Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Cybersicherheitsempfehlung des BSI Sichere Nutzung von Edge Computing

Use Cases

Sebastian Temme BSI, Referat Cloud-Sicherheit

Omnisecure 2025 - Berlin, 20.01.2025

Use Cases – Edge Computing

Bild: © littlestocker / Fotolia

Bild: © vege/ Fotolia

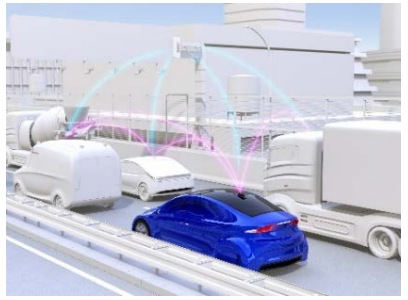


Bild: © Chesky / Getty Images

Bild: © ipopba / AdobeStock

Bild: © Waiforlight_Moment_gettyimegs

Bild: © https://de.freepik.com/vektoren-kostenlos/militaertransport-symbolsatz-luftwaffe-jet-u-boot-hubschrauber-lkw-panzer-isoliert-vektorillustrationen-fuer-armeefahrzeuge-waffe-kraftkonzept_10613233.htm auf Freepik

Bild: © leungchopan/ Fotolia

Bild: © Gandee Vasan / Getty Images

Use Cases – Edge Computing

In der Cybersicherheitsempfehlung werden 3 Use Cases betrachtet

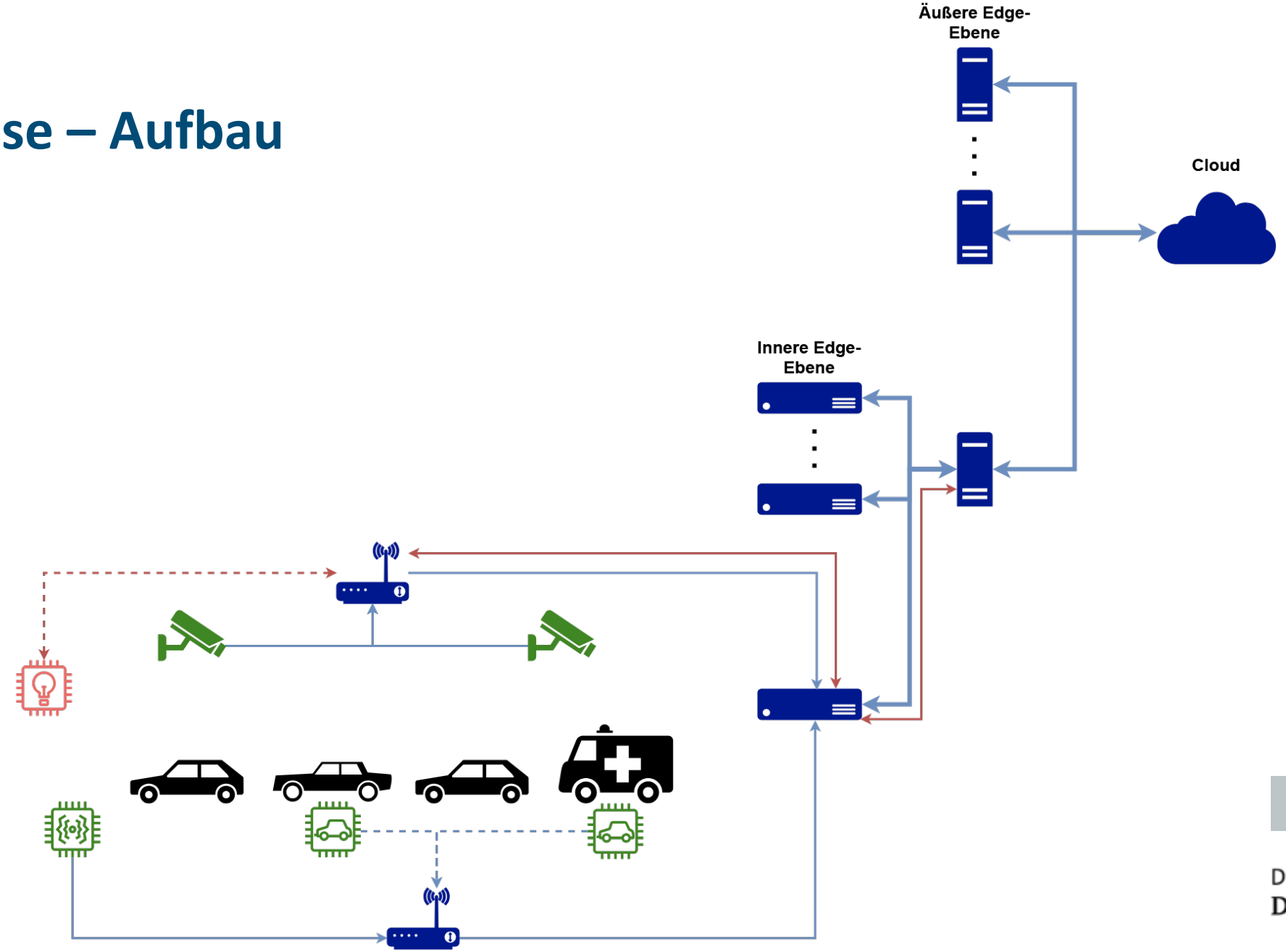
- Datenverarbeitung und Enterprise Security
- IoT für die Gesellschaft
- Industrial IoT

