CSI CONSULTING
INFORMATION AND COMMUNICATION

25 JAHRE

Polizei-Fahrzeuge mit Zwangsvernetzung

Motorisierte Smartphones wider Willen?

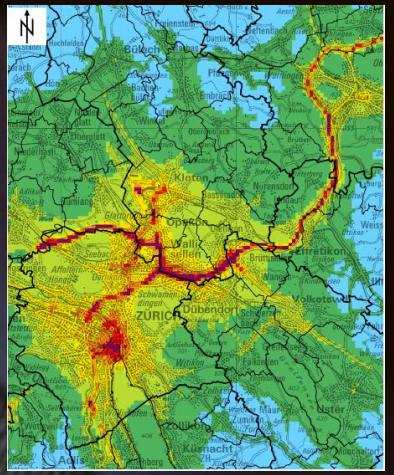
Quelle: en.cryptonomist.ch

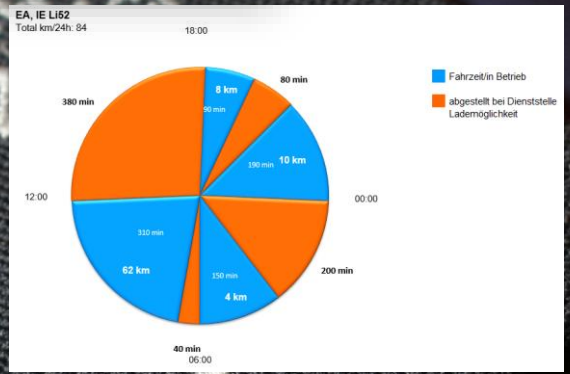
Der Auslöser

Stadt Zürich
Stadtpolizei

Projektziele: Patrouillen-Fahrzeuge

1. **Analysieren**, ob der **Fahrzeugmarkt** aktuell oder in naher Zukunft Fahrzeuge mit **alternativer Antriebsart** bietet, welche die Anforderungen an Einsatzfahrzeuge bei der Stadtpolizei Zürich erfüllen.
2. **Beschaffen** von Ersatz-Patrouillenfahrzeugen der **Verkehrs-polizei** gemäss Anforderungsprofil, unter Berücksichtigung dieser Marktanalyse.
3. **Gewinnen** von Erkenntnissen im Bereich der **datenschutzrechtlichen** Bestimmungen und Anforderungen.





Stadt Zürich
Stadtpolizei

Ausgangslage

CSI CONSULTING
INFORMATION AND COMMUNICATION

Daten-Inventar

- Schutz «meiner» Fahrzeugdaten: Vorgaben für Submission
- Nutzung «meiner» Fahrzeugdaten: Flottenmanagement und Ortung für EZ

Schaffung von Transparenz: 3 Methoden

- Reverse Engineering
- Publikationen
- Herstellerbefragung

Fahrzeugbeschaffung ist der Auftrag

- Informationssicherheit und Datenschutz sind Teilaspekte
- Erfahrungen anderer Korps und Arbeiten der PTI
- nüchterne Erwartungshaltung der Stadtpolizei Zürich gegenüber den Marktkräften

«Meine» Fahrzeugdaten, aber wo sind sie?

CSI CONSULTING
INFORMATION AND COMMUNICATION

Norm-Diagnose-Schnittstelle (OBD-II / EOBD) für Werkstatt und Hersteller

Fülle von Daten über die Diagnose-Schnittstelle

- nicht nur für die Werkstatt, sondern auch für mich als Besitzer
- Stapo ZH: Streckenerfassung mit Tanken und Verbrauchsanalyse (Fahrtenbuch)
- Stapo ZH: Ortung
- alles offline am Stecker oder **online** mit Adapter

«Meine» Fahrzeugdaten, aber wo sind sie?

CSI CONSULTING
INFORMATION AND COMMUNICATION

Norm-Diagnose-Schnittstelle (OBD-II / EOBD) für Werkstatt und Hersteller

Fülle von Daten über die Diagnose-Schnittstelle

- nicht nur für die Werkstatt, sondern auch für mich als Besitzer
- Stapo ZH: Streckenerfassung mit Tanken und Verbrauchsanalyse
- Stapo ZH: Ortung
- alles offline am Stecker (oder online mit Adapter)

Erkenntnis 1: OBD-II-Adapter sind kein universeller Ausgangspunkt für die Nutzung

- bekannte Datensätze gemäss Vorschriften, Unterlagen der Hersteller und Bastler
- professionelle Nutzung bleibt möglich, aber mit dem Segen jedes einzelnen Herstellers

Erkenntnis 2: unbekannter Datenfluss in der Werkstatt

- viele Daten sind im Fahrzeug gespeichert und fliessen über die Werkstatt ab
- sind das «meine» Daten aus meinem Fahrzeug?

«Meine» Fahrzeugdaten und wohin gehen sie?

CSI CONSULTING
INFORMATION AND COMMUNICATION

Rückschlüsse auf Fahrer (und mehr aus Publikationen)

- direkt: Müdigkeitserkennung per Kamera, Sprachsteuerung
- indirekt: Fahrstil, Gewicht, Sitzeinstellung

Aufzeichnung von Bild und Ton

Eindeutige Zuordnung der Daten auf Fahrzeug und vermutlich auf Personen

- gerechtfertigt für die Werkstatt, aber wer garantiert den Datenschutz
- wohin gehen «meine» (Fahrzeug-)Daten?

Hersteller haben nicht nur offline Diagnose-Tools in der Werkstatt

Untersuchungen u.a. vom ADAC (2015, 2019) und unsere Herstellerbefragung

- fast jedes moderne Fahrzeug spricht online (oder periodisch) mit Hersteller und mit Dritten
- Abfluss der Daten intransparent (wie früher bei den Smartphones)
- Daten als Geschäftsmodell z.B. für Staumeldung, Tanken, Hotel, …

➢ Stadtpolizei Zürich: ISDS-Konzept pro Fahrzeugtyp notwendig

Hersteller-Befragung

CSI CONSULTING
INFORMATION AND COMMUNICATION

Die Stadtpolizei Zürich war nicht das erste Korps mit Fragen im 2019

→ zum Teil sehr gute Antworten, aber auch viel Ignoranz und Ausweichen

…doch klare Grundaussagen zum Datenschutz

- die ganz heiklen Punkte (online **Ortung** und **Tonübertragung**) sind grundsätzlich lösbar
- hohe Einbusse bei **Deaktivierung** der Datenübertragung
- Zukunft: mehr Datenübertragung (v.a. Einbindung von Smartphones / Navigation)
- viele Parteien erhalten Daten, viele Datenquellen im Fahrzeug

…und klare Aussagen zur Zwangsvernetzung der Fahrzeuge

- künftig wird das Fahrzeug vernetzt sein
- nur offline Kommunikation via Werkstatt wird verschwinden
- Brisanz des Themas Datenschutz ist erkannt

«Meine» Daten und «deine» Daten

CSI CONSULTING
INFORMATION AND COMMUNICATION

Wie beim Smartphone – 3 Sichtweisen auf die Datenhoheit:

1. Ignoranz / Blackbox: «Es gibt keine Daten»
2. einseitiger Service-Gedanke: «Die Daten gehören alle dem Hersteller»
3. Kundenfokus (es gibt «meine» und «deine» Daten)

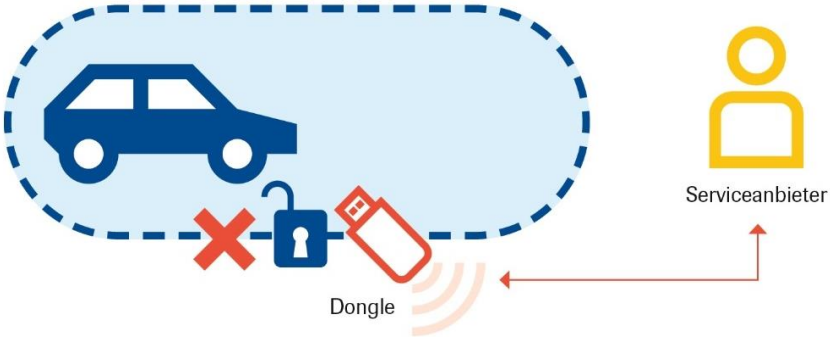
Forderung von vielen Seiten, auch von der Politik (in Europa) nach:

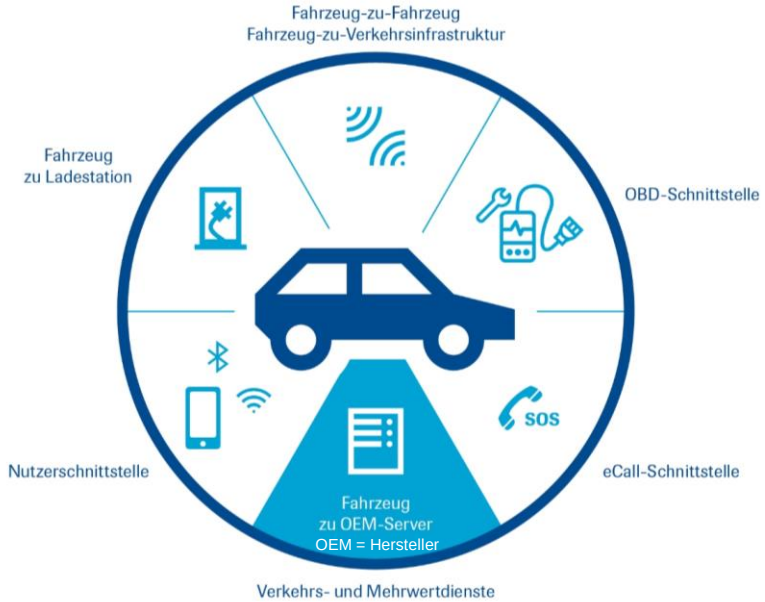
- Transparenz und Rechtmässigkeit
- Zweckbindung und Datenminimierung
- Richtigkeit / Löschbarkeit und zeitlicher Begrenzung

Quelle: www.privacyxperts.de

Umdenken und Positionierung

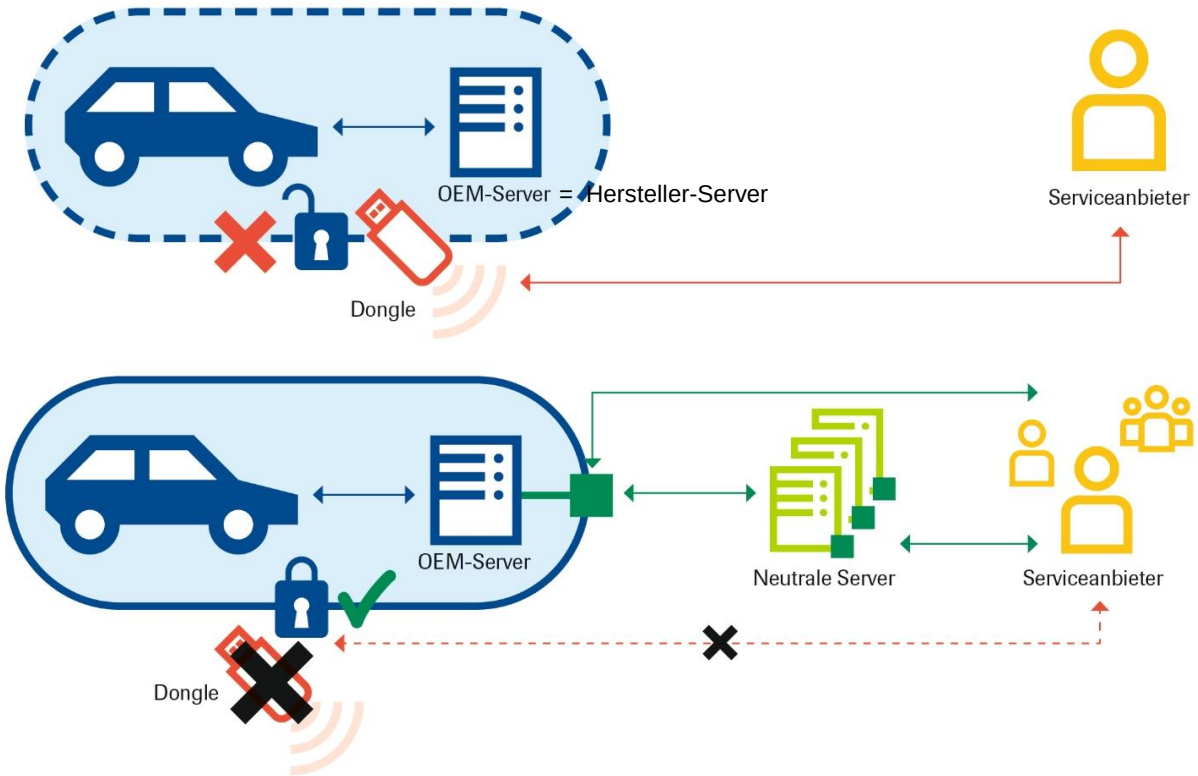
- Modell des Verbands der Automobilindustrie (VDA) per 2017
- "Extended Vehicle" (Fahrzeug-Hardware plus Fahrzeugdaten beim Hersteller)





