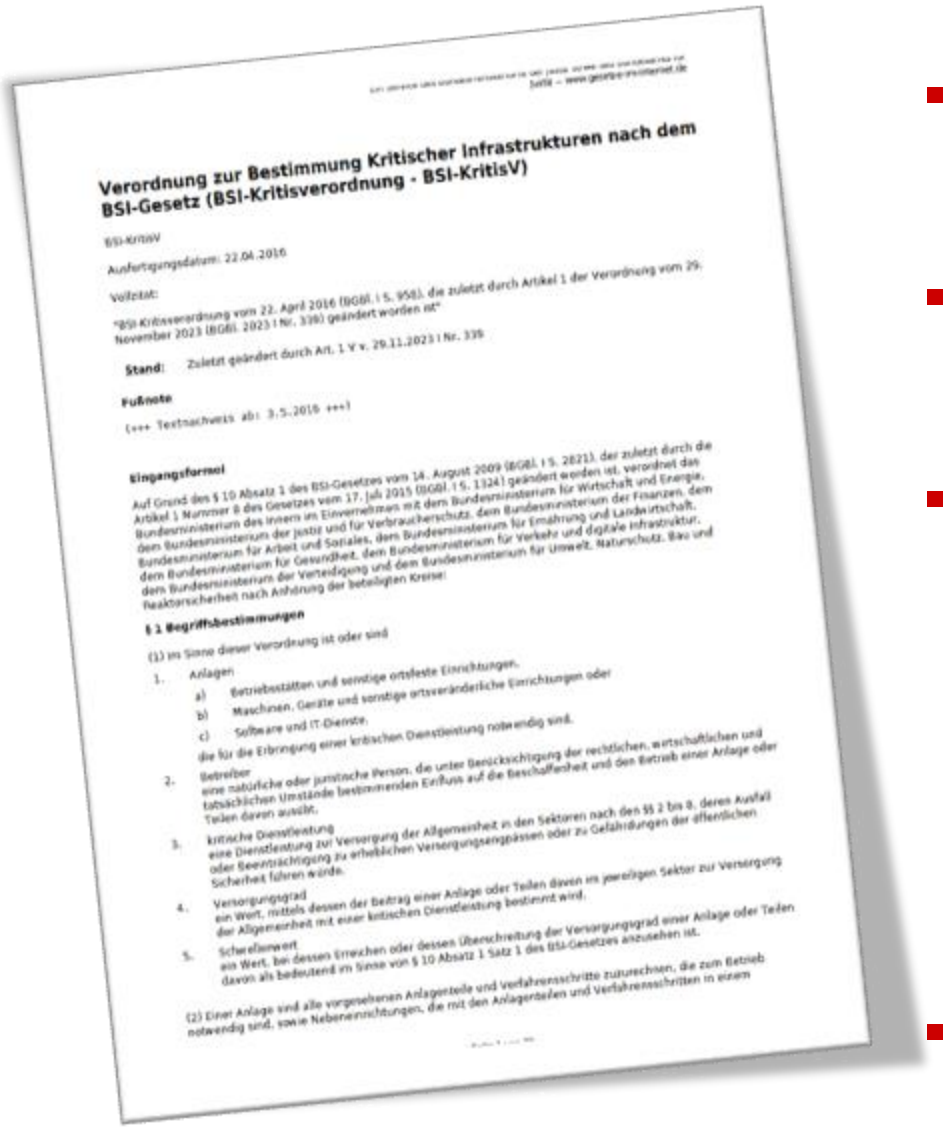
Open Traffic System City Association e.V.

IT-Sicherheitsaspekte beim C-ITS Roll-Out

C-ITS Forum – 27./28. Februar 2024
Dr. Josef Kaltwasser (OCA e.V.)

Bedeutung von IT-Sicherheit in der Verkehrstechnik



Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV)

BSI-KritisV

Ausfertigungsdatum: 22.04.2016

Vollzitat:

"BSI-Kritisverordnung vom 22. April 2016 (BGBl. I S. 958), die zuletzt durch Artikel 1 der Verordnung vom 29. November 2023 (BGBl. 2023 I Nr. 339) geändert worden ist"

Stand: Zuletzt geändert durch Art. 1 V v. 29.11.2023 I Nr. 339

Fußnote

(+++ Textnachweis ab: 3.5.2016 +++)

Eingangsformel

Auf Grund des § 10 Absatz 1 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), der zuletzt durch die Artikel 1 Nummer 8 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1324) geändert worden ist, verordnet das Bundesministerium des Innern im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit nach Anhörung der beteiligten Kreise:

