SETTEMBRE
2022

OVER DATA.

ARTIFICIAL INTELLIGENCE & TECH CULTURE

WWW.SPINDOX.IT


LIB.T

OVER DATA.

04 Intelligenza artificiale e tecnologie per la mobilità

08 Le sfide di cybersecurity nel settore automotive

18 Secure by design: la rivoluzione cyber nell'automotive

22 Caso di studio: Come Spindox testa la qualità di una connected car

27 L'importanza di studiare gli attacchi cyber e la normativa

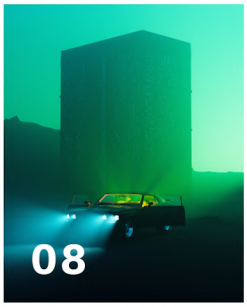
32 Il marketing per le auto di lusso nasce già sulla catena di montaggio

36 Connected health: se la sanità si fonde con l'Artificial Intelligence

44 Accessibilità e inclusione: quando le scorciatoie fanno più male che bene

49 Macchine elettriche e Fit-for-55: l'orizzonte del cambiamento sostenibile

54 L'evoluzione dello sviluppo web: è arrivato FlowerJS



OVER DATA.

www.spindox.it

MISTER SMART INNOVATION

RETE ALTA TECNOLOGIA EMILIA-ROMAGNA HIGH TECHNOLOGY NETWORK

TECNOPOLO BOLOGNA CNR

Focus: **Automotive**

Intelligenza artificiale e tecnologie per la mobilità

Il settore automotive è da sempre un terreno particolarmente fertile per lo sviluppo tecnologico. Gli anni che stiamo vivendo testimoniano un grande fermento nel mondo della ricerca hi-tech in questo mercato, anche e soprattutto in ottica della trasformazione radicale che sta subendo la nostra società. Stiamo parlando di trasformazione digitale:
un processo che tutti abbiamo imparato a conoscere in qualche misura, metaforicamente paragonabile a un fluido in movimento, con la tendenza a trascinare con sé tutto ciò che incontra.

Le informazioni digitali, estraibili anche dai sistemi elettromeccanici più datati tramite attività di retro-fitting (ovvero di sensorizzazione e digitalizzazione di tecnologie di vecchia generazione), si stanno rivelando preziose per capire sempre più a fondo il loro funzionamento. Di conseguenza, è possibile utilizzare questi elementi per ottimizzare per esempio processi, rendimenti, tempistiche, e non è pensabile che un attore di qualsiasi settore possa prescindere da questo cambio di paradigma, pena l'esclusione dal mercato.

La raccolta di dati da sola, però, non basta. Infatti, i metodi che la ricerca nel campo dell'Artificial Intelligence sta studiando e perfezionando sempre più, hanno portato a un'innovazione epocale nella metodologia con cui approcciare i sistemi tecnologici: il paradigma tramite il quale i modelli matematici imparano dai dati.
In questo caso, il modello non conosce le regole per processare l'input, ma il suo task è di ricavarle grazie alla conoscenza degli output. L'importante corollario che se ne ricava è la possibilità di utilizzarli per guidare intelligentemente i sistemi, motivo per cui si parla di sistemi "data driven".

Prospettive innovative nella mobilità

Parlando del settore della mobilità e dell'automotive, queste nuove discipline tecnologiche stanno sviluppando grandi ed importanti innovazioni, che nel futuro potranno cambiare in maniera molto significativa il nostro modo di muoverci, ma anche di concepire il mezzo di locomozione stesso.
I principali obiettivi a lungo termine sono le auto a guida autonoma e le smart cities completamente connesse, la cui realizzazione passa però, per la loro intrinseca complessità, attraverso una grande quantità di obiettivi intermedi.
Si pensi per esempio alla comunicazione in tempo reale tra veicolo e infrastruttura, che può includere dati processati da altri dispositivi, flussi video di traffic cams da elaborare a bordo veicolo oppure precedentemente elaborati, sistemi che possano agevolare la mobilità di persone portatrici di handicap interagendo con il loro smartphone, ecc.

Prima ancora, o se vogliamo anche parallelamente, ci sono le questioni di pura ottimizzazione del funzionamento del mezzo, che sono raggiunte implementando un sistema di AI di bordo che monitora la sensoristica installata, e perseguono obiettivi come la minimizzazione dei consumi, usure, ecc. Tutto ciò che rientra in questo scenario in forte fermento è testimoniato dalla grande quantità di progetti istituzionali e non, oltre ai brevetti esistenti sia a livello nazionale sia internazionale.

Potenzialità della rete 5G

Gli ambiziosi traguardi che ci poniamo possono essere raggiunti unicamente tramite gli sforzi congiunti dei diversi attori coinvolti. Per esempio, una condizione assolutamente necessaria affinché gli scenari sopracitati possano esistere è la presenza di una rete dati mobile ad alta velocità che permetta lo scambio di una grande quantità di dati fra gli autoveicoli, gli incroci, gli edifici.
Nello specifico, la rete 5G permette esattamente questo, motivo per cui è una tecnologia spesso presente nei progetti di ricerca in questo ambito.
Questa tecnologia e le sue potenzialità sono di sicuro interesse per imprese, enti e laboratori di ricerca industriale, che potranno adottarle nell'integrazione di sistemi per il miglioramento della vita delle comunità sotto diversi punti di vista. MISTER Smart Innovation, laboratorio di ricerca industriale accreditato alla Rete dell'Alta Tecnologia dell'Emilia-Romagna, ha partecipato al progetto finanziato dal bando POR-FESR Emilia-Romagna 2014-2020 5G-CAR, nel quale il focus era la sicurezza stradale dei mezzi di soccorso.

Il progetto aveva l'obiettivo di sviluppare un dispositivo da installare sul mezzo, che riceve tramite connessione 5G il flusso video di una telecamera posta a un incrocio stradale. L'hardware sul mezzo si occupava di analizzare tramite AI il flusso video, per ricavarne informazioni sull'occupazione della carreggiata ed eventualmente allertare il conducente qualche centinaio di metri prima dell'arrivo all'incrocio.

Tecnologia al servizio delle amministrazioni pubbliche

Questo è solo un esempio delle possibilità che queste tecnologie ci possono offrire: non solo mobilità smart, sicurezza stradale e attenzione per la componente green: possiamo trovare in via di sviluppo anche servizi che sfruttano la collaborazione tra mezzi e territorio.

Per esempio, è possibile utilizzare i dati degli accelerometri di bordo accoppiandoli ai dati GPS del veicolo per eseguire una mappatura delle condizioni del manto stradale. I dati possono essere inviati direttamente dal mezzo a un ambiente cloud e validati da un sistema autonomo tramite l'incrocio dei dati provenienti da più mezzi.
Studi di questo tipo sul territorio sarebbero vantaggiosi sia per le PA, che potrebbero valutare interventi di manutenzione in base a esigenze e dati reali, sia per i mezzi, i cui il sistema di bordo conoscerebbe preventivamente le condizioni delle strade da percorrere. Ciò influenzerebbe il percorso suggerito dagli strumenti di navigazione del mezzo o addirittura il percorso stesso del mezzo, in casi di veicoli a guida autonoma.

Maggiore efficienza degli spostamenti

Un'altra possibilità offerta dal tracciamento di ogni mezzo presente sulle strade potrebbe essere il rendere più robusta la valutazione delle condizioni del traffico, che attualmente si basa su metodi indiretti (per esempio, il GPS degli smartphone dei singoli utenti). Oltre a informare l'utente delle condizioni attuali, lo storico dei dati potrebbe essere utilizzato per fare previsioni a breve termine e rendere ancora più intelligenti i sistemi di navigazione. I vantaggi sarebbero particolarmente di valore per il settore della logistica, oltre a presentare evidenti implicazioni per la sostenibilità ambientale degli spostamenti.

Le sfide del settore sono molte e complesse, ciononostante la ricerca in questo campo è molto attiva e sta producendo già risultati molto promettenti.
Grazie a tecnologie come la moderna sensoristica, la comunicazione e interconnessione di oggetti IoT e l'intelligenza artificiale, l'umanità si prefigge degli obiettivi che possiamo e dobbiamo raggiungere, per far compiere al settore automotive un salto generazionale con la potenzialità di portare alla riduzione delle emissioni, all'aumento della sicurezza stradale e all'agevolazione della mobilità in generale.

AUTORE: Alessio Giberti, ricercatore di MISTER Smart Innovation

oplium
CYBER FOR LIFE
A SPINDOX COMPANY

Focus: **Automotive**

Le sfide di cybersecurity nel settore automotive

Il settore automotive evolve da sempre a ritmo elevato, imponendo nuovi standard e alzando le aspettative di guidatori e passeggeri, prodotto dopo prodotto. Offrendo un'ampia serie di servizi sempre maggiori, come anche nuove possibilità di comunicazione e intrattenimento, il progresso del settore automotive sta creando un ecosistema complesso, fatto di sensori, controllo remoto, cloud computing, 5G e altre importanti tecnologie. Sotto questo punto di vista la cybersecurity dell'automotive sta diventando una sfida sempre più centrale per le case automobilistiche: per ogni innovazione offerta al cliente, infatti, ci sono nuove vulnerabilità da considerare, nuove vie di accesso per attività criminali. Di seguito verranno esposti in modo sintetico sfide e rischi della cybersecurity nel settore automotive.

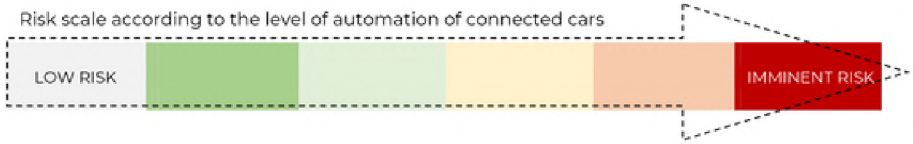
Verranno analizzate le norme ed i fattori chiave per un'implementazione sicura all'interno di questa industry e verranno dati alcuni suggerimenti per intraprendere azioni concrete lungo l'intera catena di fornitura nell'ecosistema automotive.

L'evoluzione del settore automotive

Quando si riflette sul futuro del settore automotive l'immaginario collettivo arriva inevitabilmente a pensare a una macchina autonoma al 100%, in grado di portarci ovunque senza bisogno di un conducente. Siamo ancora ben lontani dal livello 5 di automazione (o Automazione Completa, così come definita dalla SAE – Society of Automotive Engineers), raggiunto il quale il veicolo sarà in grado di funzionare autonomamente: senza bisogno di interfaccia umana, infatti, sarà in grado di muoversi su strade ed autostrade, correggendo eventuali inconvenienti mentre i passeggeri leggono, si connettono ai social network, bevono un caffè o, semplicemente, riposano.
L'avvento delle macchine autonome al 100% sarà necessariamente connesso allo sviluppo di altre tecnologie e innovazioni, quali le Smart Cities, il Cloud Computing, l'Internet of Things (IoT) e network 6G estesi, fattori necessari che permetteranno lo sviluppo di veicoli che non necessitano di alcuna interferenza umana. Tra gli altri requisiti del veicolo autonomo al 100% bisogna inoltre includere lo sviluppo infrastrutturale, come anche la risoluzione di quesiti normativi, di aspetti legali e di ottemperanza delle norme.

Barriere, queste, che nei paesi in via di sviluppo sono ancor più evidenti. Questo, tuttavia, non significa necessariamente un rallentamento nel progresso del settore automotive.
Al contrario, il suo avanzamento non è mai stato così rapido. I cambiamenti sono profondi, come i motori elettrici che sono sempre più presenti nelle offerte delle case automobilistiche, in risposta a preoccupazioni crescenti del pubblico in merito all'ambiente.
Nell'ultimo decennio il settore automotive ha visto anche l'introduzione di nuovi standard per andare incontro ad aspettative sempre maggiori da parte di conducenti e passeggeri. L'offerta vede già un ampio spettro di informazioni disponibili, maggiore comfort, funzioni di supporto al guidatore, sistemi di comunicazione e opzioni di intrattenimento, inclusi l'accesso ad internet, il monitoraggio da remoto tramite app, l'accesso a distanza alle informazioni e sistemi avanzati di assistenza. Questo progresso nel settore automotive sta creando un complesso ecosistema che comprende sensori, controllo a distanza, Cloud Computing, 5G e altre tecnologie rilevanti.

Sotto questo punto di vista la cybersecurity nel settore automotive è diventata una vera e propria sfida per le case automobilistiche, in quanto per ogni nuova funzione offerta al conducente, nuove vulnerabilità emergono, oltre a nuove opportunità per attività criminali.



