Kybernetická bezpečnost v automobilovém sektoru

Kdy budeme moct věřit svým autům?

Tomáš Kulda | Cyber & Privacy

pwc

Cyber & Privacy

PwC Česká republika | 16. 9. 2020

Kybernetické výzvy v automobilovém sektoru

750 mil

vozidel připojených k internetu do roku 2023.

100 mil

řádků kódu obsažených v průměrném moderním voze.

Nula

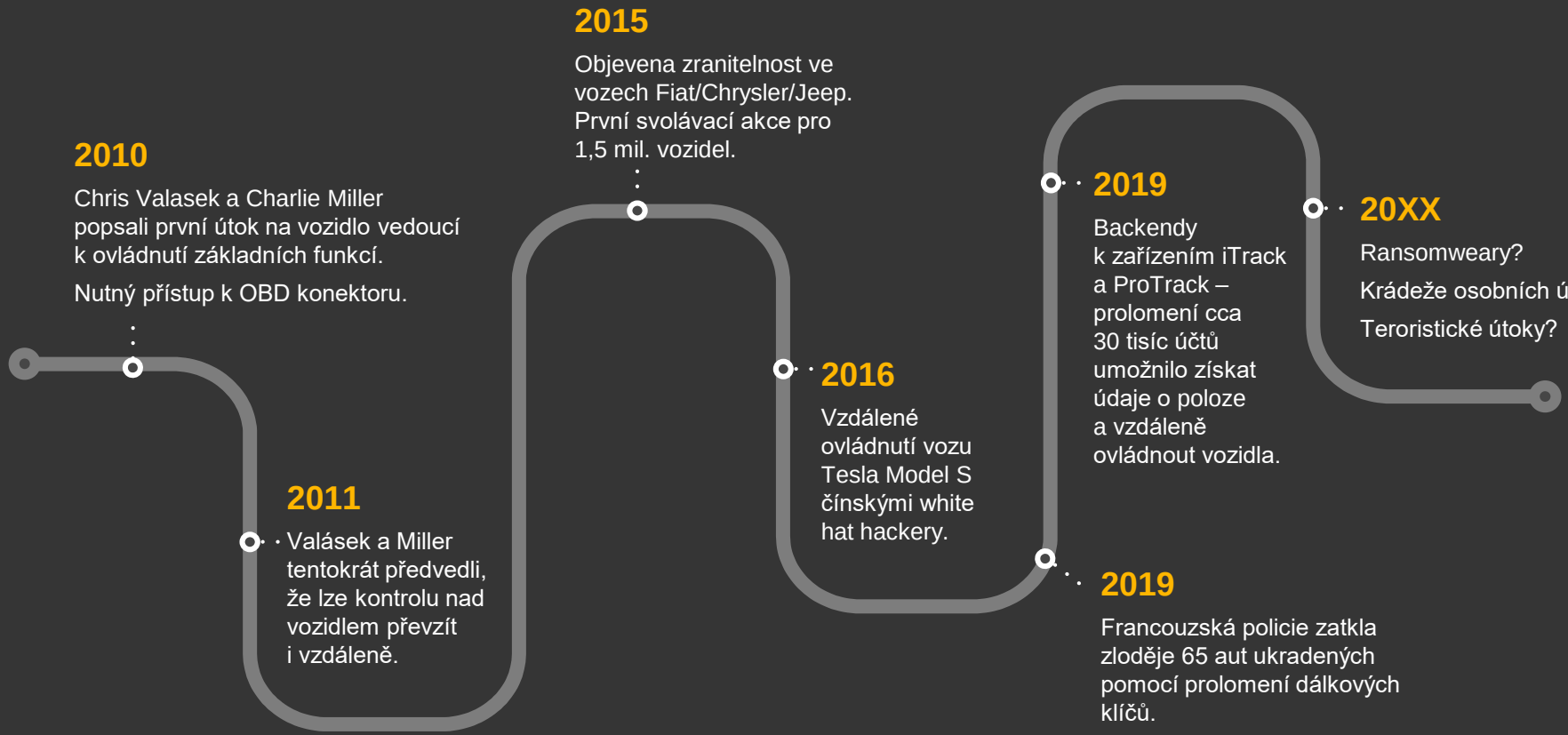
závazných regulací v oblasti kybernetické bezpečnosti vozidel.