§ 1 Begriffsbestimmungen

(1) Im Sinne dieser Verordnung ist oder sind

1. Anlagen
   a) Betriebsstätten und sonstige ortsfeste Einrichtungen,
   b) Maschinen, Geräte und sonstige ortsveränderliche Einrichtungen oder
   c) Software und IT-Dienste,

   die für die Erbringung einer kritischen Dienstleistung notwendig sind.
2. Betreiber
   eine natürliche oder juristische Person, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf die Beschaffenheit und den Betrieb einer Anlage oder Teilen davon ausübt.
3. kritische Dienstleistung
   eine Dienstleistung zur Versorgung der Allgemeinheit in den Sektoren nach den §§ 2 bis 8, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde.
4. Versorgungsgrad
   ein Wert, mittels dessen der Beitrag einer Anlage oder Teilen davon im jeweiligen Sektor zur Versorgung der Allgemeinheit mit einer kritischen Dienstleistung bestimmt wird.
5. Schwellenwert
   ein Wert, bei dessen Erreichen oder dessen Überschreitung der Versorgungsgrad einer Anlage oder Teilen davon als bedeutend im Sinne von § 10 Absatz 1 Satz 1 des BSI-Gesetzes anzusehen ist.

(2) Einer Anlage sind alle vorgesehenen Anlagenteile und Verfahrensschritte zuzurechnen, die zum Betrieb notwendig sind, sowie Nebeneinrichtungen, die mit den Anlagenteilen und Verfahrensschritten in einem

- IT-Sicherheit ist seit langem Thema in Städten (z.B. System-Kompromittierung durch Hackerangriffe) → IT-Sicherheit ist bereits sehr lange Betrachtungsgegenstand
- Aber die Verkehrstechnik war oft abgeschottet von der Mainstream IT (Eigenes, geschlossenes Netz, eigener IT-Betrieb, …)
- Aber dann: Trigger durch die BSI-KritisV (Für den Sektor „Transport und Verkehr“ ab 2017), Anhang 7, Anlagenkategorie 1.4.2:
  - Anlagenbezeichnung: *Verkehrssteuerungs- und Leitsystem im kommunalen Straßenverkehr*
  - Bemessungskriterium: *Anzahl Einwohner der versorgten Stadt*
  - Schwellenwert: *500.000*
  - (aktuell laut Wikipedia 15 Städte)
- → Anwenderkreis KritisV der OCA

IT-Sicherheit und C-ITS

- C-ITS hat eigene Anforderungen für die Teilnahme am europäischen Vertrauensraum
  - Ein zertifiziertes Informationssicherheitsmanagementsystem (ISMS)
  - Anforderungen an die Zertifizierung der Geräte
  - Registrierung im europäischen Vertrauensraum (→ PKI)
  - …
- Aber die C-ITS Infrastruktur muss auch in die allgemeinen IT-Sicherheitsanforderungen der Verkehrstechnik integriert werden
  - Neue Feldgerätetypen
  - Neue Prozesse
  - Neue Interaktion mit externen Systemen (z.B. An-Abmeldung von Stationen, Zertifikatsbezug, …)
  - …
- Wichtig: Diese Feldgeräte / Prozesse / Interaktionen sind zu einem großen Teil neu und den ISMS-Teams bislang völlig unbekannt
  → neue, aber gleichartige Geräte muss man auf neue Angriffsvektoren untersuchen,
  aber diese innovativen Geräte bringen komplett neue Angriffsflächen!

Synergie – oder eher nicht?

- Man könnte erwarten dass die Beschäftigung mit IT-Sicherheit aus zwei Beweggründen (KritisV und C-ITS Roll-Out) ein Synergiepotenzial hat
- Diese theoretische Überlegung trifft in der Praxis leider oft nicht zu
- Synergieeffekte werden oft nicht erreicht – Friktionen können sogar kontraproduktiv sein
- Schwierigkeiten:
  - Die neuartigen Feldgeräte – mit ihren unterschiedlichen Schnittstellen – bieten eine Angriffsfläche, deren Risikoanalyse noch schwer fällt
  - C-ITS nutzt bislang unbekannte Technologien, z.B. Nahbereichsfunk mit Rundspruchtechnik ohne IP-Verbindungen; bislang unbekannte Formate digitaler Zertifikate (ETSI TS 103 097), …
  - Die Forderung, dass jede ITS-Station eine Verbindung zur Zertifikatsvergabe haben muss:
    - Interne Verbindung: der Betreiber muss selber eine Zertifikatsvergabe betreiben und im europäischen Vertrauensraum registrieren → prohibitiver Aufwand
    - Externe Verbindung: Feldgerät mit Internet-Konnektivität
  - usw.

