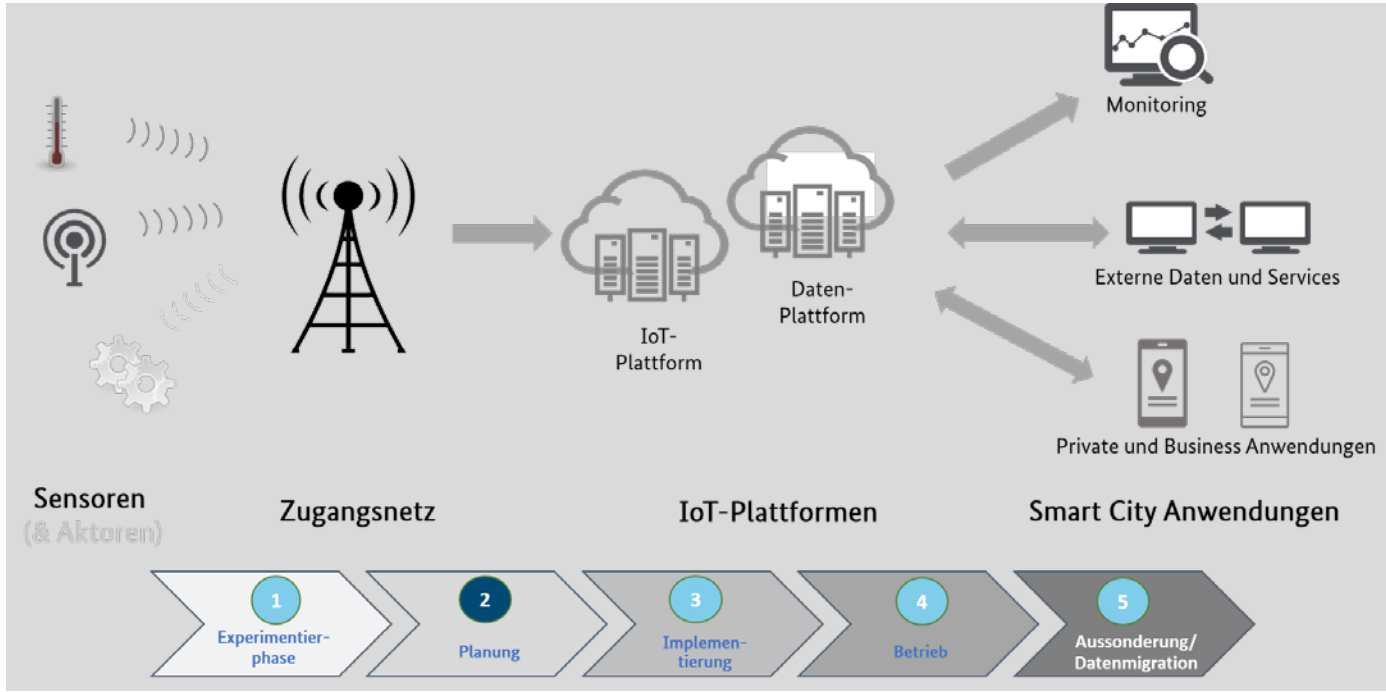


Handlungsempfehlungen: Cyber-Sicherheit in der Smart City von Anfang an mitdenken

Deutschland Digital•Sicher•BSI•

Planungsphase

- Klare Zuordnung von Verantwortung und Zuständigkeiten
- Erstellung technischer und organisatorischer Dokumentation
- Identifikation von Sicherheitsanforderungen
  - Schutzbedarfsfeststellung
  - Gefährdungs-/Risikoanalyse
- Zentrales Werkzeug: Beschaffung und Ausschreibung
  - Sicherstellung der Produktpflege
  - Verfügbarkeit der notwendigen Sicherheitsfunktionalität (ggf. Sicherheitsnachweise)
  - Vermeidung von Abhängigkeiten