Ziel:

- Abdeckung der Komponentenbreite
- **Verständnis** statt Vollständigkeit, da Möglichkeiten zu Vielfältig
- Wegweiser / Checkliste wie in der Praxis Sicherheitskriterien abgebildet werden können

Use Case: IoT für Gesellschaft (Verkehrssteuerung/Smart City)

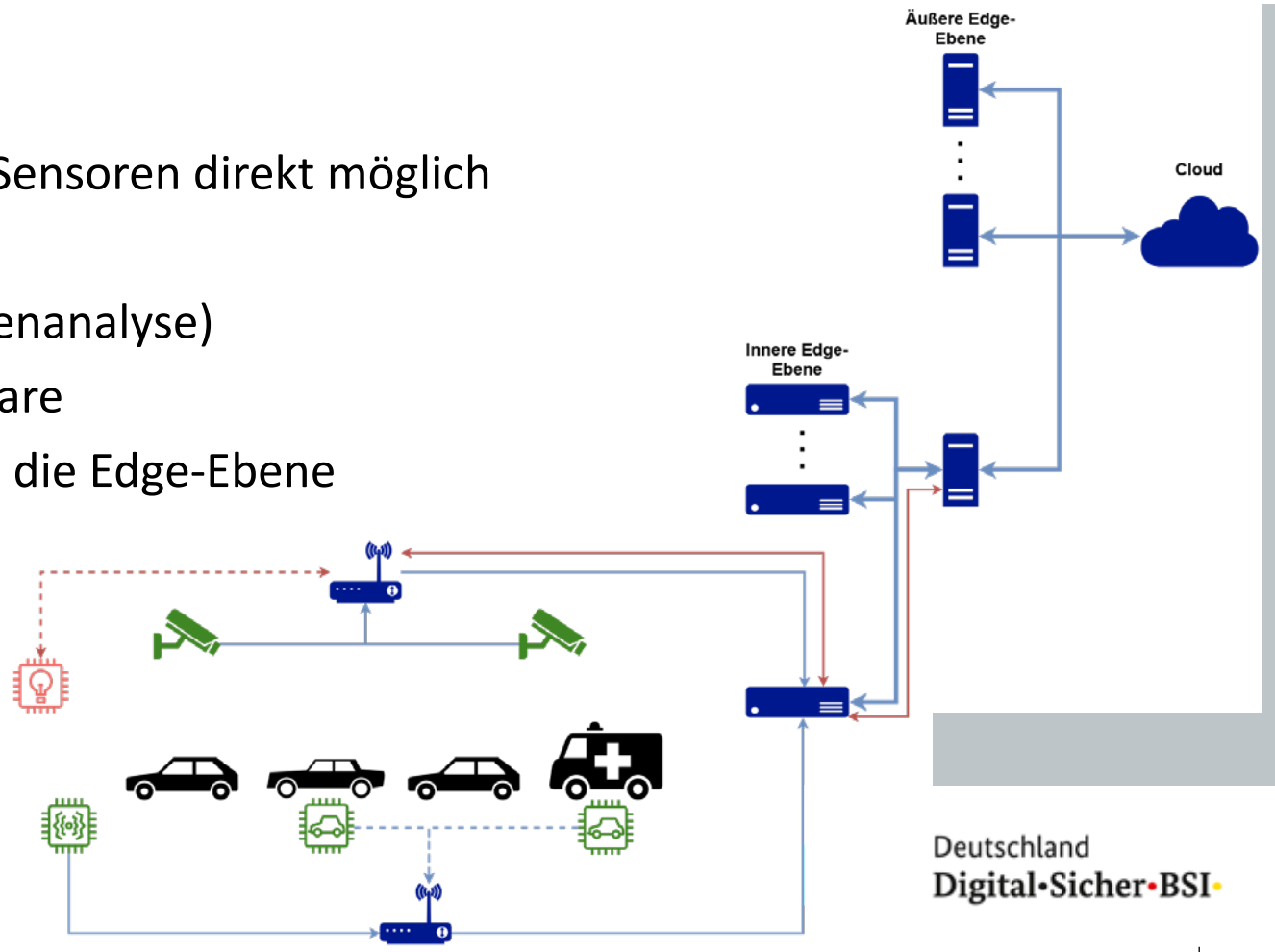
Use Case – Aufbau



Use Case – Gefährdungslage