Obsah

Kybernetické hrozby pro automobily

1

Vývoj útoků na vozidla



Hlavní oblasti ochrany

Bezpečí a zdraví uživatele a okolí

Funkčnost vozu

Ochrana osobních dat

Finanční dopady a krádeže

Výzvy pro bezpečnost automobilů

Komplexita vozů

Narůstající počet systémů ve vozech

Zvětšující se plocha útoku

Kompatibilita elektronických součástek

Propojení ECU jednotek a infotainmentu

Rozvoj autonomních vozidel

Back-end systémy

Vozy jsou napojené na systémy výrobců a poskytovatelů služeb

OTA aktualizace softwaru

Rozsáhlé sítě systémů mimo vozidlo

Dodavatelský řetězec

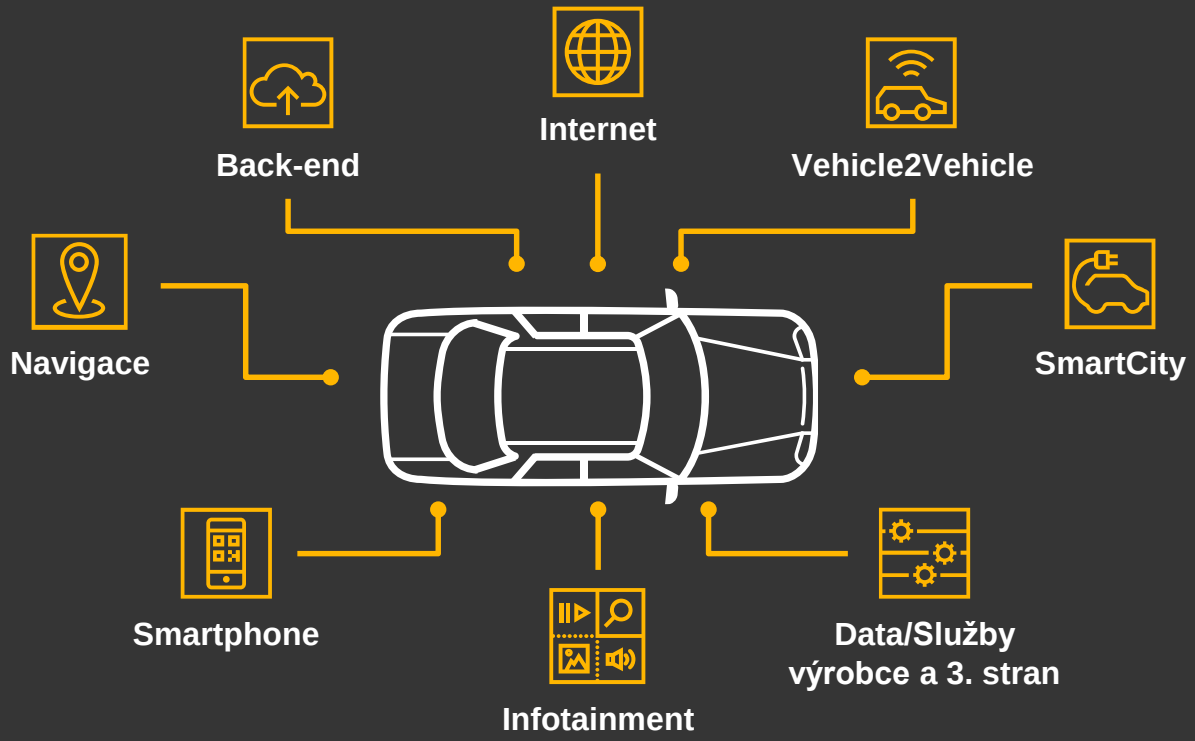
Horizontální a vertikální spolupráce

Nutnost zajistit podporu po celou dobu životního cyklu produktu

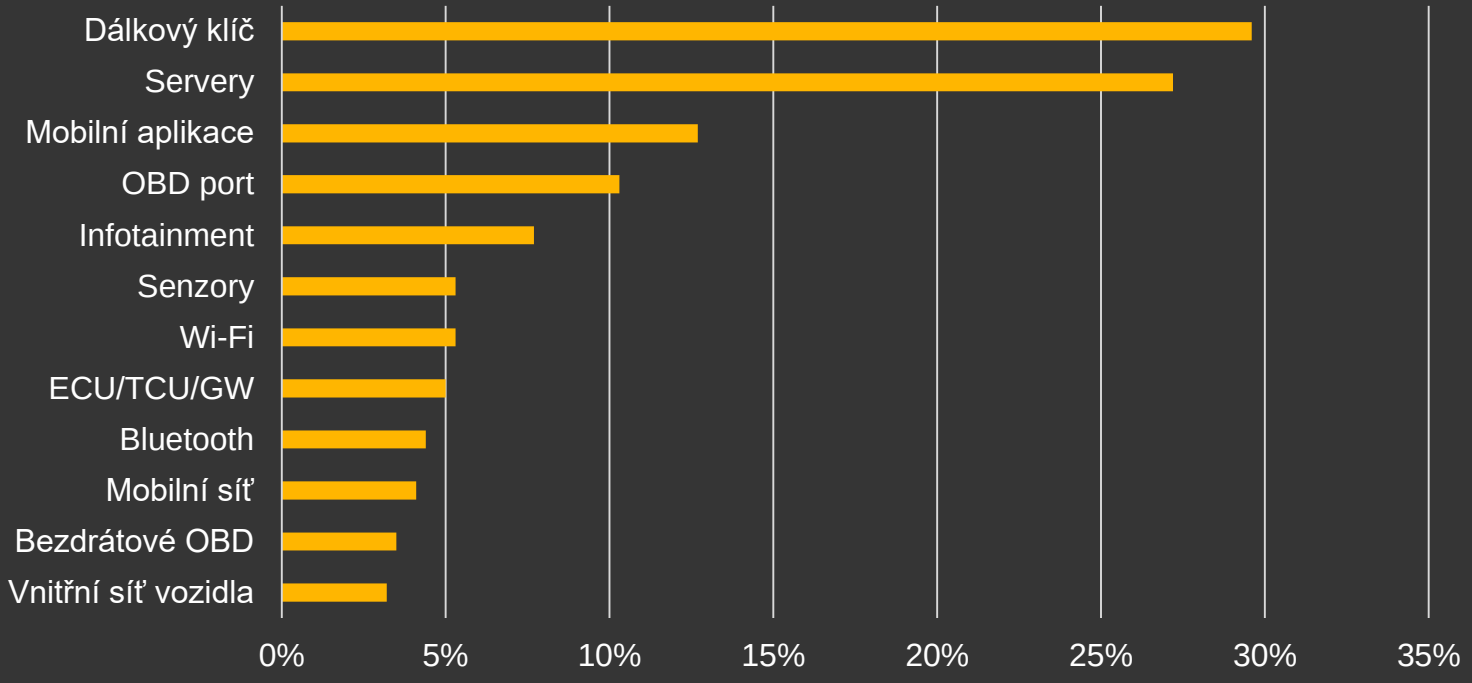
Vývoj hrozeb

Potřeba čelit novým hrozbám během celého životního cyklu vozu – může se jednat o 10–15 let

Ekosystém vozu



Rozložení cílů útoků 2010-2020



Zdroj: Upstream Security

Odpověď na kybernetické hrozby

2

Jak zajistit bezpečnost automobilu?

1 Funkční bezpečnost

Zaměření na omezení negativních dopadů na zdraví v případě technické závady na elektronice.

ISO 26262

2 Kybernetická bezpečnost vozu

Ochrana elektronických systémů před vnějšími útoky.

UNECE – CSMS

ISO/SAE 21434

3 IT bezpečnost výrobce

Zajištění ochrany systémů výrobce během vývoje vozidla a backendů používaných vozidly v provozu.

ISO 27001, TISAX

Současný přístup

Industry doporučení

- SAE J3061 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems (2016)
- ENISA Good Practices For Security Of Smart Cars (2019)

Bug-bounty programy

- Reaktivní opatření, pomáhá výrobcům odhalovat existující zranitelnosti.
- Interní systémy vozidel, back-endy, aplikace

3rd party služby

- Analýzy hrozeb a incidentů
- Řešení pro šifrování dat a CAN sítí
- Služby V-SOC

Nové regulace v automobilovém sektoru

3

Proč potřebujeme regulace?