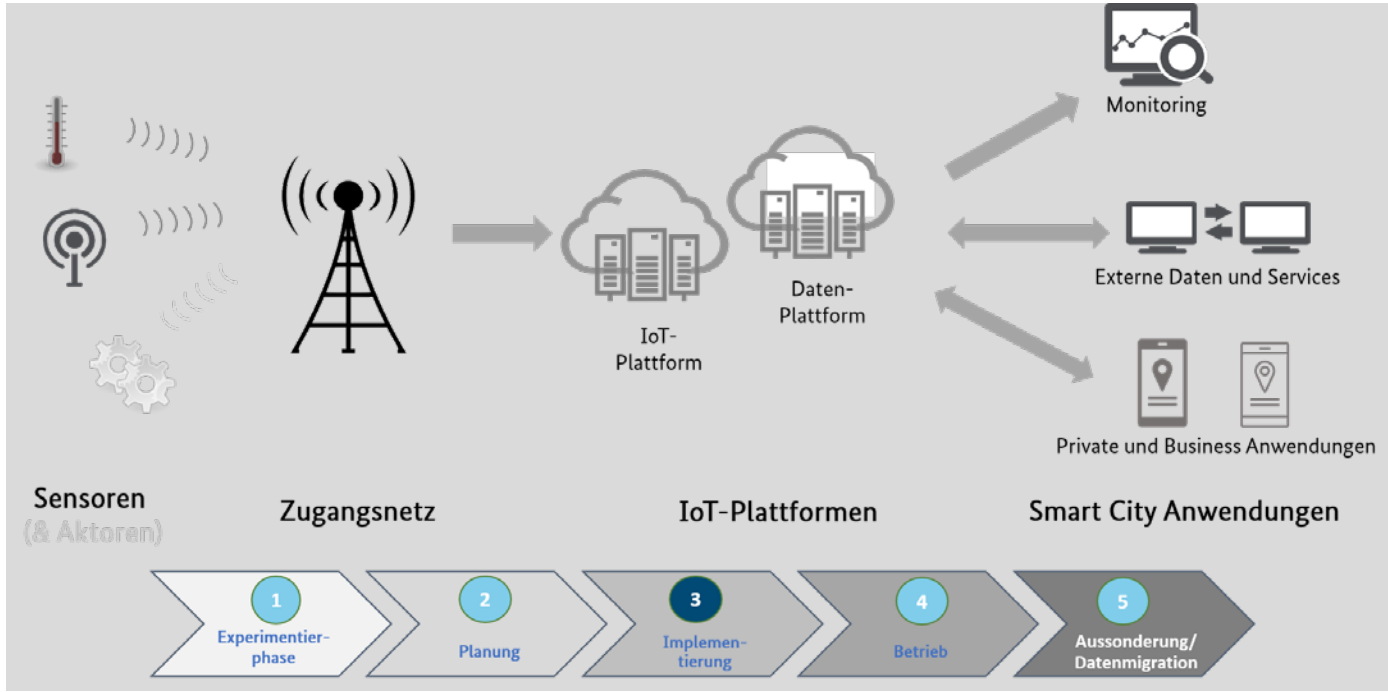
Bundesamt für Sicherheit in der Informationstechnik

Handlungsempfehlungen: Cyber-Sicherheit in der Smart City von Anfang an mitdenken

Deutschland Digital•Sicher•BSI•

Implementierungsphase

- Dokumentation der Betriebsprozesse und personellen Zuständigkeiten
- Etablierung eines technischen und organisatorischen Berechtigungsmanagements (Need-to-Know-Prinzip, Segregation of Duties)
- Sichere Konfiguration von IoT-Komponenten möglichst vor/während der Integration
- Etablierung eines Managements für kryptographische Schlüssel
- Erweiterung/Einführung des/eines Incidentmanagments auf/für die IoT-Infrastruktur

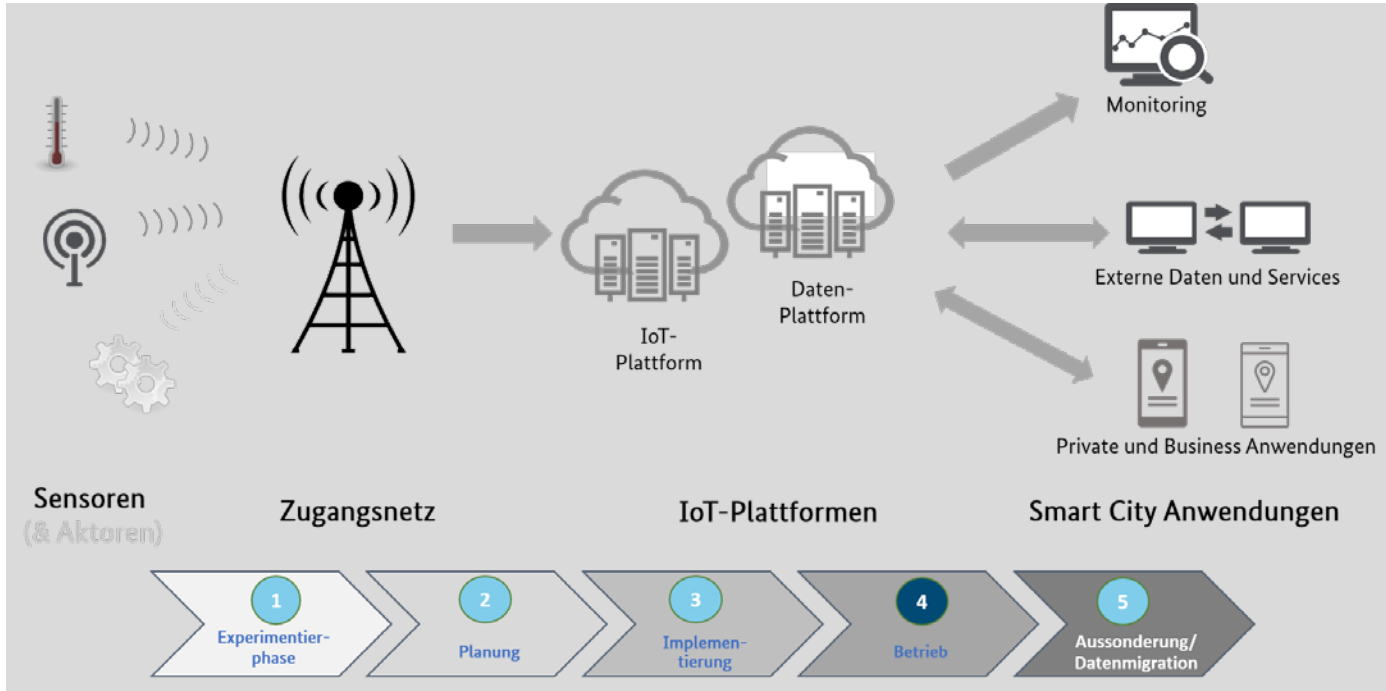


Handlungsempfehlungen: Cyber-Sicherheit in der Smart City von Anfang an mitdenken

Deutschland Digital•Sicher•BSI•

Betriebsphase

- Inbetriebnahme (ggf. Stufenweise)
- Regelmäßige Aktivitäten:
  - Aktualisierung von Schutzbedarf- und Risikoanalyse
  - Überprüfung regulatorischer Anforderungen und Aktualisierung der Berechtigungen
  - Prüfung der Einhaltung vereinbarter Anforderungen seitens Dritter
  - Audits der IoT-Infrastruktur
  - Erprobung des Incidentmanagements

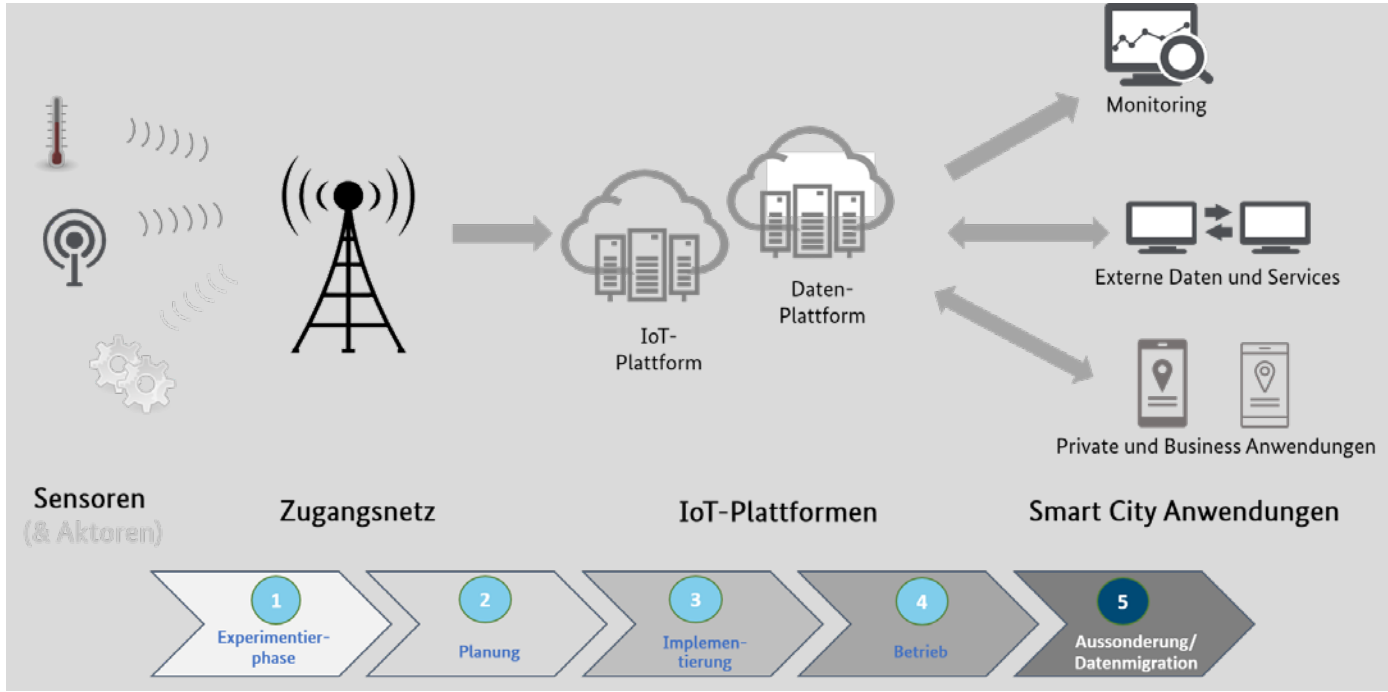


Handlungsempfehlungen: Cyber-Sicherheit in der Smart City von Anfang an mitdenken

Deutschland
Digital•Sicher•BSI•

Aussonderungsphase

- Bei Neuplanung bzw. Ablösung der IoT-Infrastruktur
  - Aufbewahrung der Dokumentation für Dienstleister und Stakeholder
  - Deaktivierung betroffener Schnittstellen und Entzug etwaiger Berechtigungen