0	1	2	3	4	5
NO AUTOMATION	**DRIVER ASSISTANCE**	**PARTIAL AUTOMATION**	**CONDITIONAL AUTOMATION**	**HIGH AUTOMATION**	**FULL AUTOMATION**
Level of most vehicles manufactured to date. Steering is 100% driver dependent	The system can help the driver with some simple activities, such as maintaining acceleration.	The system is capable of carrying out some vehicle functions on its own, such as accelerating and braking according to the limit set by the driver, using adaptive Cruise Control. It makes passive monitoring of the environment through sensors.	Vehicles that can move on their own both in the acceleration and steering part and in the active monitoring of the environment. Requires a more robust set of sensors such as laser scanners, ultrasonic sensors and radar systems	Virtually all activities will be done by the vehicle's autonomous system, including reactive skills in risky situations. But in certain situations, the driver has to take control of the vehicle	All controls and responsibility for driving being done by the vehicle's autonomous system. Sensor technology must be extremely advanced and connectivity has already become something organic in people's daily lives, possibly with 6G

Automation Levels, as defined by SAE International

Nel confronto tra l'analisi dei livelli di automazione e i livelli di rischio cibernetico introdotti dai veicoli autonomi è possibile supporre che un livello maggiore di rischio venga introdotto con l'aumentare delle opzioni che vengono rese disponibili per i conducenti. Più sensori si installano, più punti deboli si aprono per entità malevole.
Al crescere del volume di programmazione dietro a questi sistemi cresce anche la necessità della loro protezione. Più grandioso è lo scopo della connettività dei veicoli, maggiore è la superficie di attacco in un contesto estremamente competitivo quale il settore automotive, dove la mancanza di innovazione della customer experience semplicemente non è un'opzione.

Rischi cibernetici noti

Negli ultimi 10 anni, sono state effettuate diverse simulazioni di attacchi in molteplici case automobilistiche a livello globale.
In generale, questi test hanno rivelato come i veicoli connessi possano essere hackerati e quindi controllati da remoto.
Durante una di queste, nel 2013, mentre si trovava all'interno di un veicolo munito solo del proprio notebook, un hacker è riuscito a suonare il clacson, allacciarsi la cintura e muovere il volante. Due anni dopo, un altro hacker è riuscito a controllare da remoto un veicolo di un'altra casa automobilistica svolgendo alcune semplici azioni (es. cambiare la stazione della radio, attivare i tergicristalli e cambiare la temperatura dell'aria condizionata) come anche funzioni più pericolose quali mettere in folle il veicolo in movimento, disattivare i freni e accedere all'intera cronologia degli spostamenti del conducente (dato che il veicolo era dotato di navigazione satellitare).

Con lo sviluppo dell'internet mobile e l'arrivo di applicazioni smartphone in grado di controllare alcuni aspetti dell'automobile, le superfici di attacco sono ulteriormente aumentate. Una valutazione di Kaspersky Lab con oggetto 7 applicazioni da parte di importanti case produttrici ha evidenziato come tutte avessero diverse falle di sicurezza che avrebbero permesso ad hacker di prendere il controllo sulle App allo stesso livello del proprietario del veicolo ed eliminare i controlli di sicurezza fisici (allarme, blocco delle portiere) dei veicoli. Più recentemente, dei ricercatori del Concordia Institute for Information Systems Engineering hanno valutato 16 diversi fornitori di stazioni di ricarica elettrica, identificando vulnerabilità in ciascuno dei casi: a livello di firmware, nelle applicazioni mobile e nelle interfacce utilizzate per accedervi. Nessuno dei modelli testati era quindi immune da attacchi di hacking, e tutti potevano essere attaccati ed infettati da malware in grado di attivarli o disattivarli da remoto causando perdite personali, interruzioni di servizio o un sovraccarico delle reti locali fino al blackout. In uno studio recente, ricercatori della European Union Cybersecurity Agency (ENISA) stimano che, vista la dipendenza delle smart car nei confronti dello sviluppo di tecnologie di Machine Learning avanzato, il livello di rischio rappresentato da minacce cibernetiche non potrà far altro che aumentare.

7 tipi di rischio informatico nel settore automotive

Come accennato, gli attacchi informatici alle smart car possono portare ad un improvviso arresto del veicolo, causare incidenti stradali, perdite finanziarie, trasmissione dei dati sensibili del proprietario, episodi di manipolazione del sistema di intrattenimento.

Provando a raggruppare in classi le principali tipologie di rischio possiamo identificare:

- Spionaggio: le voci all'interno del veicolo vengono ascoltate attraverso un uso non corretto dello strumento di riconoscimento vocale.
- Furto di dati: furto dei dati relativi al proprietario del veicolo, come anche le informazioni di geolocalizzazione.
- Contenuti di intrattenimento: accesso ai sistemi di infotainment attraverso Bluetooth, USB o Wi-Fi.
- Alterazione dei sensori: accesso alle funzioni del veicolo attraverso le vulnerabilità presenti nei sensori installati.
- Controllo: presa di controllo su unità critiche di sicurezza del veicolo, quali controllo del motore e dei freni.
- Accesso fisico: accesso diretto a diagnostiche di bordo per la manipolazione dei dati del veicolo e altre caratteristiche del motore.
- Attacchi man-in-the-middle: Intercettazione dei pacchetti di upgrade del software installato sul veicolo attraverso upgrade online.

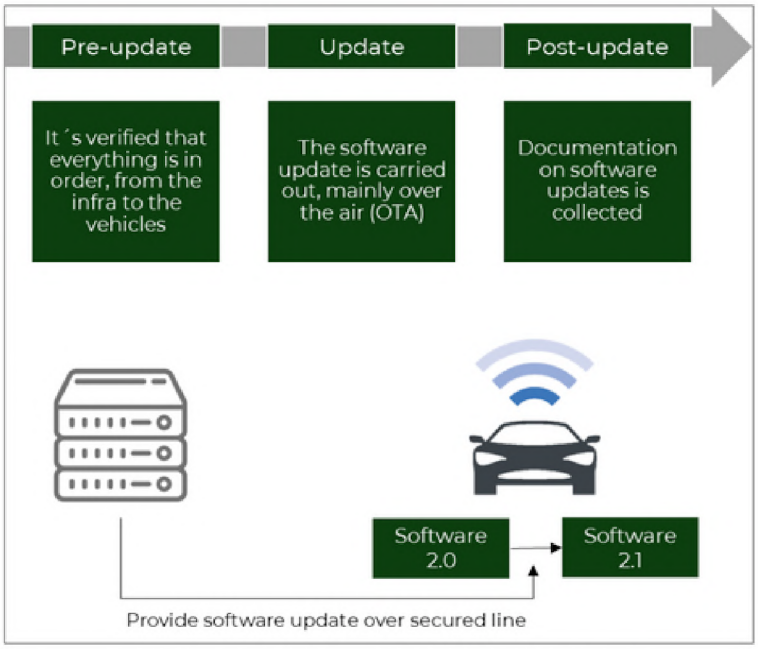
Standardizzare la cybersecurity nel settore automotive

Azioni isolate e indipendenti non sono sufficienti a proteggere i veicoli smart in maniera sicura ed efficace.
Al contrario, approcci sistematici e strategici sono necessari per coprire l'intera durata del ciclo di vita del prodotto e promuovere la sicurezza lungo tutta la supply chain dell'ecosistema automotive. Per stabilire dei requisiti per la cybersecurity automotive, quindi, l'Unione Europea ha stabilito uno standard attraverso due nuove norme:

UNECE R 155 e UNECE R 156.
La UNECE Cyber Security (UN R 155), che richiama direttamente il nuovo standard ISO/SAE 21434, si riferisce ai requisiti ingegneristici per la gestione del rischio informatico in termini di concetto, sviluppo del prodotto, operazione, mantenimento e smantellamento dei sistemi elettrici ed elettronici.
La UNECE Software Updating (UN R 156) riguarda invece gli aggiornamenti del software nei veicoli effettuati attraverso il metodo Over-the-air (OTA), ovvero tramite qualsiasi mezzo wireless al posto di connessioni cablate o di altro tipo. Questa norma introduce requisiti volti ad assicurare un processo di aggiornamento privo di rischi (ad esempio, premettendo l'aggiornamento solo a livelli di carica sufficienti) e procedure di annullamento in caso di fallimento dell'update, e simili.
Le due nuove norme cercano di indirizzare quattro aspetti principali dell'implementazione della cybersecurity:

- Gestione del rischio informatico del veicolo
- Protezione del veicolo attraverso il design (security by design) con lo scopo di mitigare i rischi lungo la supply chain
- Identificazione e risposta agli incidenti di sicurezza per tutta la flotta dei veicoli
- Fornire update sicuri e protetti, assicurando la sicurezza del veicolo.

Nell'Unione Europea, le nuove norme di cybersecurity diventeranno obbligatorie per tutti i nuovi tipi di veicoli a partire da luglio 2022 e per tutti i veicoli prodotti a partire da luglio 2024.



Software Update overview based UNECE R 156

Fattori chiave per la cybersecurity nel settore automotive

Come accennato, la UNECE R 155 definisce i requisiti necessari per la protezione dei veicoli e rappresenta un punto focale per l'implementazione dei Cyber Security Management Systems (CSMS) in tutte le case automobilistiche. Questa prerogativa cambia la prospettiva del business in quanto le loro attività di sviluppo non terminano più nell'inizio della produzione. Al contrario, c'è un obbligo continuativo di controllo dei sistemi di sicurezza per tutta la durata del ciclo di vita del veicolo, il che include anche miglioramenti alla supply chain e interessa anche il processo di update del software, secondo le specifiche della UNECE R 156.
Al fine di rispettare le norme e le sfide del settore, le case automobilistiche dovranno intraprendere azioni strategiche, rendendo la cybersecurity una parte integrante delle loro funzioni di business e dei loro sforzi di sviluppo.

Cambiamento di cultura:
le case automobilistiche hanno da sempre promosso la cultura della sicurezza – ma non ancora in termini di cybersecurity. Si devono quindi identificare le responsabilità in termini di cybersecurity relativamente ai punti focali delle attività di supply chain, e diffondere una cultura di security in tutti gli stakeholder coinvolti. Allo stesso tempo, anche i rivenditori dell'industria automotive sono chiamati a considerare i rischi di cybersecurity, dotandosi di capacità volte sia ad integrare le pratiche di sicurezza sia a collaborare in maniera efficace con i produttori per integrare e verificare soluzioni di cybersecurity end-to-end. Tutto ciò necessita la creazione di ambienti dove il software ha un'importanza centrale e caratterizzati da azioni continuative di training e awareness.

Valutazione e gestione dei rischi:
le case produttrici devono essere in grado di valutare e gestire i rischi dei sistemi automotive. Questo include identificare, valutare e gestire rischi di cybersecurity che potrebbero impattare i consumatori.
È inoltre necessario un piano di risposta per incidenti di sicurezza, con team aggiornati e allenati nella gestione dei diversi scenari di cui sopra.

Controlli di sicurezza:
le case automobilistiche devono implementare controlli di sicurezza per proteggere i veicoli da attacchi informatici. Tra questi sono inclusi processi di autenticazione, autorizzazione e criptazione. Questi controlli di sicurezza dovrebbero essere considerati finché i livelli di rischio non sono accettabili attraverso l'utilizzo di strategie di difesa profonde e separazione dei sistemi, in modo tale che, in caso di compromissione di parte del sistema (ad esempio la parte di intrattenimento), un eventuale intruso non riesca ad accedere sistemi critici (come il controllo remoto di accelerazione e frenata).

Security by Design:
la costruzione di veicoli automotive si basa un ciclo di sviluppo complesso, con una supply chain estesa che difficilmente permette modifiche a livello di design.

Perciò, le case automobilistiche devono tenere a mente la cybersecurity a tutti livelli del ciclo di vita del prodotto e non soltanto al momento della vendita al cliente. Infatti, nuove vulnerabilità tecniche possono emergere a qualsiasi stadio di sviluppo e queste problematiche possono avere un enorme impatto sui clienti e veicoli già messi in strada.

Supporto continuativo al prodotto: compagnie tech, come ad esempio case produttrici di smartphone, risolvono le questioni relative agli aggiornamenti attraverso il rilascio di nuove versioni dei loro software con correzioni di sicurezza per i loro prodotti che vanno oltre il momento della loro vendita iniziale. Tuttavia, questo processo si limita solitamente a un periodo limitato di anni mentre per quanto riguarda i veicoli la durata di vita del prodotto supera spesso il decennio e le case automobilistiche devono adattare gli update dei software per l'intero periodo. Fortunatamente grazie alle tecnologie OTA sarà possibile svolgere queste operazioni senza sprechi economici, al contrario delle pratiche correnti, che vedono l'obbligo da parte del proprietario del veicolo di riferirsi sempre al concessionario per tediose attività di riprogrammazione. L'industria automotive deve quindi sviluppare standard di cybersecurity condivisi, in modo da mantenere sotto controllo i costi di sviluppo e manutenzione.

Come aumentare la cybersecurity nel settore automotive

Le nuove norme e gli standard del settore automotive esposti in questo articolo forniscono vere e proprie linee guida che l'industria automotive dovrebbe seguire per aumentare la sicurezza informatica dei propri prodotti. In pratica, queste linee guida devono essere trasformate in pianificazioni strategiche continuative e comprensive.
Tra le diverse operazioni aziendali sottolineiamo l'importanza di strutturare in modo continuo attività di audit dei processi, valutazione della sicurezza tecnica, implementazione di controlli di sicurezza, formazione e consapevolezza, revisione del codice sorgente e intelligence del rischio informatico.