Endgeräte Ebene

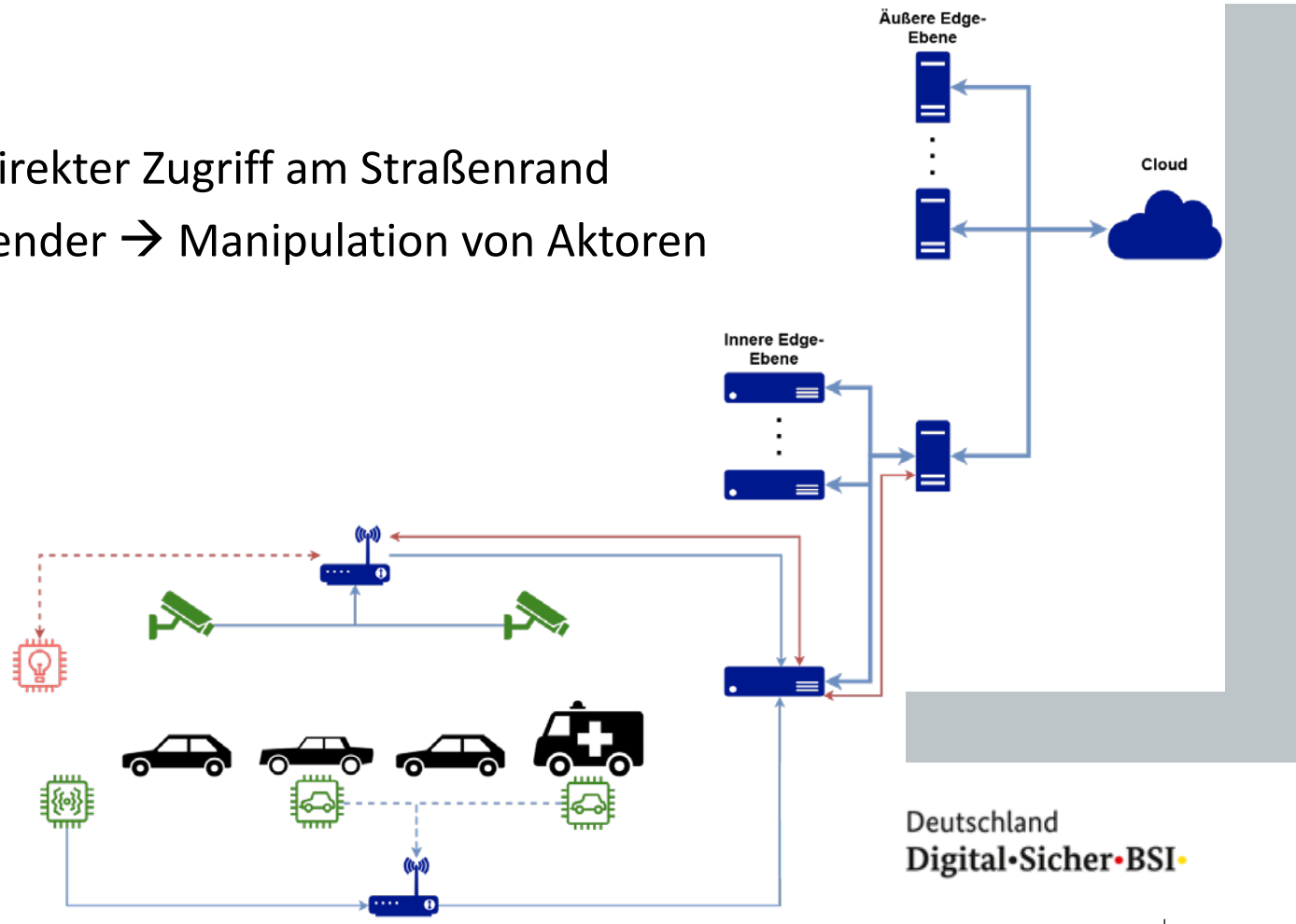
- Hohe Exponiertheit
  - Physische Angriffe auf Endgeräte sowie Sensoren direkt möglich
- Manipulation, Zerstörung
- Diebstahl / Erwerb („offline“ Schwachstellenanalyse)
- ggf. exotische Netzwerkprotokolle / Firmware
- Möglicher Ausgangspunkt von Angriffen in die Edge-Ebene