Gerätezertifizierung

- C-ITS Stations müssen gemäß Security Policy gegen ein zertifiziertes *Protection Profile* (Schutzprofil) zertifiziert werden
- Ein solches, zertifiziertes Schutzprofil existiert für allgemeine R-ITS-S noch nicht
- Übergangsweise kann man – unter Einhaltung definierter Bedingungen – auch selber gemäß Common Criteria (ISO 15408) zertifizieren lassen
  → kompliziert, zeitaufwendig und teuer
  → für Kommunen wohl nur in wenigen Fällen ein gangbarer Weg
- Aber: Im Rahmen von C-Roads wurde ein solches Schutzprofil für Feldgeräte erarbeitet, dieses liegt aber zurzeit noch zur Zertifizierung beim BSI
  → wir können davon ausgehen, dass es bald vorliegt 👍
- Wichtig: die Gerätezertifizierung bestätigt nur die Sicherheit des Geräts im Hinblick auf Vertraulichkeit, Integrität und Verfügbarkeit – die Sicherheit der Einbindung des Geräts in der Feldebene und der Konnektivität zur Zentrale sind getrennt zu betrachten (→ ISMS)
- Auch wichtig: die Anforderungen gelten für alle ITS-S → auch für die Zentrale, wenn sie Meldungen erzeugt und signiert→ Für Zentralen ist noch kein Protection Profile verfügbar

Was also tun?

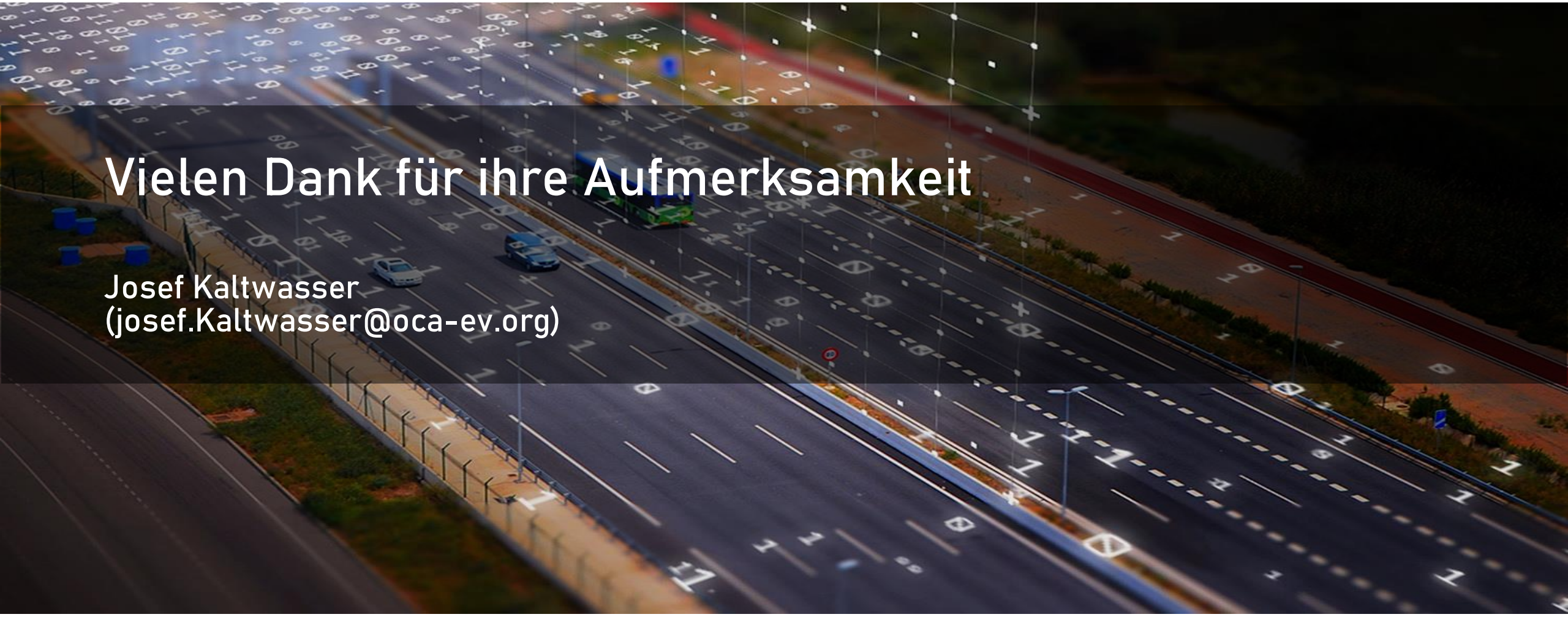
- Die Einbindung von C-ITS Systemen in die kommunale Verkehrstechnik erfordert die gleichzeitige Betrachtung der allgemeinen Anforderungen (→ KritisV) und der C-ITS-spezifischen Kriterien an IT-Sicherheitsmechanismen
- Daraus folgt die intensive Kooperation von Fachabteilung(en) und IT-Sicherheitsteam bei der Gestaltung und Zertifizierung des ISMS
- Die individuelle Gerätezertifizierung im kommunalen Umfeld auf der Basis von Common Criteria wird nur selten realistisch sein → wir brauchen das BSI-zertifizierte Schutzprofil (und dieses sollte dann natürlich in einer Überarbeitung des B3S für Anlagenkategorie 1.4.2 zitiert werden → Verantwortung beim BSI)
- Eine Entscheidung über die zu verwendende PKI-Lösung muss rechtzeitig getroffen werden – es gibt die Möglichkeit, eine eigene PKI zu betreiben und es gibt die Möglichkeit, eine PKI der Europäischen Kommission zu nutzen; der wohl von allen präferierte Weg wäre aber eine „Bundes-PKI“ für die Verwendung von Kommunen, Verkehrsbetrieben und weiteren Akteuren