Valutazione dei processi di security e pre-audit

Questo step comprende azioni di controllo dei processi nel contesto di Cyber Security Management System (CSMS) e la verifica dei requisiti di cybersecurity attraverso precise checklist e applicando una metodologia simile ai processi standard di audit e certificazione. Nel valutare l'adesione ai requisiti della UNECE R 156, ad esempio, si devono tenere in considerazione controlli di configurazione volti a documentare le versioni hardware e software, i processi di aggiornamento automatico del software (in presenza di nuove versioni), i processi di verifica di compatibilità e i processi di comunicazioni con chi fruisce dei veicoli e così via.

DevSecOps

Rientrano in questo campo tutte le azioni di conformità e l'implementazione di buone pratiche di sicurezza in tutta la pipeline di sviluppo del software, tra cui la creazione e la valutazione dei requisiti di sicurezza, le attività di revisione statica e dinamica del codice utilizzando strumenti specializzati, i test di penetrazione, le vulnerabilità e l'implementazione di un framework di sviluppo sicuro e la modellazione delle minacce.

Training and Awareness

Si tratta di formare e diffondere la cultura della cybersecurity nel settore automobilistico, per garantire che le parti interessate possano mantenere la conformità normativa, compresi il team di sviluppo e l'architettura.

Le conoscenze che i dipendenti e le terze parti devono acquisire includono, ma non solo, i requisiti normativi (significato di ciascun requisito, prove richieste, approccio di audit/test, esempi di documentazione sufficiente/insufficiente).

Intelligence del rischio informatico

Questa categoria include l'anticipazione delle minacce con un approccio di tipo shift-left, che implica il monitoraggio continuativo di minacce informatiche e attività sospette in perimetri esterni alle industrie del settore automotive. Questo perché tali attività possono implicare rischi solitamente collegati alle pratiche di sfruttamento delle vulnerabilità, intrusioni, furto d'informazioni, intercettazione di comunicazioni, minacce a livello delle stazioni elettriche di rifornimento e attacchi di tipo denial-of-service nell'ecosistema automotive. Nel complesso, le organizzazioni possono considerare due possibili strade da percorrere per aumentare la cybersecurity nel settore automotive. La prima prevede l'esecuzione delle procedure in proprio, acquisendo sistemi, tecnologie e risorse umane per le varie azioni di conformità, che possono essere costose e complesse, poiché la cybersecurity non è l'attività principale di queste aziende e il settore presenta molte lacune storiche che non sono facilmente aggirabili. La seconda, invece, implica affidarsi a compagnie specializzate per lo sviluppo e l'implementazione di queste iniziative. Alcune società di consulenza hanno molta esperienza in questo tipo di valutazioni di rischio, con risultati significativi in un periodo di tempo relativamente breve.

Conclusione

Come visto, all'innalzamento dei livelli di connettività nei prodotti offerti dalle aziende del settore automotive tramite sensori smart, accesso remoto e miglioramento generale della customer experience, aumentano anche i requisiti relativi alla cybersecurity.
Le norme in vigore hanno lo scopo di standardizzare i requisiti di cybersecurity che devono essere rispettati dalle case automobilistiche e dai loro fornitori, introducendo tra l'altro processi di auditing e di compliance volti a verificare che la cybersecurity sia un valore osservato consistentemente lungo la linea di sviluppo veicoli e il loro ciclo di vita (security by design).
Per poter aumentare i livelli di cybersecurity nel settore automotive è necessario intraprendere numerose azioni strategiche, quali l'esecuzione di controlli di sicurezza, test di intrusione, analisi di vulnerabilità, formazione dei dipendenti e delle terze parti coinvolte nella supply chain. Le case automobilistiche sono chiamate quindi a riconoscere le loro responsabilità di cybersecurity nell'integralità del settore automotive, incoraggiano lo sviluppo di un ambiente che attribuisce centralità al software e che include approcci precauzionali in materia di rischi informatico.

AUTORI: George João de Almeida Chaves | Giuliano Rulli
OPLIUM DIGITAL SECURITY

Nuova era

Dio arriverà all'alba
se io sarò tra le tue braccia.

Accarezzami

Alda Merini (1931-2009)

Focus: **Automotive**

Secure by design: la rivoluzione cyber nell'automotive

Il 2022 è l'anno in cui la cybersecurity è entrata prepotentemente nell'industria automotive europea. Il motivo è l'attuazione del Regolamento Unece 155 che impone di introdurre misure di cybersecurity fin dalla fase di progettazione - da cui la definizione di "secure by design" - dei componenti elettronici che gestiscono un autoveicolo e che possono essere sensibili ad eventuali attacchi informatici.

L'industria dell'auto sta vivendo un profondo cambiamento dovuto alla digitalizzazione che sta trasformando i veicoli in un elemento sempre più fondamentale del complesso ecosistema della mobilità. La crescente connessione e lo scambio di informazioni tra l'auto e il mondo esterno hanno fatto aumentare la consapevolezza che la cybersecurity sia un elemento imprescindibile dello sviluppo di un prodotto sempre più digitale. Questa nuova consapevolezza e l'applicazione di quanto indicato dai Regolamenti e da Norme Tecniche come la ISO/SAE 21434:2021 (Road vehicles — Cybersecurity engineering) o la ISO 26262:2018 (Road Vehicles – Functional Safety) contribuiranno a sviluppare un prodotto sempre più sicuro ed affidabile.

Cosa cambia con l'introduzione del Regolamento Unece 155?

L'impatto del l'R155 è notevole in quanto impone di gestire gli aspetti della cybersecurity su tutto il ciclo di vita del veicolo, dalla fase dell'ideazione, proseguendo per tutto il periodo della produzione fino alla rottamazione. Altro aspetto importante introdotto dalla normativa è che la valutazione dei rischi e il costante monitoraggio non riguarda solo i costruttori ma tutta la supply chain. Infatti, la normativa richiede al costruttore automobilistico di tenere sotto controllo tutti i suoi fornitori nel rispetto dei requisiti di cybersecurity. Il processo di sviluppo di una vettura "secure by design" e il monitoraggio continuo dei rischi diventa quindi un concetto diffuso ed applicato a tutti gli attori della supply chain coinvolti nella fornitura.

Oltre la definizione dei rischi di cui tener conto nella fase di design, è necessario predisporre un sistema di sorveglianza attiva sui rischi e le vulnerabilità che dovessero manifestarsi sul prodotto in esercizio.

Il sistema gestione della cybersecurity

In base alla normativa di riferimento (Regolamento Unece 155, ISO 21434, ISO 26262) viene definito un framework che porta ad evidenziare gli obblighi per i costruttori e i loro fornitori rispetto ai requisiti minimi di cybersecurity da rispettare. Aspetto fondamentale è l'implementazione del Cybersecurity Management System (CSMS), che dovrà disciplinare la struttura organizzativa, le policy, i processi di valutazione dei rischi, il monitoraggio costante e la gestione degli eventi di cyber attack. Aspetto da non sottovalutare è che la valutazione dei rischi e la sua gestione, attraverso il CSMS, non possono occuparsi solo del veicolo ma riguarda la sicurezza dell'intero ecosistema e il back-end, formato dai server che gestiscono il veicolo, che permettono gli aggiornamenti OTA (Over-The-Air) e che gestiscono i sistemi utente per interagire con il veicolo.

Come valutare l'affidabilità dei sistemi di controllo di un'auto?

La rivoluzione cyber, come era facile immaginare, non può riguardare solo i processi: il secondo pilastro fondamentale consiste nel valutare quanto siano sicure le varie centraline che controllano i veicoli che guidiamo.

In questo caso, la normativa di riferimento, definisce delle classi di rischo che devono essere considerate e rispetto alle quali il veicolo deve essere protetto.
Ai costruttori e ai relativi fornitori è lasciata la liberta di definire tecniche e soluzioni da adottare per raggiungere l'obiettivo. Passaggio fondamentale e cruciale è quindi la valutazione del rischio, attraverso lo strumento del TARA (Threat Analysis and Risk Assesment), le cui metodologie sono definite negli standard SAE J3061, ISO 21434, oltre che nell'UNECE R155. L'analisi del rischio effettuta - che dovrà sempre essere aggiornata - accompagnerà tutto il ciclo del veicolo, fino alla demolizione e dovrà contenere la valutazione delle minacce più probabili al sistema, la valutazione dei danni possibili e della loro entità e le contro misure da adottare per mitigare i rischi. I parametri di security più rilevanti da tenere in conto sono la safety, l'operatività del veicolo, il danno finanziario e la privacy dell'utente, per salvaguardare i suoi dati.

Auto sempre più connesse: siamo consapevoli dei rischi?

Oggi i veicoli che interagiscono tra di loro per scambiarsi informazioni sul traffico (V2V – vehicle to vehicle), veicoli che comunicano con infrastrutture (V2I – vehicle to infrastructures) oppure veicoli che comunicano informazioni ad una qualsiasi entità che possa influenzarli (V2X – vehicle to everything) sono sempre più diffusi. Le tecnologie a disposizione permettono ad un veicolo di interagire con il mondo esterno per scambiare informazioni che riguardano dati personali o dati di funzionamento del veicolo, in quanto è possibile accedere all'interno del veicolo stesso.
All'interno di un autoveicolo sono presenti mediamente più di 100/140 centraline, totalmente aggiornabili da remoto, e comunicanti tra loro attraverso reti interne. Ci si trova quindi di fronte ad una superficie di attacco molto ampia, dove i fattori di rischio sono molteplici anche se poco percepiti dall'utente.

In un contesto di questo tipo la cybersecurity assume un aspetto fondamentale, non solo per la protezione del dato ma per la protezione del mezzo stesso e del suo corretto funzionamento. Il punto però è creare la giusta consapevolezza e quindi le giuste contromisure in termini di competenze e comportamenti.
È necessario quindi fare formazione per sensibilizzare e far conoscere gli strumenti a disposizione per prevenire i rischi.

L'impegno di Bureau Veritas Italia per la cybersecurity nell'Automotive

Forte della collaborazione tra le divisioni dedicate rispettivamente alla Cybersecurity e all'Automotive, Bureau Veritas è pronta a rispondere alle esigenze delle aziende del settore che devono allinearsi alle nuove disposizioni.

L'implementazione del Cybersecurity Management System è una fase molto importante, delicata ed impegnativa: il supporto di Bureau Veritas alle aziende consiste proprio nell'identificare il modo migliore in cui implementare il CSMS, nel rispetto dei requisti richiesti dalla normativa e nella forma che meglio si integra nella struttura organizzativa in cui il CSMS dovrà essere applicato ed operare.

L'offerta di servizi è ampia e integrata: dalla GAP Analysis ai pre audit, passando per tutte le fasi di verifica e analisi legate al CSMS, fino ad arrivare ai relativi test.
Bureau Veritas è riconosciuto come Technical service presso le Type Approval Authority e il supporto si estende a tutti gli ambiti direttamente legati alle norme ISO di riferimento (ISO 26262, ISO 21434), e a tutti gli aspetti disciplinati dai regolamenti R155 e R156.
Parallelamente, Bureau Veritas ha sviluppato un'ampia offerta di corsi di formazione basati sulle norme di riferimento come la ISO 21434 o il Regolamento Unece 155.
Tramite la formazione è possibile acquisire consapevolezza dei reali rischi e acquisire le basi per costruire modelli e sistemi di gestione della cybersecurity efficienti ed implementare valutazioni dei rischi efficaci.

AUTORI:
Alessandro Ferrari
Digital Transformation & Ind 4.0 –
Cybersecurity Products Line Manager
BUREAU VERITAS ITALIA

Simone Dore
Manager AUTOMOTIVE & MOBILITY
BUSINESS UNIT
BUREAU VERITAS ITALIA

Come Spindox testa la qualità di una connected car

La Business Unit di Software Quality Assurance è stata coinvolta in attività di verifica e validazione in ambito E2E per il servizio di auto connessa per un cliente del mercato Luxury Car.

Obiettivo del progetto:

I nuovi obiettivi delle aziende manifatturiere di automobili non sono più solo legati ad asset tradizionali come la sicurezza e le performance del veicolo. Quello che inizia ad avere un peso sempre maggiore nelle scelte dei clienti, è la disponibilità di tutti i servizi accessori che sono in grado di migliorare l'esperienza di guida. In quest'ottica, si parla sempre più di connected-car o veicoli connessi, ossia auto con a bordo un sistema di Infotainment, che comunica direttamente con l'app del cliente, attraverso dei sistemi di Internet Of Things, fornendo una experience unica al cliente, sia on-board sia off-board.
La BU di Software Quality Assurance di Spindox sta portando avanti un progetto a lungo termine per un cliente di Luxury Car, che include attività di analisi, verifica e validazione in ambito Connected-Car, seguendo ed eseguendo gli use-cases possibili tra il veicolo e l'app dell'utente finale, ma anche verifiche dell'architettura disegnata per la soluzione.
Oggetto dell'attività è quindi la verifica del corretto comportamento delle seguenti componenti, basandosi sulla definizione delle specifiche tecniche e funzionali:
- *Macchina, ossia il "core" dell'intero progetto.* Qui sono stati analizzati e verificati i seguenti protocolli:
a. CAN: È il protocollo utilizzato in ambito automotive, come standard, per far comunicare tra di loro i vari sensori dell'auto (ad esempio: un portiera aperta, non è altro che un messaggio con valore 0 oppure 1, relativo a quel particolare componente);

b. MQTT: Protocollo open source utilizzato in maniera massiva in ambito IoT (Internet-Of-Things), per trasmettere in maniera semplice, veloce e sicura, dati di piccole dimensioni da un certo dispositivo (in questo caso l'auto), verso un server; il messaggio CAN ricevuto veniva impacchettato e trasmesso tramite questo protocollo;

c. Reti Mobili: Utilizzando le reti telefoniche 2G/3G/4G/5G, ed utilizzando delle SIM/e-SIM, l'auto è sempre connessa alla rete Internet, e può trasmettere i dati MQTT al Server centrale (da ora in avanti, chiamato Back-End).