Use Case – Gefährdungslage

Innere Edge-Ebene

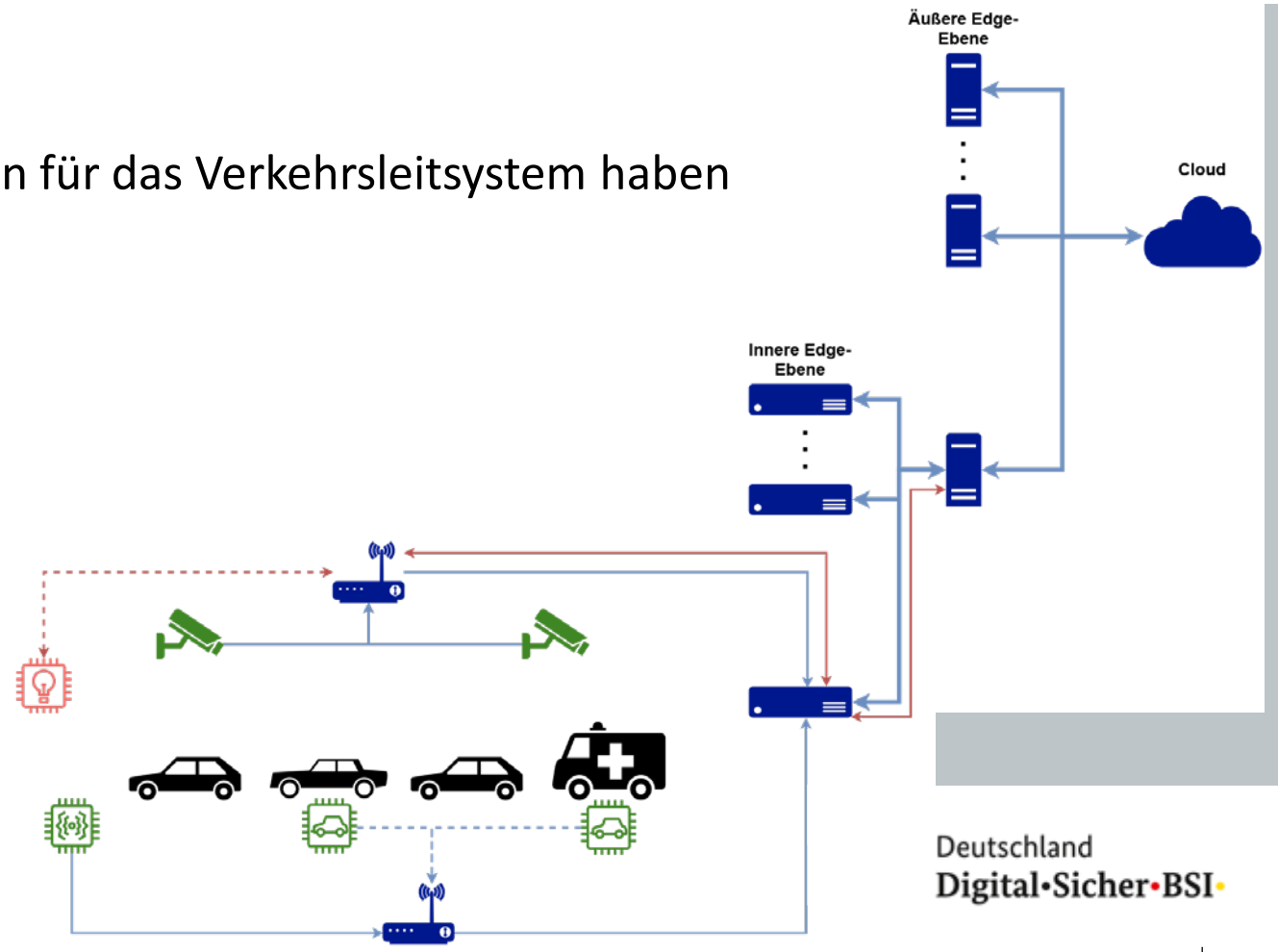
- Weniger exponiert als Endgeräte
- Kompromittierung über Endgeräte, oder direkter Zugriff am Straßenrand
- Folgen der Manipulation sind schwerwiegender → Manipulation von Aktoren