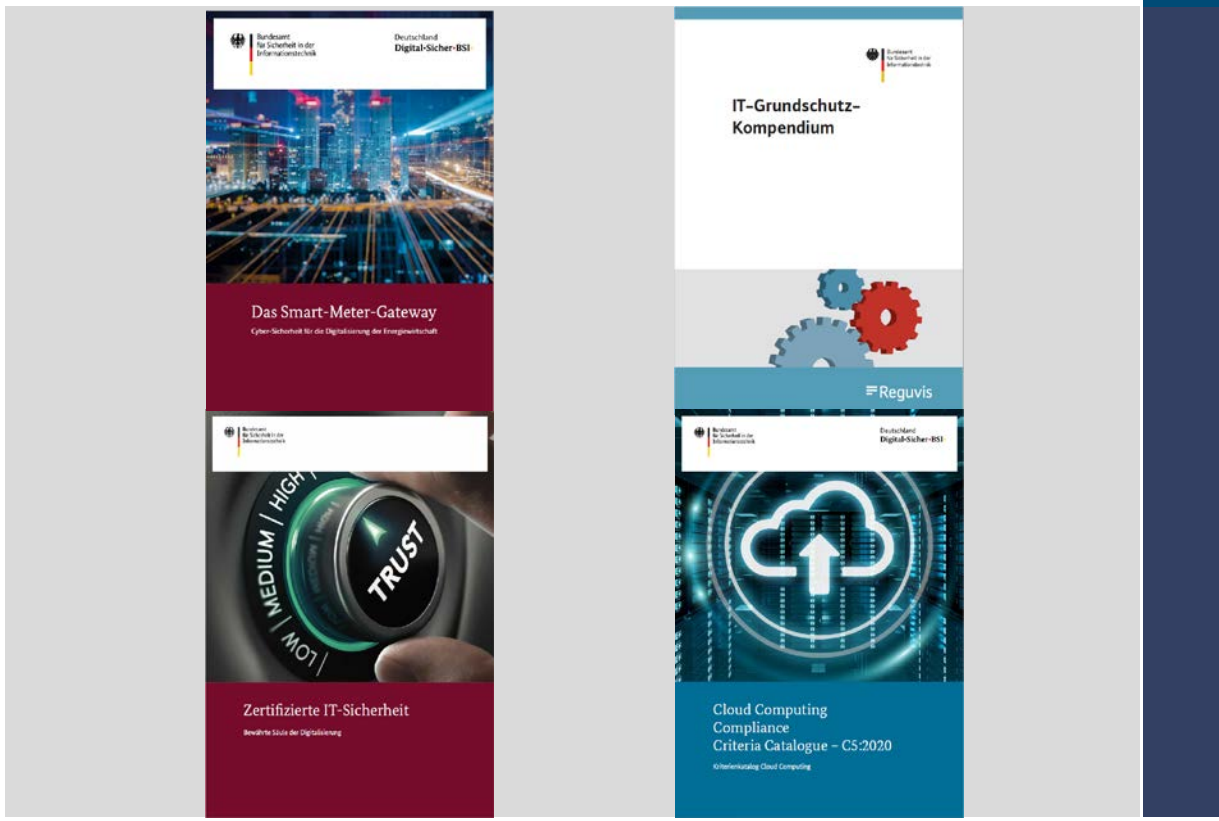


Handlungsempfehlungen: Cyber-Sicherheit in der Smart City von Anfang an mitdenken

Deutschland
Digital•Sicher•BSI•

Weitergehende Konzepte

- Informationssicherheit mit System – IT Grundschutz
  - Standardisiertes Vorgehen für
    - Etablierung eines ISMS*
    - Risikomanagement
    - Notfallmanagement
  - Nachweisbar durch Zertifizierung
- Produktzertifizierung
- Testierung der Erfüllung von Kriterien des Cloud Computing Compliance Criteria Catalogue
- Sektor-spezifische Sicherheitsstandards



*Information Security Management System - Managementsysteme für Informationssicherheit

Sichere urbane Datenplattform – Projektidee

Deutschland
Digital•Sicher•BSI•

Vorgehen/Ziele (aktuelle Planung):

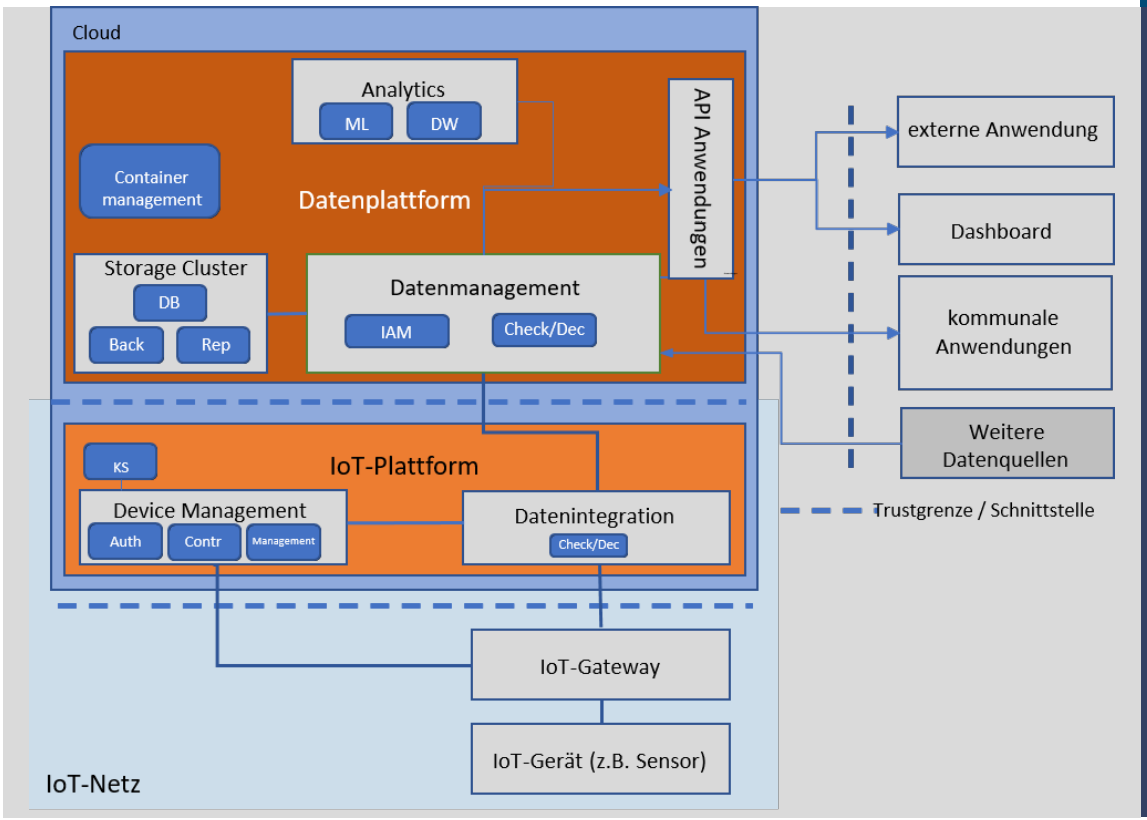
- Architekturanalyse bestehender/geplanter urbaner Datenplattformen mit ca. 5 kommunalen Projektpartner
- Modellierung einer generischen Architektur
- Bedrohungs-/ risikobasierte Ableitung geeigneter Sicherheitsanforderungen/-empfehlungen
- Piloten zur Evaluierung und Bewertung der Sicherheitsanforderungen/-empfehlungen in ca. 3 bestehenden urbanen Datenplattformen
  - konzeptionell (Analyse von Designdokumenten)
  - praktisch (Penetrationstests)
- Veröffentlichung des technischen IT-Sicherheitsstandards zu kommunalen Datenplattformen

Sichere urbane Datenplattform – Zusammenarbeit mit kommunalen Partnern

Deutschland Digital•Sicher•BSI•

Zeitplan (aktuelle Schätzung):

- Q3 2022: Bestandsaufnahme
  - hinreichend geplante und bestehende Systeme
- Q2 2023: Konzeptionelle Analyse
  - hinreichend geplante und bestehende Systeme
- Q3 2023: Penetrationstest
  - bestehende (Test-)Systeme
- Q1 2024: Veröffentlichung des technischen IT-Sicherheitsstandards zu kommunalen Datenplattformen
- bei Interesse an einer Zusammenarbeit gerne ab sofort unter smartcity@bsi.bund.de melden

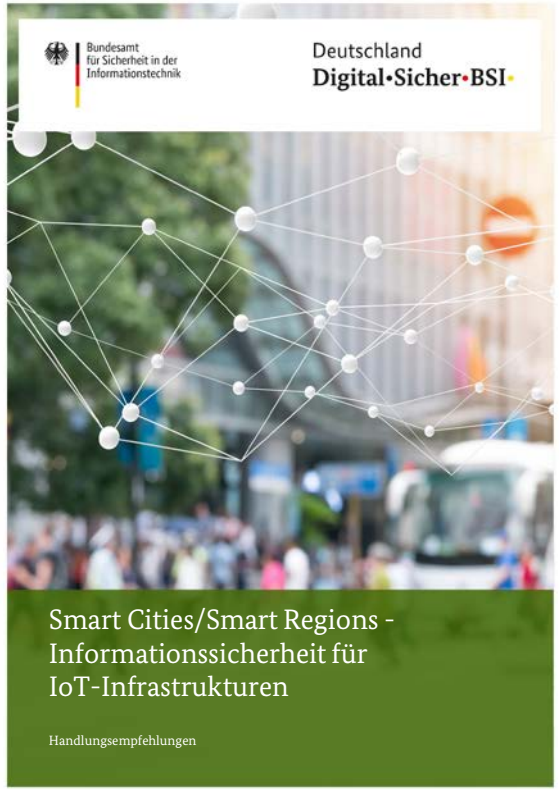


Fazit

Deutschland
Digital•Sicher•BSI•

Kernbotschaften

- Cyber-Sicherheit ist integraler Bestandteil der Digitalisierung
- Cyber-Sicherheit bedarf von Anfang an effektiver Prozesse zur Identifikation und Mitigation von Risiken („Security-by-Design“)
- BSI-Handlungsempfehlungen erleichtern den Einstieg in eine strukturierte IT-Sicherheitsbetrachtung für kommunale IoT-Infrastrukturen
- Verständnis des Anwendungsfalls und der technischen Infrastruktur ist ein Schlüssel für den Erfolg
- Beschaffungen und Ausschreibungen sind ein zentrales Werkzeug zur Gestaltung der IT-Sicherheit



Vielen Dank für Ihre Aufmerksamkeit!

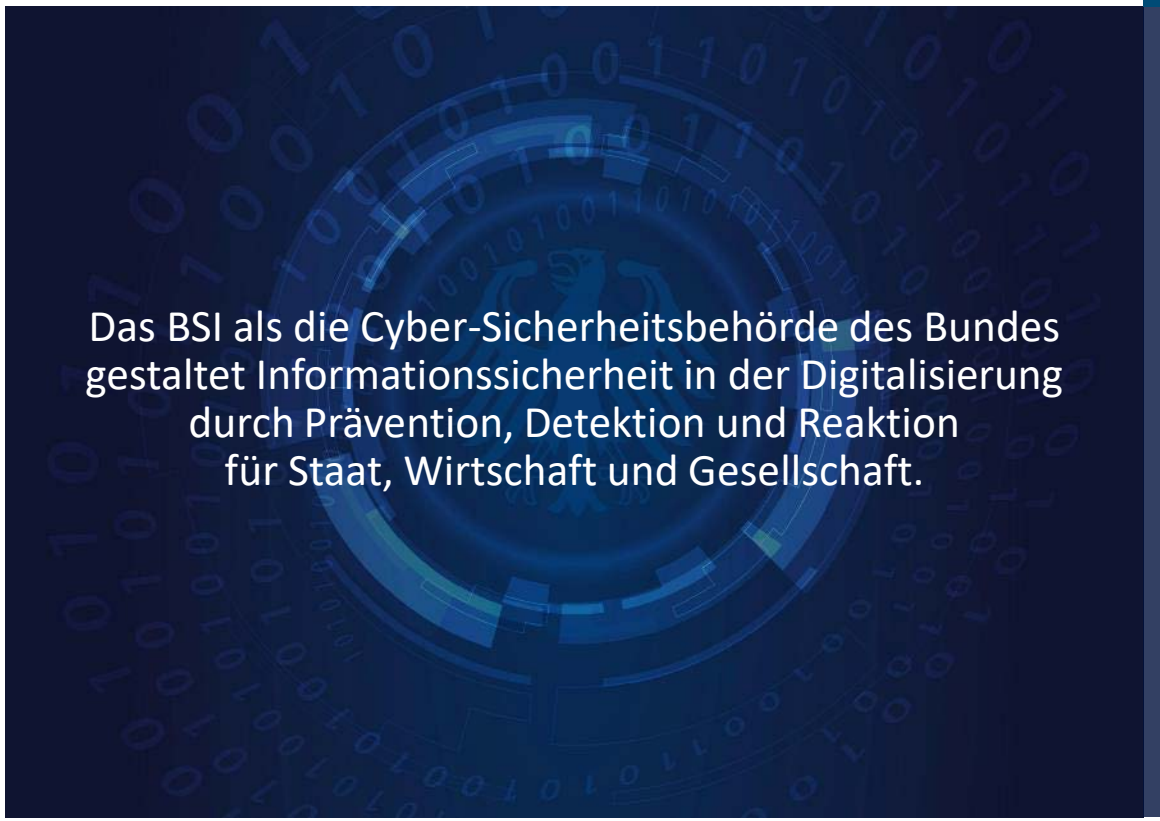
Deutschland
Digital•Sicher•BSI•

Kontakt

Dimitri Eichhorn
Referent – Cyber-Sicherheit in Smart Home und Smart Cities

smartcity@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