Quelle: VDA

Umdenken und Positionierung: VDA-Modell



alte Welt: ODB-II
(idealisierte Gegenwart)

neue Welt: «Cloud»

Quelle: VDA

Daten-Inventar im VDA-Modell

CSI CONSULTING
INFORMATION AND COMMUNICATION

Kategorie 1	Kategorie 2	Kategorie 3a	Kategorie 3b	Kategorie 4
Daten zur Verbesserung der Straßenverkehrs-sicherheit	Daten für marken-übergreifende Services	Daten für marken-spezifische Services	Daten für die Komponen-tenanalyse und Produkt-optimierung	Persönliche Daten
Verkehrssicherheitsrele-vante Daten	Undifferenzierte Fahrzeugdaten	**IP = geistiges Eigentum** Differenzierte und für den OEM IP-relevante Fahrzeugdaten	Differenzierte und für den OEM sowie Zulieferer IP-relevante Fahrzeugdaten	„Recht auf Zugriff" nur für zur Datenverarbeitung befugte Parteien (Befugnis durch Gesetz, Vertrag oder Vereinbarung)
Daten für z.B.: öffentliche Verkehrsleitzentralen	Diskriminierungsfreier Datenzugriff für Dritte[#2] [#3]	**OEM = Hersteller** OEM oder vom OEM beauftragter Partner	**OEM = Hersteller** OEM oder vom OEM beauftragter Partner	Vom Kunden ausgewählte(r) Partner
Feuerwehr, Polizei, …	Produkt	Händler, Tochterges.	Produkt	Kunde

Der Kunde[#1] wird über die Nutzung der Daten informiert. Die OEMs werden dem Kunden Entscheidungsoptionen, die er jederzeit widerrufen kann, zur Verfügung stellen, es sei denn, die betreffende Funktion ist gesetzlich vorgeschrieben.

[#1] Der Begriff „Kunde" wird hier einheitlich und weit gefasst genutzt. Kontextual abhängig sind hier Fahrer, Halter oder Nutzer gemeint.
[#2] Beteiligung und technische Umrüstung des Fahrzeugs können vom OEM nicht verlangt werden.
[#3] Die Leitprinzipien sind bei der Nutzung des definierten Dateninterfaces zu beachten. Die Nutzung des Interfaces schließt Rechte und Pflichten mit ein.

Quelle: VDA

Einschätzung Informationssicherheit

CSI CONSULTING
INFORMATION AND COMMUNICATION

Leistungsnachweis aus der Vergangenheit (und Gegenwart) schlecht

- viele Fehler der ICT nochmals gemacht
- Gefahrenbewusstsein und Haltung ändern sich nur langsam
- Technologie (z.B. Cloud-Lösungen) ändert sich schnell(er)

Ansätze (auch VDA) gut, adressieren aber die Informationssicherheit nicht direkt

Hoffnung auf Besserung wegen Herstellerhaftung bei Unfällen berechtigt, aber

- lohnendes Hackerziel (DoS-Angriffe), ob Kunde (z.B. Polizei-Korps) oder Hersteller
- steigende Komplexität der Car2X-Kommunikation
- höhere Qualität bei Steuerung als bei Komfortfunktionen

Angst um Autonomieverlust der Fahrzeuge bei Sicherheitsproblemen

Für Nutzer (inkl. Korps) bleibt das Fahrzeug weitgehend eine Black-Box

- Verträge, Vertrauen und punktueller Dialog
- ggf. Deaktivierung oder getrennte Systeme (Funk, Boardcomputer, Wifi-AP)

Einschätzung Datenschutz

CSI CONSULTING
INFORMATION AND COMMUNICATION

Vernetzung mittelfristig nicht vermeidbar (Zwangsvernetzung)

Datenabfluss online / offline ist unvermeidlich auch an Dritte

- Zulieferer wie bisher, aber neu auch für (Mehrwert-)Dienste
- neben fahrzeugbezogenen Daten auch potentiell personenbezogene Daten
- Normen und Industrie-Standards am Entstehen

viele Kräfte fordern Daten (auch Umweltschutz, Verkehrslenkung)

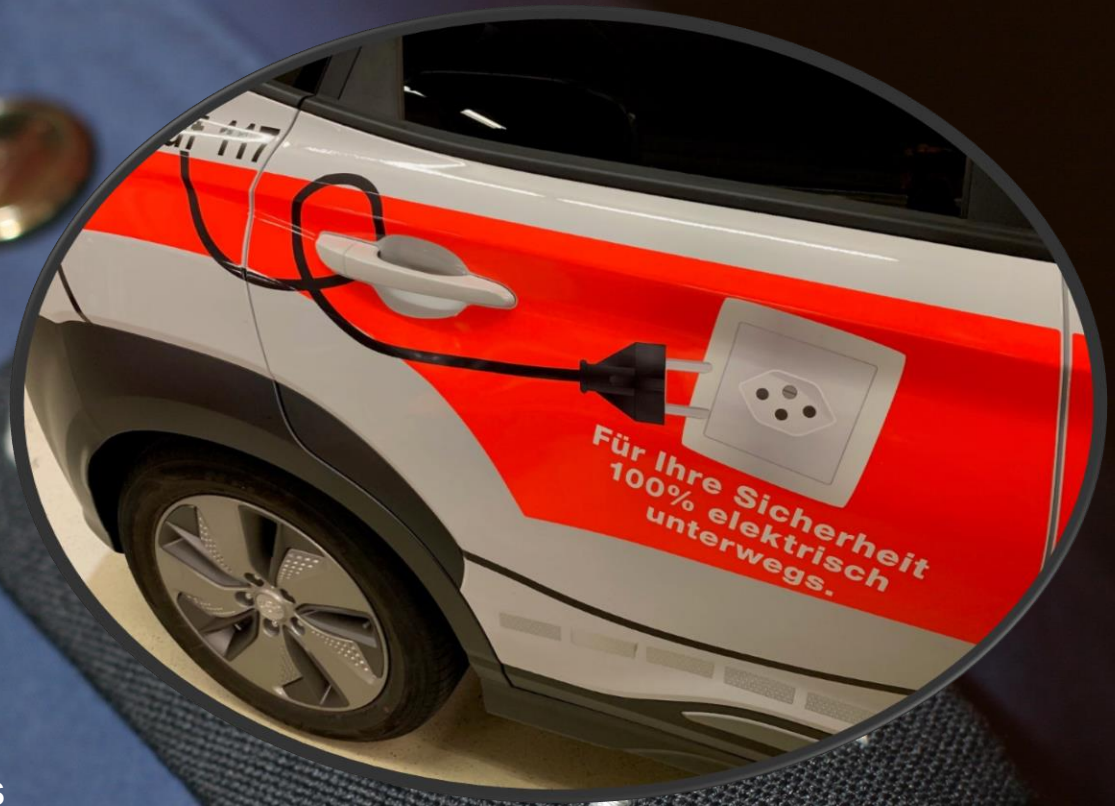
keine generelle Entwarnung: die Korps bleiben in der Pflicht

Daher Entscheide der Stadtpolizei Zürich für die Fahrzeugbeschaffung:

1. kein Verbot für online Vernetzung
2. keine Modifikation der Fahrzeug-Sensorik
3. keine Eignungskriterien für Submission sondern Selbstdeklaration / Dialog
4. ISDS-Konzept für Fahrzeugnutzung (mit Vorgaben / Schulung für Nutzer)

Schlussbetrachtung

- auch Polizei-Fahrzeuge sind im Sog des IoT
- operative und gesetzliche Auflagen unterliegen der Sorgfaltspflicht der Korps
- neben der Physik des Fahrzeugs lernen wir mit seiner IT umzugehen
- mit dem Markt und mit den Mitarbeitenden finden sich vertretbare Lösungen, wie damals bei der **Einführung der Smartphones**



Stadt Zürich
Stadtpolizei

CSICONSULTING
INFORMATION AND COMMUNICATION

Patrick Gerber

patrick.gerber@csiconsulting.ch