Use Case – Gefährdungslage

Äußere Edge-Ebene

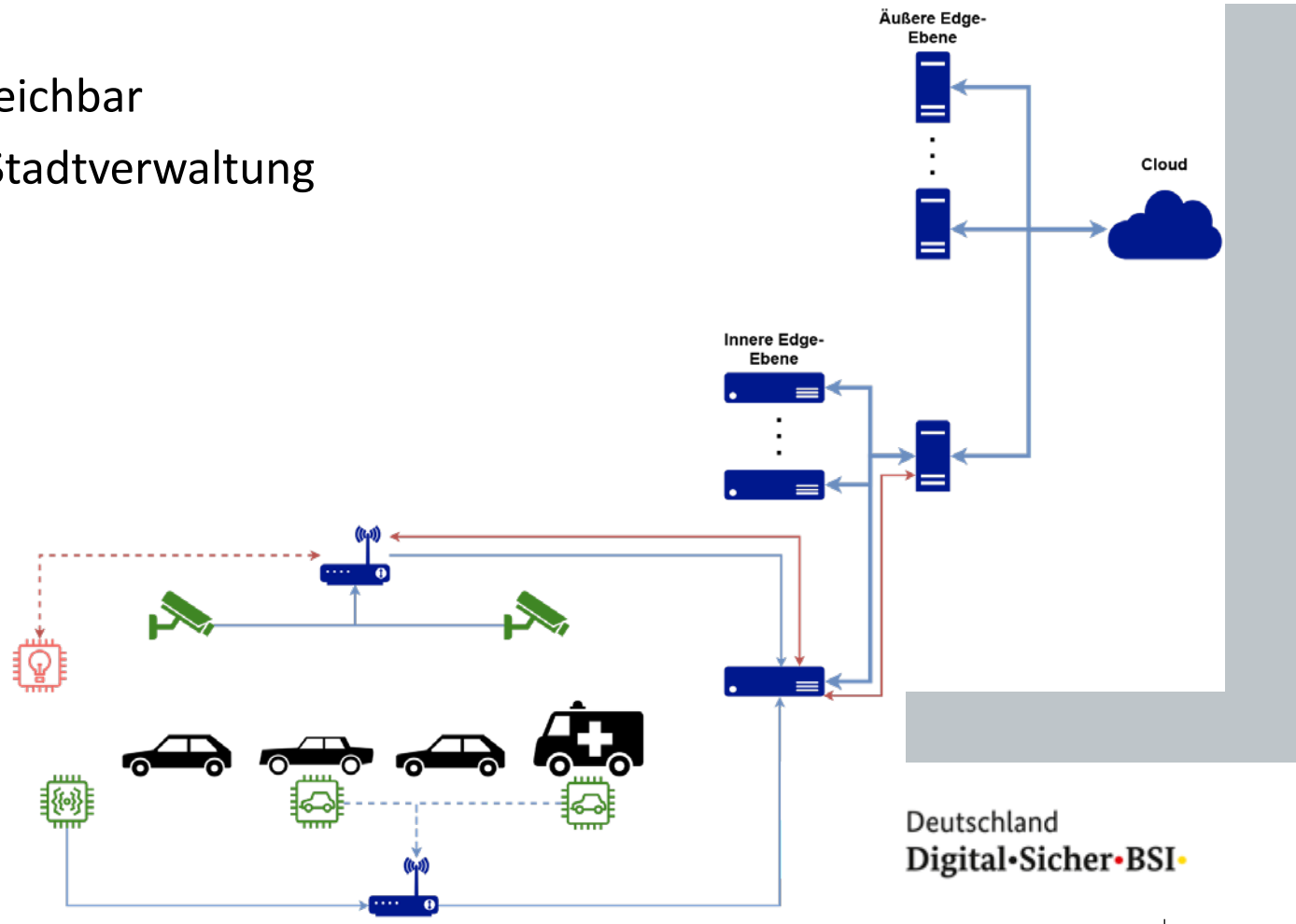
- Schwer erreichbar, z.T. im RZ
- Manipulation kann schwerwiegende Folgen für das Verkehrsleitsystem haben