Aktuelle Entwicklungen

- Das Schutzprofil für ITS-Stations liegt zur Zertifizierung beim BSI und hat bereits wesentliche Schritte absolviert → von einer Verfügbarkeit in naher Zukunft ist auszugehen
- Die aktuelle Version 3.0 des EU Security Policy (2023) referenziert die NIS / NIS2-Richtlinien und damit das BSIG und die KritisV:
  „C-ITS Station operators that operate an essential road transport service according to the NIS [10] or NIS 2 [11] Directives may apply the security measures and security requirements defined by the national transposition of the NIS [10] or NIS 2 [11] Directives instead.“
  → Die Maßnahmen zur Umsetzung der KritisV erfüllen die Anforderung der EU
- Diskussionen im *ITS Beirat Digitalisierung der Mobilität* des BMDV lassen hoffen, dass eine Verfügbarkeit einer „Bundes PKI“ aktiv betrieben wird
- Die Automobilindustrie zeigt Roadmaps, auf denen auch die Anwendungsfälle an signalisierten Kontenpunkten vorkommen → in Zukunft können sowohl die Anwendungsfälle für die Priorisierung (ÖPNV, Einsatzkräfte, …) als auch für den MIV in der Realität umgesetzt werden

Conclusio

- Die Berücksichtigung von IT-Sicherheitsaspekte hat beim C-ITS Roll-Out große Bedeutung
- Eine sinnvolle Vorgehensweise bedingt frühzeitige Überlegung und das Zusammenbringen unterschiedlicher Organisationseinheiten (beachte: Vertrauen braucht Zeit)
- Hürden existieren, sind aber zunehmend überwindbar
  - Aktuelle Security Policy erlaubt Synergie von C-ITS mit KritisV Anforderungen bzgl. ISMS
  - Ein Schutzprofil für ITS-Stations als effektive Grundlage der Zertifizierung der Feldgeräte wird bald zur Verfügung stehen
  - Die Notwendigkeit, den Zugang zu einer regelbetriebsfähigen PKI für alle Akteure (insbesondere auch Kommunen und Verkehrsbetriebe) zur Verfügung zu stellen, ist verstanden worden
  - Der Markt von verfügbaren Geräten wächst
  - …
- → Eine Planung von C-ITS Roll-Out im Regelbetrieb kann begonnen werden!
  Die Planung muss natürlich noch an einigen Stellen mit Bedingungen arbeiten (Verfügbarkeit Schutzprofil gegeben?, Zugang zu PKI erstellt?, …) und muss daher flexibel ausgelegt werden



Vielen Dank für ihre Aufmerksamkeit

Josef Kaltwasser
(josef.Kaltwasser@oca-ev.org)