Roční objem trhu v oblasti kybernetické bezpečnosti automotive sektoru vzroste z 4.9 mld USD v roce 2020 na 9.7 mld USD v roce 2030.

GSA & McKinsey
Cybersecurity in automotive

Ochrana uživatelů

Splnění požadavků regulace poskytuje zákazníkům garanci, že bezpečnosti vozu byla věnovaná patřičná pozornost.

Nastavení rámce pro všechny zainteresované strany

Zlepšení spolupráce mezi výrobci vozů, dodavateli dílů, softwaru a poskytovateli služeb.

Usnadnění vývoje nových produktů a služeb v oblasti kybernetické bezpečnosti aut.

Nové regulace a standardy

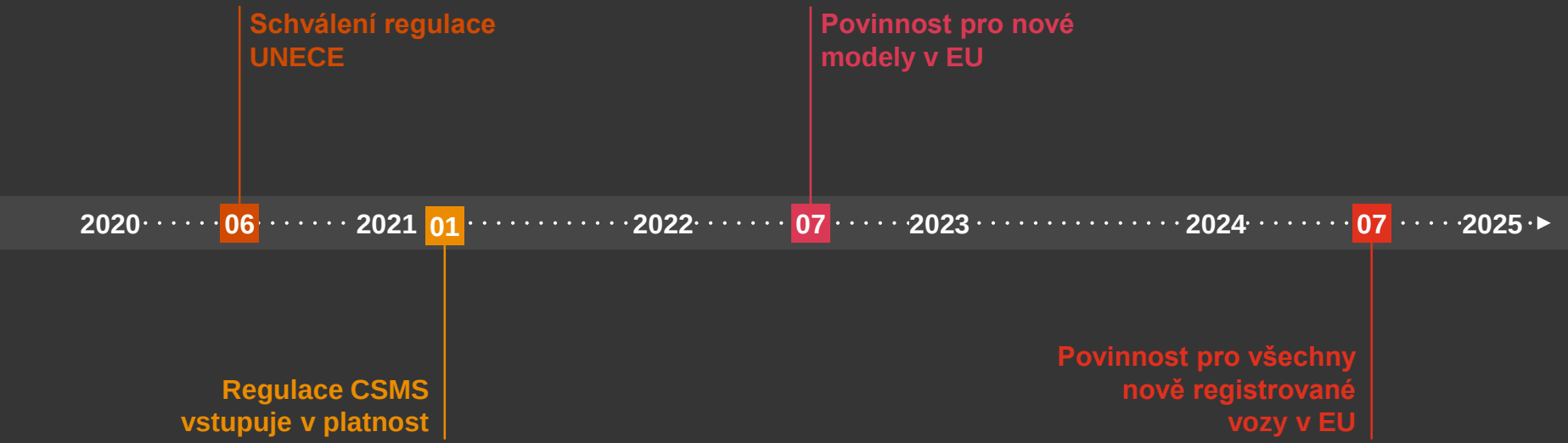
UNECE

- UNECE WP.29 Regulation on Cybersecurity and **Cyber Security Management Systems (CSMS)**
- UNECE WP.29 Regulation on Software Updates and **Software Updates Management Systems (SUMS)**

ISO

- ISO/SAE 21434 Road vehicles – **Cybersecurity engineering**
- ISO 24089 Road vehicles **– Software Update Engineering**

Timeline zavádění regulací UNECE – CSMS & SUMS



CSMS – Certifikace společnosti

Životní cyklus

Systém CSMS musí pokrývat všechny fáze životního cyklu vozidel: vývoj, výrobu i provoz.

Včasná reakce na incidenty a rizika

Výrobce musí doložit, že je schopen identifikovaná rizika a incidenty řešit bezodkladně.

Dodavatelský řetězec

Výrobce je odpovědný za rizika, která by mohla vzniknout u subdodavatelů, poskytovatelů služeb, nebo podřízených společností.

Systém řízení rizik

Výrobce musí zavést systém na řízení kybernetických rizik vozidel, pokrývající všechny elektronické díly a funkce.

Kontinuální aktualizace rizik

Posuzování rizik musí být kontinuální. Výrobce zajistí, že nové hrozby nebo zranitelnosti budou posouzeny i na komponentách v provozu.

Monitoring vozidel a Incident response

Výrobce musí zajistit monitoring vozů a systém na detekci a řešení bezpečnostních incidentů v ekosystému vozu. Každý rok podává zprávu o proběhlých incidentech.

CSMS – Certifikace vozu

Kompletní analýza rizik vozu

Ke každé komponentě musí být zpracována detailní analýza rizik zaměřená na dopady na uživatele vozu.

Posouzeny musí být všechny hrozby uvedené v příloze 5 regulace UNECE.

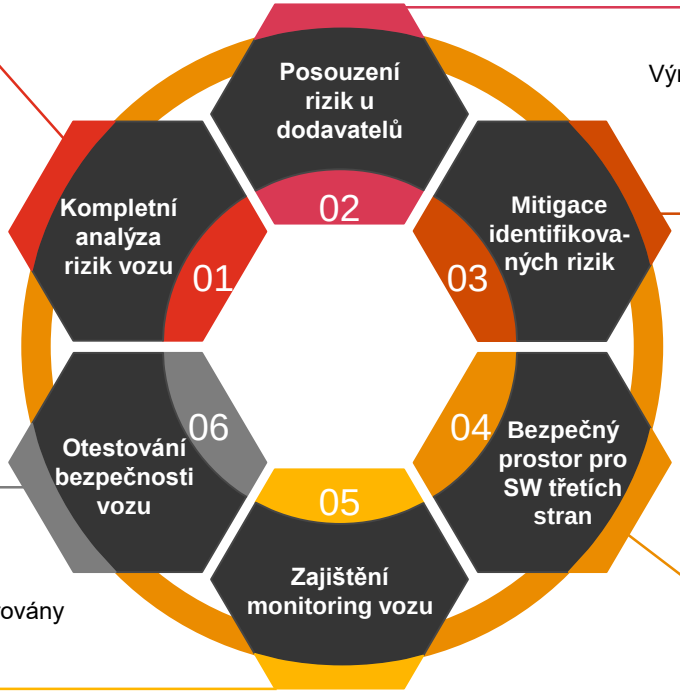
Otestování bezpečnosti vozu

Před homologací vozu je nutné otestovat jeho systémy proti případným útokům.

Testy jsou zaměřené na bezpečnost vozidla jako celku a interakcí mezi jednotlivými díly.

Zajištění monitoringu vozu

Elektronické systémy ve vozech musí být monitorovány interním IDS systémem, který odesílá záznamy o incidentech výrobci vozidla.



Posouzení rizik u dodavatelů

Výrobce musí doložit výsledky analýzy rizik u všech komponent a SW dodaných subdodavateli. Posuzování by mělo probíhat na základě smluv potřebných pro certifikaci společnosti.

Mitigace identifikovaných rizik

Všechna identifikovaná rizika jak u výrobce, tak dodavatelů, musí být řádně ošetřena.

Doporučené mitigační kroky jsou opět popsané v příloze 5 regulace UNECE.

Bezpečný prostor pro SW třetích stran

Vůz musí mít dedikované úložiště pro SW třetích stran, který je oddělený od zbytku elektroniky a chrání vůz před škodlivým SW.

SUMS – Software Update Management System

Asset management

- Evidence HW a SW v jednotlivých vozech
- Evidence verzí SW a statusu aktualizací v každém voze

Vyhodnocení rizik

- Dopady update na ostatní funkce voze
- Vliv na funkce vozu
- Dopady na bezpečnost vozu a řízení

Informovanost uživatele

- Povinnost informovat uživatele o update
- Potřeba jeho schválení na displeji vozu
- Instrukce pro úspěšný update

Procesní dokumentace

- Řádně popsané všechny relevantní procesy
- Certifikace SUMS technickou autoritou

Kdy tedy budeme moct věřit svým autům?

Děkuji za pozornost

Tomáš Kulda
Cyber & Privacy
PwC Česká republika
tomas.kulda@pwc.com