Use Case – Gefährdungslage

Cloud-Ebene

- Im Rechenzentrum des CSP i.d.R. nicht erreichbar
- ggf. Phishing Angriffe auf Mitarbeiter der Stadtverwaltung
- Fehlkonfiguration von Cloud-Diensten
  - Shared Responsibility der Cloud-Nutzer



Use Case – Angriffsszenario

- Reconnaissance: Schwachstellen in Sensoren und Aktoren
  - ggf. auch „offline“ möglich durch Akquise/Diebstahl
- Angriff über Schwachstellen
- Ausbreitung von Malware
  - Payload, Reverse Shells, …
- Bewegung im System über Lateral-Movement/Privilege-Escalation
  - Über Edge- und Cloud-Ebene
- Verschlüsselung der Daten / Störung des Systems
  - Erpressung durch Lahmlegung der Verkehrssteuerung

Use Case – Handlungsempfehlungen

- Angemessene Produktauswahl
- Rollen-Rechte Konzepte
  - Least Privilege-Prinzip, Separation of Duties
- Patch- und Konfigurations-Management
  - Versionskontrolle, Automatisierung
- Logging und Log-Auswertung
  - Detektion von Abweichungen / auffälligem Verhalten
- Systemhärtung, Firewalling
- Mitarbeiter-Schulung / -Überprüfung
- Sicherung physisch exponierter Komponenten
  - Verplomben, Versiegeln, Kontrollieren, …
- …

Prävention, Detektion, Reaktion

Use Case – Fazit / Netto-Risiken

- Für einzelne Komponenten gelten **ähnliche Gefährdungen** wie außerhalb des Edge Computings
  - ➢ Dies gilt auch für Handlungsempfehlungen
- Unterschied: Besonders **weite Vernetzung** der einzelnen Komponenten
  - ➢ Viele Einstiegspunkte für Angreifer
  - ➢ Großer Spielraum für Bewegungen im System (Lateral Movement)
- Wichtig: **Backup**-Maßnahmen und **Redundanzen** bei Edge-Komponenten
  - – Verringerung der Anlaufzeit / Ausfälle / Erpressbarkeit / …
- Beim Wechsel auf Edge-Komponenten Rückbau / Abschaffung herkömmlicher Systeme betrachten
  - – Herkömmliche Systeme können als Fallback dienen

Bundesamt
für Sicherheit in der
Informationstechnik

Sebastian Temme BSI, Referent Cloud-Sicherheit

cloudsecurity@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn

www.bsi.bund.de

Follow us: