Comunicato stampa

Cybersecurity e automotive: le 3 sfide del 2022 per la sicurezza dell'utente secondo Teoresi

Il 2022 sarà l'anno decisivo per la cybersecurity nell'automotive, per lo sviluppo della smart mobility e per la creazione di connected car sempre più sicure ed efficienti: ***Teoresi*** *affianca l'industria dell'automotive per garantire all'utente finale privacy e sicurezza del veicolo.*

Nell'industria automobilistica si sta verificando un profondo cambiamento dovuto all'interesse crescente degli utenti per la **smart mobility** e per il mercato delle **connected car**. In Italia, nello specifico, i dati sono particolarmente ottimistici: secondo quanto riporta nel 2021 il Global Automotive Consumer Study, il 71% dei consumatori italiani si dice favorevole all'idea di veicoli sempre più connessi, contro il 46-44% di Stati Uniti, il 42% e 33% di Francia e Germania. Un'elaborazione dell'Osservatorio Autopromotec riporta inoltre che **entro il 2025 i veicoli connessi dovrebbero rappresentare circa il 70% di quelli in circolazione**. Il mondo dell'automotive si trova di fronte a una **trasformazione digitale** che porterà presto a vedere la scelta del veicolo influenzata dalla qualità della *digital experience* dell'utente.

Smart mobility e connected car sono dunque il futuro (e il presente) dell'industria: veicoli destinati a essere sempre più connessi e inseriti in un sistema di **smart city**, dove potranno comunicare e scambiare informazioni con la mobilità pubblica, con le altre automobili private e con le aziende produttrici attraverso infrastrutture di connettività per lo scambio dati, che includono il 5G e le piattaforme cloud. Una "città intelligente" che stiamo già costruendo grazie alla **mobilità elettrica e alla mobilità condivisa**: secondo l'Osservatorio Smart & Connected Car della School of Management del Politecnico di Milano, l'87% delle pubbliche amministrazioni considera la smart mobility di grande importanza in questo ambito e il 39% degli utenti ha usato almeno una volta un servizio di mobilità condivisa, soprattutto **car sharing** (21%).

Per far sì che questa comunicazione tra veicoli, aziende e utenti possa svolgersi in efficienza e sicurezza c'è bisogno di una specifica **cybersecurity per i veicoli connessi**. Il 2022 sarà un anno decisivo per la cybersecurity in Europa: a giugno entra in vigore la normativa Unece

R155, approvata dall'Unione Europea, che definisce gli obblighi di cybersicurezza per le aziende dell'automotive. I car maker saranno tenuti a rispettare tali regole per ottenere l'omologazione di una vettura nell'Unione Europea.

"Le connected car sono ormai realtà. Pertanto gli esperti di cybersecurity dovranno sempre più collaborare, in maniera costruttiva, con i realizzatori dei veicoli e con la supply chain relativa al mondo veicolare, per poter garantire l'utilizzo di queste tecnologie, la connettività e le funzioni in completa sicurezza". A sottolinearlo è **Gianluca Cerio, Technology Project Manager Leader di Teoresi**, società internazionale di servizi di ingegneria che progetta soluzioni all'avanguardia lungo tutta la filiera dell'automotive, dalla prototipazione alla ingegnerizzazione di sistemi installati a bordo veicolo.

Grazie alle sue competenze trasversali, **Teoresi** è in grado di occuparsi della tecnologia dell'informazione (Information Technology) presente nel veicolo, come anche degli aspetti inerenti il motore e i freni (Operation Technology): il fine è collaborare con le aziende e assicurare all'utente la migliore esperienza dal punto di vista della performance e della sicurezza.

Affinchè il mercato della *smart mobility* possa svilupparsi e perché vengano immesse in commercio *connected car* sempre più efficienti e affidabili per gli acquirenti finali, la **cybersecurity per l'automotive** passa per **3 step fondamentali**. Sono queste anche le principali sfide che i *car makers*, a fianco di partner come Teoresi, dovranno affrontare nel prossimo futuro. Proprio a partire dal 2022.

1 – Adeguamento alla normativa in vigore dal 2022
Disporre di una normativa sempre applicabile, con elevati livelli di sicurezza, è una necessità. A questo scopo nasce la norma omologativa Unece wp.29, risultato di un World Forum delle Nazioni Unite per l'armonizzazione della cybersecurity in ambito veicolare. La normativa Unece R155, approvata dall'Unione Europea, entrerà in vigore a giugno 2022 per i veicoli di nuova omologazione e a luglio 2024 per tutti gli altri veicoli prodotti, definendo per le aziende dell'automotive specifici obblighi di cybersicurezza. Si applicherà a tutti gli stati membri e le aziende che vorranno mettere in commercio i loro veicoli in questi paesi, dovranno assicurarsi di rispettare il regolamento. Rafforzare la collaborazione con esperti di cybersecurity che conoscano nel dettaglio la normativa, dunque, diventerà una priorità per le imprese del settore automotive.

2 – Attenzione alla sicurezza dell'utente
La normativa prevede che, per garantire la sicurezza dell'utente, siano identificate nel **TARA** (Threat Analysis and Risk Assessment) le minacce più probabili al sistema, valutati i danni possibili e giudicata la loro entità. Tra i **parametri di sicurezza** ci sono la *safety,* l'operatività del veicolo, la *privacy* dell'utente e il danno finanziario. Lo standard prevede una

procedura di analisi e gestione del rischio, valutando anche quanto il danno sia perseguibile e con quale facilità. Un aspetto molto importante: l'analisi TARA accompagna il veicolo per tutto il suo ciclo di vita, dallo sviluppo alla produzione, sino alla fase di post-produzione quando è ancora in circolazione seppur non più in produzione.

3 – Sicurezza per tutto il sistema, non solo per la connected car

Una connected car è immersa in un sistema e comunica pertanto con un back-end: il processo di cybersecurity management, quindi, non può occuparsi solo della gestione del veicolo. La cybersecurity passa per la **messa in sicurezza dell'intero back-end**, tipicamente formato dai server che gestiscono il veicolo, dai server che permettono gli aggiornamenti OTA e dai server che gestiscono i sistemi utente per interagire con l'auto (come le più comuni app dei cellulari). Grande importanza assumerà sempre più la privacy dell'utente, al fine di salvaguardare i suoi dati personali (stile di guida, luoghi visitati, conversazioni, contatti).

Se, a oggi, per gli acquirenti la sicurezza fisica di un veicolo è senza dubbio uno dei fattori principali, nel prossimo futuro la cybersecurity costituirà un ulteriore elemento differenziante tra case automobilistiche, influenzando la scelta del consumatore. Al pari degli investimenti delle dotazioni di *safety*, le aziende lavoreranno sempre più sulla *security*.

Note per la stampa - fonti

- Global Automotive Consumer Study
- Autopromotec
- Osservatorio Smart & Connected Car della School of Management del Politecnico di Milano

Teoresi Group

Teoresi è nata a Torino nel 1987 come società di consulenza informatica. Oggi Teoresi Group è una società internazionale di servizi di ingegneria, che supporta le aziende nella creazione di progetti con le tecnologie più all'avanguardia: dall'auto a guida autonoma alle nanotecnologie applicate all'ambito medicale. Forte di una competenza globale in ambito engineering, Teoresi Group offre progettazione, sviluppo e consulenza tecnologica con attenzione agli aspetti innovativi di ogni sfida progettuale. Affianca il cliente dall'analisi all'ideazione del prodotto finale, dall'idea progettuale al prototipo, dal prototipo al mercato. Teoresi Group è una delle 10 aziende selezionate da Amazon per collaborare allo sviluppo di nuovi prodotti basati sull'interazione vocale di Alexa.

Ufficio stampa Teoresi

Agnese Vellar | +39 340 2620331 | agnese@agenziapressplay.it
Marco Puelli | +39 320 1144691 | marco@agenziapressplay.it