- *Back-End applicativo*, ossia tutto quello che non viene visto dall'utente finale, ma che permette il funzionamento corretto dell'eco-sistema Connected Car, dove sono stati analizzati e verificato il corretto comportamento dei protocolli:

d. API SOAP/REST: Architettura a micro-servizi per sistemi distribuiti e non centralizzati; in questo caso l'auto connessa, sfruttando questi servizi integrati, richiedere delle informazioni tramite delle REQUEST, e il Back-End, se rispetta i criteri di Sicurezza e Profilazione Utente, risponde con una RESPONSE, contenente i dati richiesti, sia in caso positivo, sia in caso negativo
e. Database SQL: I dati ricevuti dal veicolo in maniera continuativa e cadenzata vengono storicizzati in istanze diverse di database, pronti per essere utilizzati su richiesta di utenti finali, ma anche per ricerche di analisi interne, per il filone del mondo big data.

- *App Mobile*, ossia l'app cliente, utilizzata dall'utente finale, scaricata da App Store e Google Play per Android. L'app utilizzata e testata per i clienti finali è un'app nativa, quindi con sviluppi completamente slegati tra le due piattaforme iOS end Android.

Il cliente finale, quindi, avrà a disposizione un'auto connessa con la propria app, per poter gestire al meglio i servizi che ha acquistato.

Punti di forza:

L'utilizzo di vetture reali ha permesso di testare ancora una volta l'esperienza di Spindox in ambito IT al servizio del mondo Automotive.
Nel dettaglio, sono stati validati i seguenti sistemi:

- Veicolo
- Back-end Veicolo a microservizi
- Customer App
- CRM del cliente
- Amazon Alexa Auto
- Here OTA platform
- Vodafone M2M Platform

Attività di R&D&I svolte nel 2021

Informazioni preliminari:
-*Durata del progetto:* Attività di verifica e validazione è iniziata nel febbraio 2020. La fine è prevista per luglio 2024.

Le attività di R&D sono state le seguenti:

- *Test dei Gray Services*

Servizi che vengono attivati dall'app, e che informano l'utente nel caso di violazione del veicolo, se supera una certa soglia di velocità, se esce/entra in una zona geografica specificata dall'utente, la possibilità di verificare lo stato del veicolo (posizione, carburante, portiere/finestrini aperti, chilometri percorsi ed eventuali spie di allarme) e la strada da dover fare a piedi per raggiungere il veicolo parcheggiato.
Sono stati eseguiti circa 300 casi di test, che comprendono casistiche di perdita di connessione dati e/o perdita di segnale GPS, oltre che violazioni borderline sia come soglie di velocità che geografiche.

- *Test degli aggiornamenti del SW del veicolo*

Tramite la piattaforma OTA è possibile creare delle campagne di aggiornamento di tutti o di determinati veicoli, in modo da poter fare gli upgrade di nuove funzionalità sulle auto, senza bisogno di andare in concessionario.
Lato test sono state eseguite circa 50 casistiche di test, per verificare gli aggiornamenti tra diverse versioni software, oltre che di possibili problemi in fase di download dell'aggiornamento o di installazione.

- *Test di Alexa Auto integrato sul veicolo*

Amazon Alexa è stato integrato direttamente all'interno del veicolo, ed è quindi possibile non solo interagire con skills di Musica, Calendario e altro ma soprattutto con comandi dedicati sul veicolo, come interazioni con il clima, con i colori delle lampade interne, con le direzioni stradali nel navigatore integrato e le navigazioni tra i vari menu dell'infotainment.
Su questa integrazione sono stati realizzati circa 200 casi di test, sia sui vari MSP (Music Service Provider), come Amazon Music, Deezer, ecc), sia sulle utterances (ad es: "Alexa, aumenta aria condizionata"), sia sulle navigazioni, per le lingue italiano, inglese, francese, tedesco e spagnolo.

Inoltre, un'auto ha la nuova funzionalità di poter registrare, dalle due videocamere poste dentro il veicolo, una gara in un qualunque tipo di percorso o tracciato, e decidere di poterli rivedere direttamente sulla sua app e condividerli.
Su questa feature sono stati individuati ed eseguiti 70 casi di test, con problemi che possono risiedere nella creazione del video, problemi nell'upload del video, nell' inconsistenza tra i dati registrati dal veicolo e quelli post-prodotti e visualizzati sull'app.

Risultati

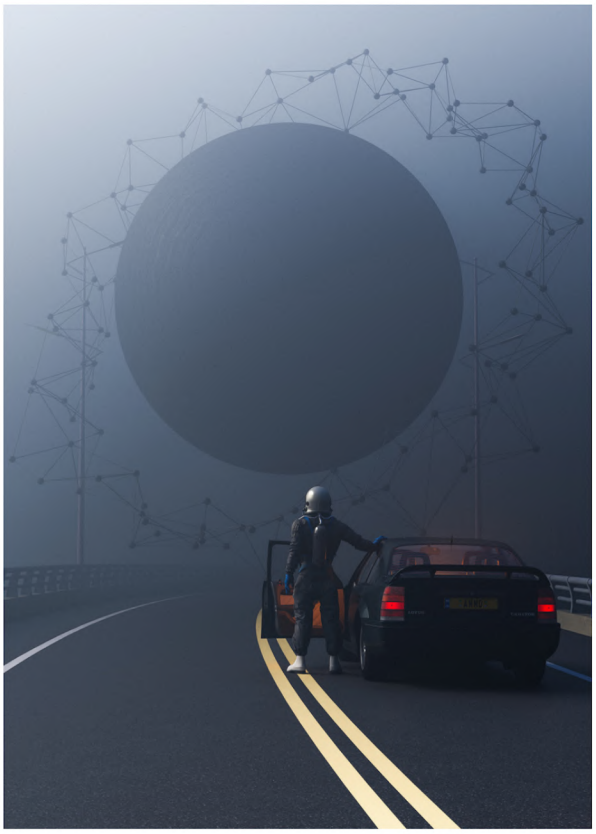
Le attività sono iniziate a febbraio 2020, e sono tutt'ora in corso; le azioni di analisi, definizione degli use case e loro successiva simulazione in tutti gli scenari previsti hanno portato all'individuazione di molteplici problemi di varia natura. La segnalazione e la conseguente risoluzione dei suddetti problemi hanno portato ad un delivery di altissima qualità del prodotto finale dal punto di vista delle prestazioni del sistema E2E complessivo: Veicolo – Back-End – App.

Vigilanza

Mi scompaio come l'oggetto
troppo a lungo guardato.

Patrizia Cavalli
(1931-2009)

ISTITUTO
DI INFORMATICA
E TELEMATICA



Focus: **Automotive**

L'importanza di studiare gli attacchi cyber e la normativa

L'importanza di considerare gli aspetti di cybersecurity all'interno delle nostre auto è diventata evidente a partire dal 2015, quando due ricercatori statunitensi, Miller e Valasek, per la prima volta hanno dato dimostrazione pratica di come un'auto, nel loro caso una Jeep Cherokee, potesse essere soggetta a questo tipo di problematiche proprie come un comune computer connesso ad Internet.

Questo problema può essere affrontato su fronti diversi. Da una parte c'è il lato offensivo dove vengono studiate le vulnerabilità e i punti deboli del sistema che abbiamo di fronte, provando di fatto degli attacchi all'auto.

Dall'altro lato, c'è la ricerca sul lato difensivo, dove sono sviluppate e implementate soluzioni affinché le nostre auto siano più sicure dal punto di vista cyber.

La ricerca offensiva

Essendo un dominio applicativo nuovo, così come spesso accade nella vita, per proteggersi al meglio occorre avere consapevolezza del pericolo e conoscerlo quanto più possibile. Proprio per questo, dal 2015, l'attività di ricerca "offensiva" ai fini di scovare vulnerabilità nelle auto, ha prodotto molti esempi di attacchi. Nel 2020, al CNR, abbiamo trovato una vulnerabilità all'interno di un sistema di infotainment proprietario che permetteva di accedere attraverso lo stesso ad alcune funzionalità del veicolo.
Una volta le auto erano composte solo da parti meccaniche, successivamente si sono evolute sempre più verso dei Cyber-Physical System, le cui componenti software interagiscono con la parte meccanica del veicolo e ne comandano le azioni. Nel 1982, Bosch ha introdotto il protocollo CAN bus come "mezzo di trasporto" delle informazioni fra centraline elettroniche diverse all'interno dell'auto. Le centraline inizialmente erano poche, pochissime, poi sono aumentate in numero e servono a regolare e gestire le funzionalità dell'auto come ad esempio i freni, i sensori interni e così via. Il CAN è stato subito adottato perché poco costoso e molto efficiente ma è totalmente privo di sicurezza: ad esempio, i messaggi non sono autenticati e passano in chiaro.

Ma questo non è un problema e nessuno aveva pensato che potesse esserlo perché nessuno si sarebbe mai aspettato che prima o poi le nostre auto sarebbero state connesse con il mondo attraverso Internet. Infatti, l'introduzione nell'auto di dispositivi di assistenza alla guida o di intrattenimento possono esporre vulnerabilità all'esterno, soprattutto quando l'auto viene connessa ad Internet.

La necessità di uno standard

Le auto, quindi, non sono state pensate secure-by-design, cioè non sono state progettate per essere sicure dal punto di vista informatico e come spesso accade, introdurre la sicurezza a posteriori non è detto che sia un'azione risolutiva ed a costo zero. Tuttavia, negli ultimi 10 anni, l'interesse dell'industria automobilistica alle problematiche di cybersecurity al fine di includere soluzioni di sicurezza nelle auto è andato crescendo. Questo, però, ha visto una particolare indipendenza dell'adottare misure di sicurezza in cui accadeva che ogni casa automobilistica implementava le proprie soluzioni. Da qui l'esigenza di definire delle linee guida che chiarissero i parametri da considerare per poter definire un'auto sicura o quantomeno un'auto progettata in modo sicuro. Finalmente, nell'agosto del 2021, è stata rilasciata la ISO/SAE21434 in cui tali linee guida sono state definite e saranno implementate entro il 2022 su tutte le auto di nuova produzione ed entro il 2024 su tutte le nuove versioni dei modelli esistenti permettendo quindi di avere auto "Secure-by-Design".

Così, la crescente domanda di uno standard comune e condiviso di cybersecurity ha portato nel 2016 l'International Organization for Standardization (ISO) e la Society of Automotive Engineers (SAE) a iniziare a lavorare allo standard ISO/SAE 21434, rilasciato nell'agosto 2021. la ISO/SAE21434 è il nuovo standard di cybersecurity per i sistemi Elettrici ed Elettronici (E/E) del veicolo e si combina al regolamento UNECE WP29 R155 dedicato anch'esso alla sicurezza dei veicoli.

Il settore automotive è altamente standardizzato, infatti diversi standard come ISO 9001, IATF 16949 o ISO 26262 sono già ampiamente applicati. In questo contesto, la ISO/SAE 21434 deve relazionarsi e affiancarsi con gli standard già esistenti, in particolare con le norme di qualità e protezione degli utenti. Per questo motivo, è indispensabile analizzare il rapporto tra ISO/SAE 21434 e le altre norme già esistenti. Ad esempio, è possibile notare la stretta correlazione tra ISO/SAE 21434 e ISO 26262, la norma dedicata alla safety degli utenti e dei veicoli. Queste ISO hanno elementi comuni che riguardano le regole per la condivisione delle informazioni raccolte dai veicoli e la necessità di una valutazione sulla qualità dei processi di protezione utilizzati.
La ISO/SAE 21434 è stata realizzata partendo anche da elementi solidi già definiti nella SAE J3061 e ISO/IEC 18045:2008. Dalla prima, vengono ereditati quegli elementi che fanno parte del processo continuo di gestione della cybersecurity e la richiesta di una cultura della sicurezza nell'ambiente di sviluppo dei componenti. Dalla seconda, la ISO/SAE 21434 eredita la definizione del rating di fattibilità dell'attacco e la definizione dell'approccio basato sul potenziale di attacco. Inoltre, la ISO/SAE 21434 integra dalla ISO/IEC/IEEE 15288:2015 gli aspetti utili per definire un quadro utili a descrivere il ciclo di vita di un sistema e che fornisce una definizione specifica di alcuni termini attraverso un glossario ben specifico.
La ISO/SAE 21434 è uno standard che ha richiesto un processo lungo di sviluppo che è durato per tanti anni. Dopo tutto questo tempo, lo standard ha dimostrato una certa maturità, completezza e si è ben inserito in un contesto altamente standardizzato.

In particolare, la ISO/SAE 21434 fornisce un processo composto da diverse fasi e documenti che coprono tutto il ciclo di vita di un componente dall'accordo tra cliente e fornitore fino alla dismissione. Tuttavia, ciò non vuol dire che lo standard ISO/SAE 21434 non è esente da alcuni possibili limiti che potrebbero essere migliorati. A tal proposito, lo standard non fornisce tecnologie, metodi o soluzioni da implementare per ottenere componenti sicuri e la compliance con lo standard. Da un lato, la ISO/SAE 21434 si vuole presentare ad un livello generico e lasciare il produttore libero di adottare le soluzioni migliori per ogni sistema. Dall'altro lato, questa mancanza può creare scenari in cui ogni azienda utilizza la propria soluzione proprietaria, dimostrata sicura ma su livelli diversi, creando possibili conflitti e diverse "qualità" di cybersicurezza. Per esempio, non avendo definito dei limiti all'interno della ISO/SAE 21434 riguardo le analisi del rischio, si potrebbero generare delle situazioni in cui componenti analoghi di diversi produttori hanno livelli di cybersecurity differenti, senza però che il cliente ne abbia percezione, perché entrambi conformi a ISO/SAE 21434. Così, potrebbe essere necessario definire ed integrare alcuni approcci specifici a seconda del dominio, per esempio telaio, powertrain o carrozzeria.

Cosa abbiamo capito?

L'introduzione della ISO/SAE 21434 ha indiscutibilmente dato una spinta importante al mondo automotive ad investire nella cybersecurity e soprattutto a pensare e concepire le nostre auto sicure fin dalla loro progettazione. Investire nella sicurezza-by-design è un passo necessario e decisivo al fine di garantire che la sicurezza sia adottata su tutti i veicoli in circolazione in maniera certificata e rispondente a linee guida dettate univocamente.
L'attività di offensive security diventerà parte integrante del ciclo di sviluppo dei veicoli e possibilmente non più un'attività fatta a posteriori che, se non condotta in modo responsabile, può portare enormi danni sia agli utenti che alle case costruttrici.
Finalmente, quindi, le problematiche di sicurezza nel dominio automotive sono diventate parte integrante del ciclo di vita delle nostre auto. Questo porterà nel prossimo futuro ad avere finalmente auto che non solo si guidano da sole ma che lo fanno in modo più cyber-sicuro.

AUTORI:
Gianpiero Costantino, Marco De Vincenzi, Ilaria Matteucci
Istituto di Informatica e Telematica del CNR di Pisa

Aspirazione

La vita non è una serie di lampioncini
disposti simmetricamente;
la vita è un alone luminoso.

Gita al faro (1927)

Virginia Woolf

Il marketing per le auto di lusso nasce già sulla catena di montaggio

Aggiornare periodicamente un acquirente nel settore automotive del lusso è il presupposto per una strategia di marketing il più possibile coinvolgente.
Centrali, in quest'ottica, sono i materiali fotografici che documentano l'avanzamento nell'assemblaggio dell'autovettura.

Strategie di marketing nel settore automotive del lusso

«A innescare cambiamenti e processi d'innovazione, il più delle volte, è l'esigenza di soddisfare, qui e ora, la richiesta di un cliente». È su questo aspetto che insiste Cristiano Carlevaro, Managing Director di Spindox Labs, nell'introdurci alla genesi di un progetto avviato e alimentatosi a più riprese tra le sedi di Trento e Maranello del gruppo Spindox.
Il cliente, in questo caso, è in attesa della sua auto nuova e scintillante. Il punto, però, è che i tempi di produzione previsti da un'azienda automotive del lusso sono diversi da quelli a cui siamo comunemente abituati, essendo diversa la cura riposta nei dettagli e nella personalizzazione del prodotto. È norma, dunque, che tra il momento dell'acquisto e quello della consegna in concessionaria intercorrano anche parecchi mesi. In tale lasso di tempo, tenere periodicamente aggiornato l'acquirente, renderlo in qualche misura partecipe rispetto al processo di produzione, rientra in una strategia di marketing concepita per essere il più possibile coinvolgente.

L'impiego di immagini dalla catena di montaggio per un approccio emozionale

Il percorso di avvicinamento al giorno della consegna è scandito da una comunicazione che il brand ritaglia attentamente sui suoi customer.
Prevale un approccio emozionale, con ricorso prevalente all'uso di immagini.
Il che spiega la rilevanza assunta dai materiali fotografici relativi allo stato di avanzamento nell'assemblaggio dell'autovettura.
La precisione nel documentare i passaggi, il ricorso ad accorgimenti tecnici nell'adempimento – anche normativo – delle suddette operazioni sono stati presi in carico da Spindox Labs.
Roberto Larcher in Spindox Labs è Technical Project Leader. Di fronte allo schermo del suo pc, mi guida lungo una catena di montaggio del settore automotive. L'esplorazione a distanza si avvale di un sistema di foto seriali degli ambienti di produzione. Il sistema, sviluppato in precedenza sempre da Spindox, è ora parte stessa del processo produttivo.
Lo spazio di lavoro è popolato da molteplici componenti tecnologiche, essendo in quegli ambienti che avviene il "confezionamento" definitivo del prodotto. Per questo, l'obiettivo è di "scremare" le foto scartando automaticamente quegli scatti che ritraggono dettagli superflui o di disturbo. Ad esempio, un cartello d'avviso lì a segnalare passaggi di lavorazione da ultimare.
Oppure operai al lavoro, che la legislazione in materia di privacy impedisce di ritrarre. E ancora, imperfezioni estetiche presenti nel telaio o nell'abitacolo di un'autovettura. Tutti fotogrammi che, se non passati a vaglio attento, rischierebbero di inficiare quell'immagine puntuale e precisa da restituire all'acquirente.

Un laboratorio ininterrotto di idee e soluzioni

Le tecnologie impiegate per i processi descritti, rientranti nell'ambito della Computer Vision, sono state approfondite da Spindox Labs a più riprese. È in tal senso MIMEX, il progetto europeo di Micro-Market Experience tuttora in via di sviluppo, a dover essere considerato il laboratorio più provvido. Qui sono stati approfonditi gli strumenti di People Identification per individuare la presenza di persone in spazi chiusi. Qui, con tecniche di Object Detection, si è giunti a rilevare la presa e il rilascio di oggetti attraverso software di visione ed elaborazione continua di fotogrammi. Stesso discorso per Pose Estimation, Image Processing e Defeat Detection, tecniche anch'esse impiegate nel progetto Car photo shooting, rientranti nel bagaglio di competenze accresciutosi con MIMEX e, quel che più conta, destinate a sviluppi ulteriori in altri contesti.

È infatti sugli scenari futuri per gli applicativi realizzati da Spindox Labs nel settore automotive del lusso che Carlevaro non manca d'insistere. Ad esempio, individuare per tempo situazioni di pericolo durante i processi di produzione come nel caso di dispositivi automatici di sicurezza sul lavoro. O, ancora, rilevare situazioni di emergenza o difetti lungo la catena di montaggio per consentire di correggere anomalie e imperfezioni prima che si arrivi a fine linea. Sono alcune delle evoluzioni immaginabili. Il filo conduttore è facile da rintracciare. Sta nella coerenza interna e nella forza d'innovazione della ricerca targata Spindox.

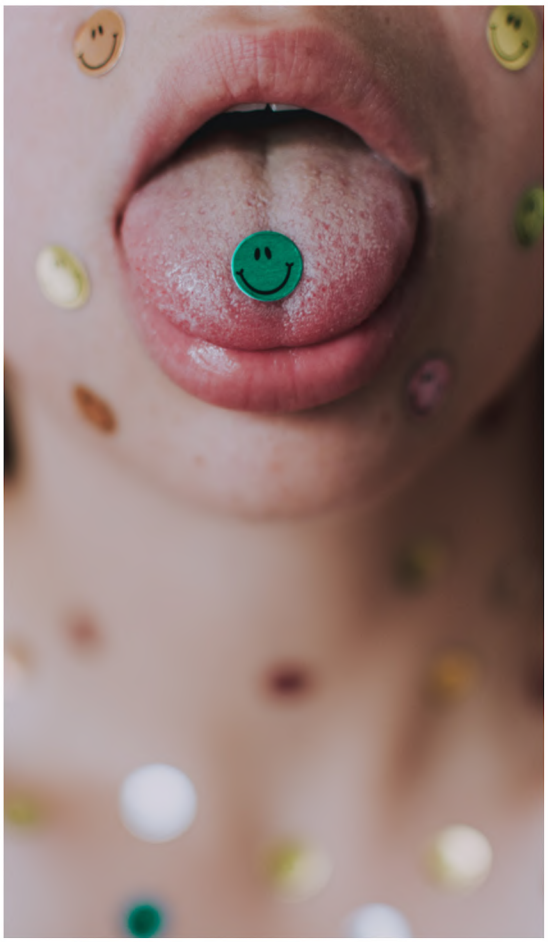
Pensiero laterale

Il mare d'inverno
È un concetto che il pensiero non considera
È poco moderno
È qualcosa che nessuno mai desidera.

Il mare d'inverno (1983)

Enrico Ruggeri

Connected health: se la sanità si fonde con l'Artificial Intelligence



L'industria farmaceutica italiana è ai primi posti in Europa per valore della produzione. A frenarla sono il peso della burocrazia e l'esiguità dei finanziamenti alla ricerca. Intanto anche il mondo del pharma e della salute incontra l'AI. Potrebbe essere l'inizio di un grande cambiamento.

La pandemia del Covid-19 ha enfatizzato il ruolo dell'industria farmaceutica e della ricerca biomedica per la gestione delle grandi crisi sanitarie. Il Pharma & Life Sciences Summit, organizzato il 4 luglio scorso dal Sole 24 Ore, ha offerto l'occasione per tracciare il quadro delle trasformazioni che interesseranno Pharma, Biotech e Life Sciences nei prossimi anni. Un mondo che vedrà un utilizzo crescente della telemedicina, dell'intelligenza artificiale, del machine learning, dei big data e della realtà virtuale. «Occuparsi di ricerca nel settore dell'industria farmaceutica è molto importante per il nostro paese» ricorda Fabio Tamburini, Direttore del Sole 24 Ore. «È necessario investire di più in questo settore perché in questo campo la strada da fare è ancora lunga. Infatti il nostro punto debole è quello della ricerca e dello sviluppo di nuovi prodotti. L'obiettivo è proprio quello di investire in questa fase.» Ed aggiunge il Ministro della Salute, Roberto Speranza: «la vera sfida dei prossimi mesi, oltre a quella del Covid-19, è quella di trasformare la più grande crisi che abbiamo vissuto negli ultimi decenni sul piano sanitario in una possibilità di ripartenza, in un'opportunità di rilancio del servizio sanitario nazionale e più in generale delle politiche della salute e della scienza della vita. Oggi c'è una consapevolezza, che non c'era prima del Covid-19, di quanto siano centrali e fondamentali le politiche della salute. È quindi necessario investire sulle risorse. Ma le risorse da sole non sono sufficienti. Sono anche necessarie politiche per la ricerca. Un'altra sfida da affrontare è quella di superare un modello storico di programmazione della spesa sanitaria basato su silos chiusi.»

L'industria farmaceutica in Italia

Quello dell'healthcare è un settore strategico, non solo per la salute degli italiani, ma anche per l'economia nel suo complesso. L'Italia è un paese che ha numeri importanti nel settore della farmaceutica e dell'innovazione delle nuove terapie: siamo tra i paesi leader nella produzione, raggiungendo un valore pari a 34 miliardi. Al contrario, secondo l'EFPIA il nostro paese non occupa una buona posizione per quanto riguarda le risorse investite nel settore della ricerca. Se ci confrontiamo con i maggiori paesi europei, scopriamo di essere molto indietro. L'Italia investe della ricerca farmaceutica solo 1,6 miliardi di euro, la Francia 5 miliardi, mentre la Germania arriva addirittura a 17. C'è poi il comparto Biotech. Nel nostro paese sono 376 le aziende che si occupano di biotecnologie applicate alla salute. Esse corrispondono al 48% del totale delle aziende biotech. Queste imprese rappresentano un'opportunità di crescita perché il mercato europeo investirà fino a 418 miliardi di euro entro il 2028.
«La ricerca e la produzione nel settore farmaceutico e biotech sono un asset strategico che i singoli paesi devono avere in agenda come priorità» ricorda Silvio Brusaferro, presidente dell'Istituto Superiore di Sanità. «La ricerca deve essere innovata attraverso due grandi pilastri. Il primo è quello della ricerca finalizzata, orientando le risorse per affrontare questa pandemia. Il secondo pilastro è quello della traslazione, ovvero fare in modo che ciò che emerge dalla ricerca, trovi spazio nel mondo produttivo

La pandemia del Covid-19 ha enfatizzato il ruolo dell'industria farmaceutica e della ricerca biomedica per la gestione delle grandi crisi sanitarie. Il Pharma & Life Sciences Summit, organizzato il 4 luglio scorso dal Sole 24 Ore, ha offerto l'occasione per tracciare il quadro delle trasformazioni che interesseranno Pharma, Biotech e Life Sciences nei prossimi anni. Un mondo che vedrà un utilizzo crescente della telemedicina, dell'intelligenza artificiale, del machine learning, dei big data e della realtà virtuale. «Occuparsi di ricerca nel settore dell'industria farmaceutica è molto importante per il nostro paese» ricorda Fabio Tamburini, Direttore del Sole 24 Ore. «È necessario investire di più in questo settore perché in questo campo la strada da fare è ancora lunga. Infatti il nostro punto debole è quello della ricerca e dello sviluppo di nuovi prodotti. L'obiettivo è proprio quello di investire in questa fase.» Ed aggiunge il Ministro della Salute, Roberto Speranza: «la vera sfida dei prossimi mesi, oltre a quella del Covid-19, è quella di trasformare la più grande crisi che abbiamo vissuto negli ultimi decenni sul piano sanitario in una possibilità di ripartenza, in un'opportunità di rilancio del servizio sanitario nazionale e più in generale delle politiche della salute e della scienza della vita. Oggi c'è una consapevolezza, che non c'era prima del Covid-19, di quanto siano centrali e fondamentali le politiche della salute. È quindi necessario investire sulle risorse. Ma le risorse da sole non sono sufficienti. Sono anche necessarie politiche per la ricerca. Un'altra sfida da affrontare è quella di superare un modello storico di programmazione della spesa sanitaria basato su silos chiusi.»

L'industria farmaceutica in Italia

Quello dell'healthcare è un settore strategico, non solo per la salute degli italiani, ma anche per l'economia nel suo complesso. L'Italia è un paese che ha numeri importanti nel settore della farmaceutica e dell'innovazione delle nuove terapie: siamo tra i paesi leader nella produzione, raggiungendo un valore pari a 34 miliardi. Al contrario, secondo l'EFPIA il nostro paese non occupa una buona posizione per quanto riguarda le risorse investite nel settore della ricerca. Se ci confrontiamo con i maggiori paesi europei, scopriamo di essere molto indietro. L'Italia investe della ricerca farmaceutica solo 1,6 miliardi di euro, la Francia 5 miliardi, mentre la Germania arriva addirittura a 17. C'è poi il comparto Biotech. Nel nostro paese sono 376 le aziende che si occupano di biotecnologie applicate alla salute. Esse corrispondono al 48% del totale delle aziende biotech. Queste imprese rappresentano un'opportunità di crescita perché il mercato europeo investirà fino a 418 miliardi di euro entro il 2028. «La ricerca e la produzione nel settore farmaceutico e biotech sono un asset strategico che i singoli paesi devono avere in agenda come priorità» ricorda Silvio Brusaferro, presidente dell'Istituto Superiore di Sanità. «La ricerca deve essere innovata attraverso due grandi pilastri. Il primo è quello della ricerca finalizzata, orientando le risorse per affrontare questa pandemia. Il secondo pilastro è quello della traslazione, ovvero fare in modo che ciò che emerge dalla ricerca, trovi spazio nel mondo produttivo in tempi rapidi e con

una scala adeguata alle esigenze di mercato. Il mondo farmaceutico è un ecosistema in cui sono presenti quasi tutti gli attori. Il problema è l'interconnessione tra questi attori e la regolazione dei flussi tra questi. Bisogna creare, quindi, una rete, una struttura che determini sia tempi che modi per comunicare».

I limiti burocratici in Italia

Il Covid-19 ci ha permesso di constatare come la collaborazione tra pubblico e privato sia stata di successo nel superare tante barriere, soprattutto burocratiche, che rendono l'ambiente sfavorevole alla ricerca e all'innovazione. Gli ostacoli che le aziende incontrano sono soprattutto di tipo burocratico oltre che economico. Ed è proprio a causa di questi ostacoli che l'Italia non riesce ad attrarre sufficienti risorse. Ecco perché, mentre nel campo della produzione abbiamo un mercato vivace, nella ricerca siamo indietro. Un chiaro esempio dei limiti che la burocrazia pone alle aziende riguarda l'implementazione del regolamento europeo sulle sperimentazioni cliniche che è in ritardo nella sua applicazione. Il regolamento è stato introdotto nel 2018. Con la Legge Lorenzin sono stati messi a disposizione 12 mesi per poter implementate tutti i decreti attuativi. Ma questo decreto non è ancora entrato in vigore.

Parola d'ordine per il decollo dell'industria farmaceutica

«L'industria farmaceutica avrebbe bisogno di regole stabili che consentano di essere più veloci e al passo con gli altri paesi» osserva Massimo Scaccabarozzi, Presidente di Farmindustria. «I decreti non vengono adottati rapidamente mentre i comitati etici sono stati ridotti, ma sono ancora tanti».

La consapevolezza è fondamentale nel settore farmaceutico. Soprattutto la consapevolezza di far parte di un ecosistema. E la consapevolezza che ciascun attore coinvolto all'interno di questo ecosistema abbia un ruolo che deve rispettare e gestire in maniera proattiva. Inoltre è fondamentale il sistema di valutazione. Perché solo valutando sistematicamente si possono valorizzare tutte le fasi del processo, dalla ricerca al paziente.
Ed infine, fare squadra. Lavorare in partnership tra pubblico e privato per poter fare in modo che i risultati si raggiungano più velocemente. Un esempio di questa collaborazione è il progetto IMI DRIVE, che ha come obiettivo accelerare lo sviluppo di farmaci più efficaci e sicuri per i pazienti.

Industria farmaceutica e salute: tutto interconnesso

Il futuro della salute è connesso. Le nuove tecnologie ci stanno permettendo in ogni ambito di accorciare le distanze. Questo implica nuovi modi di muoverci, di acquistare, di curarci e addirittura di vivere. All'interno di questo contesto che cosa definiamo come connected health? Si parla di connected health quando le cure incontrano il digitale, quando l'introduzione di software e della tecnologia possono stabilire progressi e risultati misurabili in termini di salute.
Le ricerche di mercato suggeriscono che nei prossimi tre anni 652 milioni di consumatori nel mondo utilizzeranno una terapia digitale. L'aspirazione è ottenere migliori risultati in termini di salute e una migliore qualità delle cure sta portando il segmento della connected health ad una crescita esponenziale. Oggi il mercato globale vale oltre 216 miliardi di dollari. Ma è previsto che raggiungerà un triliardo e mezzo entro il 2030. Si prevede inoltre che i segmenti dei dispositivi medici connessi e della telemedicina siano quelli che crescono di più e più velocemente. Ecco alcuni dati forniti da Andrea Russo, Energy, Industry & Life Sciences Division Director presso Capgemini: «da una nostra ricerca condotta a livello globale, compresa l'Italia, su 500 executive di aziende farm e biotech, l'84% degli intervistati ha dichiarato che l'opportunità di business della connected health supererà di molto quella del tradizionale business del farmaco. Ed in media il 13% del fatturato totale sarà derivato da prodotti connessi nei prossimi 5 anni. Tuttavia le aziende che intraprenderanno questo percorso dovranno gestire una trasformazione. Questo significherà ridefinire l'intera esperienza del paziente, andando oltre il farmaco. Costruendo così un programma che coinvolga tutti gli stakeholder interni ed esterni all'organizzazione. Tra le sfide maggiori che queste aziende si troveranno ad affrontare ci sono la sicurezza dei dati, l'introduzione di nuove tecnologie digitali e al tempo stesso l'incremento di competenze digitali all'interno delle organizzazioni».

Il sistema sanitario del futuro

Oggi c'è la volonta nazionale, attraverso gli investimenti di digitale, di creare

un'infrastruttura e far arrivare il digitale a casa di ciascuno di noi. L'inclusione infatti è uno dei temi fondamentali. Perché, se il digitale divide, perde la sua efficacia.
L'ospedale del futuro è diverso da come viene concepita oggi un'infrastruttura sanitaria. Per questo motivo è necessario rivedere l'organizzazione al suo interno per accogliere il paziente digitale. È necessario rivedere i percorsi di cura inserendo il digitale all'interno di essi, non considerandoli come un'alternativa.
L'analisi svolta dall'Osservatorio del Politecnico di Milano afferma che nel 2021 l'utilizzo della telemedicina è diminuito rispetto al 2020. Questo dimostra che se la telemedicina viene considerata un'alternativa alla visita in presenza è destinata a non crescere. Se invece si considera la telemedicina in tutti i suoi aspetti all'interno di un percorso di cura, allora sarà anche un modo per risolvere il problema della sostenibilità del sistema sanitario.
Attualmente l'incidenza del fondo sanitario sul PIL non cresce. Anzi, al contrario, sarà a livelli più bassi rispetto all'anno precedente per un valore di 6,4%. Quindi da un lato c'è un problema relativo alla scarsità delle risorse dedicate alla gestione, dall'altro c'è una mancanza di risorse umane.
Un'indicazione chiave del PNRR riguarda il fascicolo sanitario. Questo strumento non sarà più considerato una repository o un archivio di referti. Al contrario, diventa un sistema di connected care, ovvero un sistema interattivo fra pazienti, ospedali e territorio. In questo contesto il paziente deve avere un suo ruolo. Deve quindi essere un paziente competente. Da qui nasce il tema di come preparare il paziente a questa trasformazione digitale.

Lami: nuove modalità per nuovi medici di base

Lami è una start up nata nel 2020 con l'obiettivo di aiutare le persone a prendere le decisioni giuste per la loro salute, facilitando l'interpretazione dei sintomi e l'interazione con il medico.
Tre dati importanti che sono alla base di Lami. Si prevede che nei prossimi 5 anni in Italia ci saranno 30.000 medici di base in meno, su una base di 45.000 attuali. Il 60-70% di accessi al pronto soccorso sono codice bianco e verde. Si tratta quindi di situazioni che non richiederebbero alcun tipo di emergenza. Ed infine l'Italia è un paese in cui gli italiani consultano Internet, più precisamente Google, quattro miliardi di volte in un anno per questioni relative alla salute. E questo dato ha un tasso di crescita del 15% anno.

Lami & l'AI

Quindi come funziona Lami? Lo spiega Davide Barenghi, Founder & CEO della start up. «La persona immette il sintomo che sta riscontrando, vengono analizzati la presenza di eventuali fattori di rischio, patologie croniche e chiaramente la situazione concreta in cui la persona si trova. Viene quindi indicata la patologia alla base del sintomo che il paziente sta riscontrando. Successivamente Lami indica il percorso di cura più adatto – se è necessario andare al pronto soccorso o semplicemente consultare un medico di base –. Ed infine suggerisce in che modo quel paziente può interagire con il servizio sanitario- visita in presenza o televisita.»

L'obiettivo della start up è automatizzare l'indirizzamento del paziente nel percorso di cura più adeguato ovviamente a beneficio del paziente ma a beneficio anche dell'iter del sistema. Accorciando i tempi di diagnosi si accorciano i tempi della presa in carico. Si crea un beneficio sia per il sistema pubblico privato che per il paziente. L'obiettivo quindi non è quello di distinguere tra due patologie prossime ma rispondere alla domanda " Devo preoccuparmi? Cosa devo fare?" attraverso l'interazione macchina medico.
Attualmente un medico di base artificiale non è ancora come un medico di base tradizionale, ma quella è l'ambizione.

Gamification

Panem et circenses

Giovenale (Satire X, 81)

Accessibilità e inclusione: quando le scorciatoie fanno più male che bene

L'accessibilità del web è un tema antico quasi come l'origine del digitale, ma spesso dimenticato in fase di sviluppo. La soluzione non è scegliere la via più breve, ma quella più giusta.

Era l'ottobre 1994 quando il padre del web, Tim Berners-Lee, menzionò per la prima volta il concetto di accessibilità web. Siamo alla International World Wide Web Conference a Chicago, la seconda di una serie di conferenze che ancora oggi si tengono a cadenza più o meno annuale e che hanno l'obiettivo di discutere le direzioni future del World Wide Web.

L'accessibilità si è da subito presentata come una componente naturale del web, una prerogativa di sviluppo più che un optional da inseguire in un secondo momento. Nella visione di Berners-Lee (una citazione, questa, del '97): il potere del Web sta nella sua universalità. L'accesso per tutti, indipendentemente da disabilità, è un aspetto essenziale. Sempre nel 1997, il World Wide Web Consortium (W3C, ancora oggi l'organizzazione che fa da spina dorsale dello sviluppo del web) lancia ufficialmente la WAI o Web Accessibility Initiative, progetto specificamente dedicato ad abbattere le barriere di accesso al web da parte di persone diversamente abili, promuovendo design, strumenti e linee guida per siti web più inclusivi.
Fin dai suoi albori, quindi, il web è stato inteso come uno strumento che, a parte essere egalitario e indipendente da aspetti quali posizione, lingua o supporti (software e hardware), è anche in grado di funzionare ed essere alla portata di tutti, indipendentemente dal livello di abilità cognitiva, uditiva, visiva e motoria.

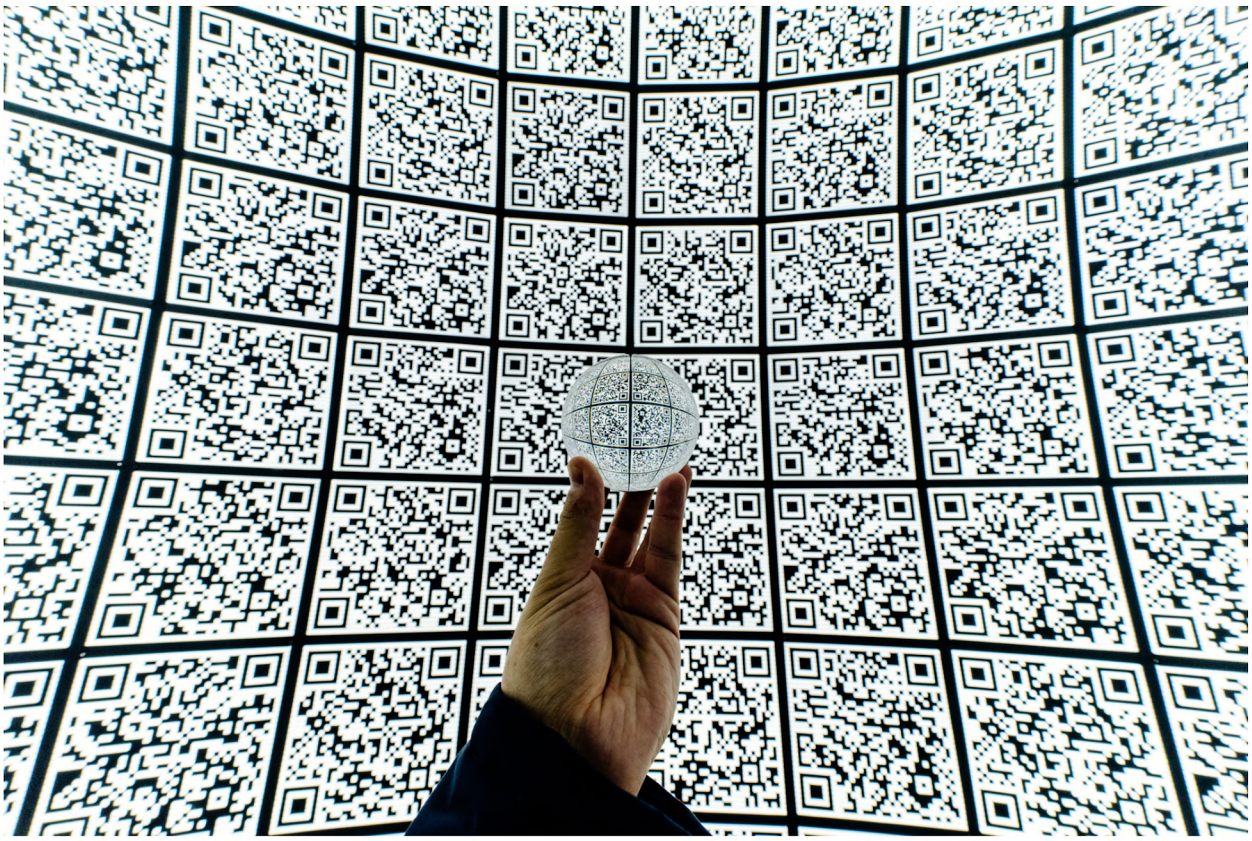
Siti più belli per tutti: l'accessibilità non è un optional

Ma allora perché, dopo oltre un quarto di secolo, lo sviluppo del web non è andato a passo con l'implementazione della sua accessibilità? Ancora oggi, è difficilissimo trovare siti accessibili come solo testo.

A febbraio 2022, un'idea dell'entità di questo problema ce l'ha fornita WebAIM, associazione senza scopo di lucro che opera dal 1999 per rendere i siti web più accessibili. Anche quest'anno WebAIM ha condotto uno studio, The WebAIM Million, volto a valutare l'accessibilità delle home page di 1 milione di siti web attraverso il loro tool proprietario, Wave. Dall'analisi è emerso che il 96.8% delle homepage presenta errori di accessibilità, con una media di 50.8 errori per pagina. Dati impressionanti, se si pensa che la selezione delle homepage oggetto di studio è la combinazione di tre autorevoli ranking di popolarità. Dati pericolosi, se si considera che la pandemia, enorme catalizzatore della trasformazione digitale a livello globale, ha portato a un miglioramento di 1 solo punto percentuale (nel 2019, le homepage con errori costituivano circa il 97.8% del campione). Ancora una volta, assistiamo a un trend di sviluppo che va in direzione opposta rispetto all'inclusività e che non potrebbe essere più lontano dall'utopia immaginata dai padri fondatori del web. Un'evoluzione che polarizza, perché viene offerto sempre di più e sempre il meglio a chi il di più e il di meglio ce l'ha già. Così facendo, si lasciano indietro pubblici nascosti. La lettura di questi dati ci dice che forse si sta prediligendo componente estetica (la grafica che stupisce e gli effetti che ammaliano) rispetto ad un sito accessibile, che offre la stessa quantità di informazioni ad ogni tipo di pubblico.

Accessibilità e PA: da problema a discriminazione

Ma c'è di più. I problemi di inclusività non riguardano soltanto siti d'informazione, homepage corporate o marketplace. Riguardano anche la pubblica amministrazione, dove il problema si fa ancor più serio. Con la digitalizzazione post-pandemica di molte procedure, la mancanza di un'implementazione accessibile di queste ultime è una vera e propria discriminazione e un'inottemperanza della legge.
I primi provvedimenti in termini di accessibilità sono stati introdotti dalla legge Stanca nel 2004, e ancora oggi ci sono problemi quali valori di contrasto troppo bassi o moduli in pdf illeggibili per non-vedenti, per citarne solo alcuni, che non permettono a persone con disabilità visive e non solo di accedere a procedure altresì disponibili al resto della popolazione.
Dati i 18 anni di tempo e l'accelerazione incrementale dell'ultimo periodo, forse, siamo autorizzati a parlare di una violazione della carta dei diritti fondamentale dell'unione Europea. L'articolo 21 del titolo III, sulla non discriminazione, ci dice infatti che: "è vietata qualsiasi forma di discriminazione fondata, in particolare, sul sesso, la razza, il colore della pelle o l'origine etnica o sociale, le caratteristiche genetiche, la lingua, la religione o le convenzioni personali, le opinioni politiche o di qualsiasi altra natura, l'appartenenza ad una minoranza nazionale, il patrimonio, la nascita, la disabilità, l'età o l'orientamento sessuale.



I falsi amici dell'accessibilità web

L'obbligo di accessibilità non riguarda soltanto le PA. Con il dl. 76/2020, anche le aziende che negli ultimi 3 anni hanno avuto un fatturato medio superiore a 500 milioni di euro sono chiamate ad adeguarsi. L'AgID, Agenzia per l'Italia Digitale, ha quindi esteso anche a queste entità le linee guida sull'accessibilità degli strumenti informatici. Ovviamente, con un aumento di domanda (di accessibilità), aumenta anche l'offerta di soluzioni. Negli ultimi anni, una serie di tool è salita alla ribalta, offrendo soluzioni a basso prezzo che, sulla carta, permettono alle aziende di correre ai ripari. Sulla carta, perché la realtà dei fatti è ben diversa: questi tool, infatti, oltre a non risolvere il problema, spesso lo aggravano. Lo spiega bene Roberto Scano, professionista italiano nel campo di accessibilità (e non solo). In sintesi, questi strumenti aggiungono un ulteriore livello di codice a un determinato sito web, cercando di tradurre il contenuto non accessibile in accessibile. Se il principio potrebbe anche funzionare, a livello concreto si arriva a creare un sito parallelo rispetto a quello originale, il cui contributo verso l'accessibilità è minimo. Il più delle volte, infatti, ci si concentra su problematiche che vengono già risolte da dispositivi hardware e software di cui una persona diversamente abile si è già dotata autonomamente. Questi dispositivi di risoluzione automatica possono perfino complicare la situazione e diminuire il livello di accessibilità, proprio perché si tratta di processi automatizzati. Infatti, non essendo dotati della criticità tipica dell'elemento umano, gli errori di interpretazione da parte di questi strumenti sono tanti e spesso invalidanti.
Come spiega l'autore, questi tool:

- Non risolvono i problemi di accessibilità strutturale e di contenuti;
- Non attuano modifiche a livello tecnico-organizzativo per la disposizione di contenuti accessibili;
- Non sono conformi alla normativa vigente, che indica l'obbligo di un sito nativamente accessibile.

Per gli attori che sono interessati ad ottenere un'accessibilità vera ed efficace è sconsigliata l'adozione di questi strumenti, che purtroppo sono simili all'applicazione di un cerotto su un braccio rotto. Una soluzione inadatta, inefficace e alla lunga controproducente.

Accessibilità: un problema di sostenibilità sociale

La verità è che l'accessibilità sembra difficile da risolvere solo perché non la si guarda con la lente giusta. La si considera un obbligo, un adempimento di legge insidioso e difficile, che porta inevitabilmente alla ricerca di scorciatoie.
E se considerassimo l'accessibilità una questione di sostenibilità sociale?
Come un impegno serio per l'inclusione e la rappresentazione?
Allora sì che si potrebbe intendere la tecnologia nel modo giusto: una trasformazione che supporta l'uomo nel raggiungere il livello successivo, senza lasciare indietro nessuno. Non uno strumento in grado di funzionare e auto-risolversi senza supervisione.

La soluzione per siti e contenuti davvero accessibili è quella di aprire il design alla questione dell'accessibilità. Fare scuola, a tutte le fasi del progetto e per tutte le persone coinvolte, affinché si propaghi una cultura di inclusività. In questo modo, anche decisioni a livello operativo saranno prive di bias che discriminano i diversamente abili, e i prodotti finali saranno puliti, inclusivi, ponderati. Promuovere la formazione degli attori coinvolti, senza limitarsi a istituire esperti di accessibilità che supervisionano il progetto, è un investimento che non può non tornare utile anche a livello di business. Perché nel medio e lungo termine, le linee guida menzionate in questo articolo saranno applicate in maniera sistematica. Una formazione di questo tipo eviterà al business del domani di dover ricorrere a soluzioni palliative e scorciatoie controproducenti.

Percepire l'accessibilità in termini di sostenibilità sociale è quindi la decisione più responsabile, quella che serve per dare un messaggio chiaro e serio: questo prodotto è per tutti, questo prodotto è stato pensato per tutti, in tutte le sue fasi, in ogni suo momento.

Macchine elettriche e Fit-for-55: l'orizzonte del cambiamento sostenibile

Dal 2035, non potremo più comprare veicoli a combustione interna. È la spinta di cui avevamo bisogno.

La questione del cambiamento climatico è ormai ben nota alla società globale. L'innalzamento dei livelli dei mari, lo sbiancamento dei coralli e la conseguente morte lenta delle barriere coralline, gli incendi colossali, le innumerevoli specie animali in via di estinzione, i disastri naturali e gli episodi climatici sempre più violenti sono esempi purtroppo lampanti di come l'innalzamento delle temperature causato dall'uomo stia mettendo in pericolo il futuro dell'intero pianeta (e quindi anche della specie umana).

Il dibattito climatico non è mai stato così acceso, così veemente e talvolta (sfortunatamente) violento. Specialmente dopo la pandemia, abbiamo assistito a un momento epifanico della società globale, dove ci siamo accorti che la finestra di azione per poter invertire il processo distruttivo si sta restringendo molto velocemente. Ascoltando il parere di attivisti, scienziati, esperti e appassionati, la realtà è una. I prossimi dieci anni saranno anni di make or break, dove l'umanità tutta è chiamata a cambiare la rotta.

Sulla scia di questo risveglio, l'Europa si è imposta l'obiettivo sfidante di raggiungere la neutralità entro il 2050. In altre parole, dedicare la prossima trentina d'anni alla rivoluzione ecologica che interesserà tutte le aree produttive (economia, trasporti, energia, ecc.). L'obiettivo è di eliminare/compensare le emissioni e trasformare il vecchio continente nel primo al mondo ad azzerare il proprio impatto su ambiente e clima.

Nasce così il Green Deal Europeo e l'iniziativa Fit-for-55, che mettono su carta questi buoni propositi traducendoli in obblighi legislativi e finanziamenti che accompagneranno il cambiamento. Se il Green Deal si riferisce alla neutralità ambientale/climatica da raggiungere entro il 2050, il Fit-for-55 si concentra su un obiettivo nel medio termine, ma altrettanto importante: ridurre le emissioni del 55% entro il 2035. Un passo intermedio, ma fondamentale per rendere gli obiettivi nel lungo termine raggiungibili.

Fit-for-55 e macchina elettrica: la soluzione per il tallone d'Achille climatico

In questo contesto, il settore dei trasporti non poteva rimanere escluso. D'altra parte, si tratta di un settore che produce ben 20% delle emissioni a livello globale, rendendolo una delle componenti più influenti e dolorose quando si parla di cambiamento climatico. Alla luce di questa consapevolezza, il programma fit-for-55 colpisce il settore dei trasporti con molta decisione e poca pietà. Sono infatti innumerevoli i cambiamenti introdotti nel settore dei trasporti. Dal trasporto marittimo a quello aereo, dall'efficientamento energetico ai combustibili alternativi, l'impegno dell'Unione Europea supera le aspettative, sorprendendo per la qualità dei suoi intenti e obiettivi.

Macro-cambiamenti che andranno ad influenzare anche il livello micro, legato alla nostra vita quotidiana. Ne è un esempio il caso della macchina elettrica, che si andrà a sostituire progressivamente ai veicoli a combustione interna nel corso del prossimo decennio. Se una vasta gamma di case automobilistiche si trova d'accordo sul traslare la produzione verso i soli veicoli elettrici entro il 2030, dal 2035 non sarà più possibile acquistare veicoli a combustione interna.

Se la notizia potrebbe inizialmente spaventare, basta addentrarsi nell'analisi dell'enorme serie di benefici che derivano da questa transizione per capire che, in realtà, questo cambiamento forzato sarà una ventata d'aria fresca, per noi e per l'ambiente.

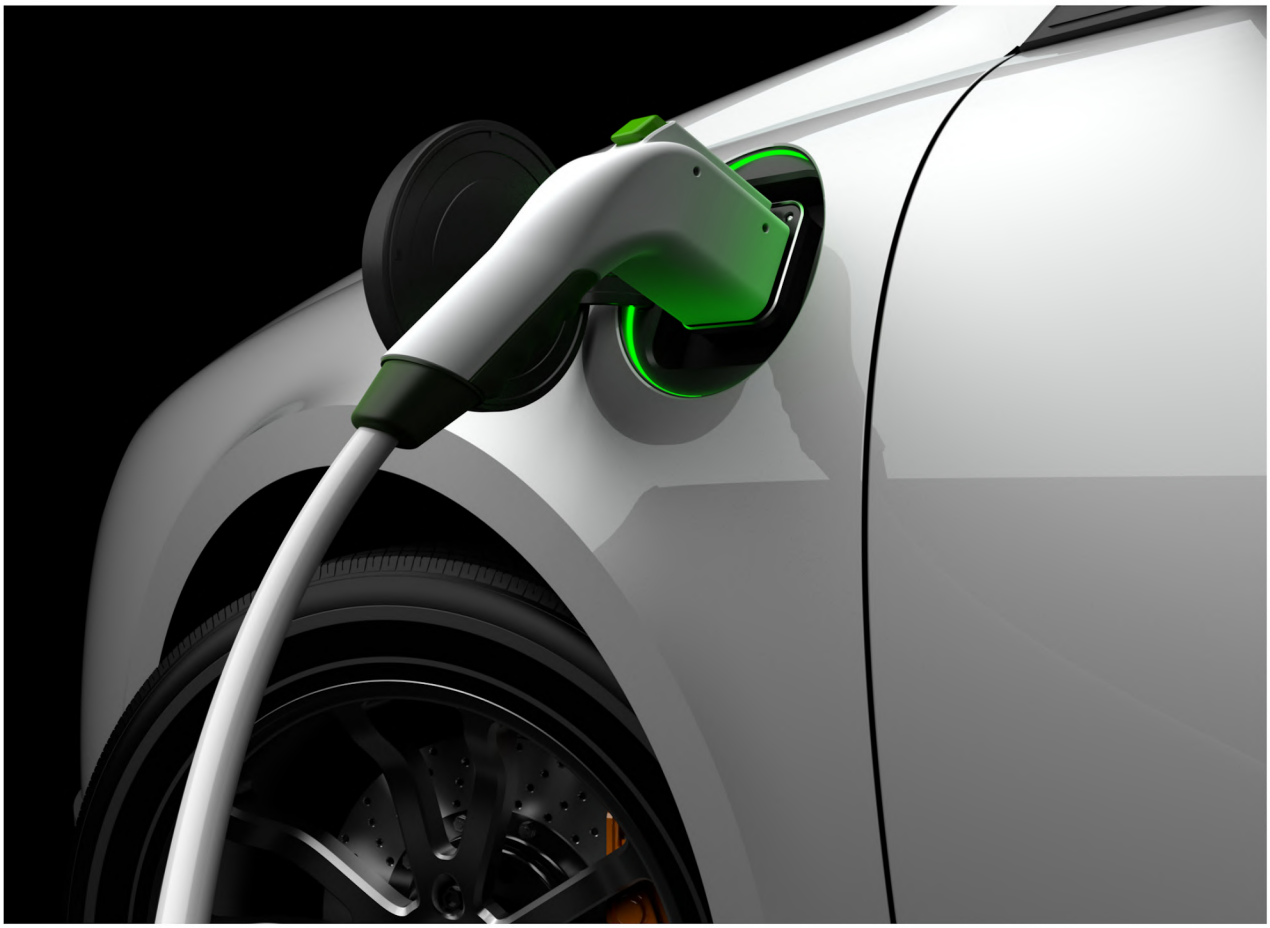
Macchina elettrica: benefici e supporto

Oltre a rappresentare un passo importante per il clima e per l'ambiente, i benefici della traslazione all'elettrico nel settore dei trasporti sono palpabili anche a livello micro, della nostra personale esperienza di consumatori. Innanzitutto, la macchina elettrica avrà bisogno di una manutenzione decisamente ridotta rispetto ai vecchi motori a combustione interna.
A parte il cambio pneumatici e la manutenzione dei freni, la macchina elettrica necessiterà di poco altro. Meno malfunzionamenti, meno visite dal meccanico e riparazioni estremamente ridotte e a baso prezzo. L'auto elettrica ci darà meno preoccupazioni con un ciclo di vita meno esigente e più leggero sul portafogli.
Ma la lista non si ferma qui. Infatti, i proprietari di auto elettriche avranno diritto a un'esenzione dal bollo (fino a cinque anni, a seconda della regione di appartenenza) e, una volta superato il periodo, al pagamento di una tariffa estremamente ridotta rispetto a quella piena. Inoltre, sarà possibile circolare liberamente in tutte le zone ZTL e parcheggiare sulle strisce blu senza dover pagare la sosta. Per quanto riguarda il rifornimento è difficile immaginare uno scenario peggiore di quello che stiamo vivendo, con i rincari sul costo della benzina che abbiamo visto negli ultimi mesi. Allo stesso tempo, però, la ridotta diffusione (ad oggi) delle stazioni di ricarica potrebbe causare qualche preoccupazione.
Saremo in grado di ricaricare la macchina più agevolmente? I nostri viaggi a lunga tratta saranno difficili da programmare, in quanto dipendenti dalla presenza o meno di colonnine?
Anche in questo caso, il futuro sembra portare cambiamenti importanti. L'avanzamento dell'industria nel settore (portata dall'accordo vincolante da parte delle case automobilistiche di cui sopra) sarà immancabilmente accompagnato dall'introduzione di batterie sempre più ottimizzate, oltre a una diffusione esponenziale delle stazioni di ricarica. Arriveremo perfino a poter ricaricare l'auto da casa e a costo zero, grazie ai numerosi provider energetici (ad esempio Sorgenia) che si stanno impegnando per lo sviluppo di colonnine domestiche collegate a impianti fotovoltaici.
Come se non bastasse, le auto elettriche saranno anche più sicure, con sistemi e sensori che proteggeranno sia chi è dietro al volante, che persone e altri veicoli in circolazione. Questo vincolo sostenibile sembra quindi promettere un futuro sereno per gli automobilisti.

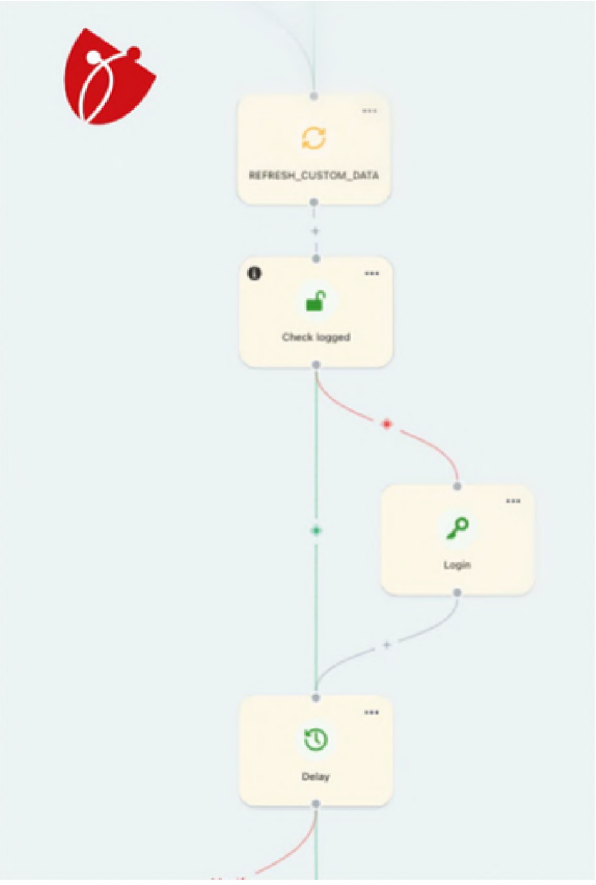
Ci aspetta un decennio di cambiamento sostenibile

Il passo compiuto dall'Europa nelle scorse settimane rimane ambizioso e coraggioso: è la spinta di cui avevamo bisogno per invertire la rotta del cambiamento climatico. Il singolo consumatore potrebbe avere comunque qualche perplessità in merito a quello che, a livello individuale, potrebbe essere percepito come una data di scadenza su un bene a cui si era abituati.

Specialmente in Italia, dove la macchina è talvolta irrinunciabile, ci si potrebbe sentire persi di fronte a un'imposizione che ci spinge verso scelte d'acquisto per cui non siamo pronti.
Anche a livello di vera sostenibilità ambientale, abbiamo già discusso l'insidiosa complessità del tema dell'auto elettrica in un articolo sul nostro blog. Forse, un po' di scetticismo è lecito, ma bisogna ricordare l'orizzonte nel quale questa rivoluzione del settore dei trasporti si inserisce. Non siamo infatti di fronte a un singolo cambiamento che andrà a impattare il singolo consumatore che dovrà trovare il modo di adattarsi. Al contrario, stiamo assistendo a un immenso e irreversibile progetto che andrà a interessare tutte le aree produttive e della nostra esistenza, come cittadini e come consumatori. Investimenti di larga scala, iniziali come di supporto faranno da spina dorsale alle nuove introduzioni in tutti i settori, incentivando parallelamente l'avanzamento tecnologico e la ricerca. Nel migliore delle ipotesi, tra 10 anni guarderemo indietro a questi giorni come se fossero di un'altra era, orgogliosi di aver saputo cambiare rotta quando è venuto il momento. Il tutto, in una transizione multilaterale e, con un po' di fortuna, anche indolore.



L'evoluzione dello sviluppo web: è arrivato FlowerJS



L'avvento delle tecnologie mobile, i nuovi processori, i nuovi studi sulle AI, insomma, tutti i grandi cambiamenti dell'ultimo periodo hanno visto gli antichi software monolitici diventare obsoleti e vedono il sistema andare verso "micro servizi".
È necessario chiedersi: quale sarà il futuro della programmazione? Esisterà sempre la programmazione come l'abbiamo conosciuta?

La riposta arriva forse da uno degli ultimissimi trend di questi anni: la "programmazione Low Code".
Trend iniziato diversi anni fa con la nascita di CMS e App builder vari.

Vediamo però cosa cambia.

CMS VS BPM Engine

La differenza tra un CMS/App builder ed un “BPM engine” o “Workflow engine” è evidente. Il concetto base sta nella flessibilità. I primi (CMS) in genere sono studiati per generare processi di piccolo taglio, sono stati inventati per “generare pagine web”, “form” e poco altro. Questi però possono generare non pochi problemi se malamente utilizzati anche per creazione di progetti più ampi.
WordPress potrebbe essere un esempio in tal senso: ha permesso a tutti di creare pagine Web e tutt’oggi è importantissimo per alcuni processi, ma non è certamente ottimale per progetti di grandi dimensioni.
I sistemi di App builder, un po’ più complessi, hanno permesso la generazione di App per il web.
Spesso si tratta di “app prefabbricate” dal sistema, senza possibilità alcuna di flessibilità. Sicuramente a loro tempo sono state considerate un'innovazione, che però oggi non rispondono in alcun modo alle esigenze business per le evolutive poiché presentano comunemente discreti problemi sui bug, drammaticamente irrisolvibili. Hanno inoltre problemi di aggiornamenti, non è possibile generare nuovi flussi, le tecnologie sono quelle prestabilite e basta.

Quali sono i vantaggi del "Low Code"?

Da qui nascono i "Low Code" engine, motori in grado, attraverso interfacce grafiche, di “generare codice”. Non più “applicazioni”, semplicemente codice.

Perché questo è così importante?

- Perché spesso e volentieri le best practice insegnano che interi flussi e intere porzioni di codice (ben scritto si intende) possano essere riutilizzabili cambiando solo la parte grafica (CSS e similari).
- Perché attraverso diagrammi di flusso si può avere maggiore controllo del progetto che si sta portando avanti, confrontandosi con maggiore facilità con gli analyst che possono anch’essi partecipare al processo di sviluppo, monitorando e collaborando attraverso la stessa interfaccia grafica.
- Perché il mondo ci sta chiedendo “velocità”, i mercati ed i clienti, se già prima avevano i tempi stretti per le evolutive, oggi ne hanno sempre meno.
- Perché un'azienda per sopravvivere alle dure leggi del mercato di oggi ha bisogno di potersi evolvere senza dover aspettare lunghi tempi di sviluppo.

Ad oggi non esistono tantissimi sistemi Lowcode di sviluppo, nessuno di questi ha preso il dominio del mercato. Tutti però stanno studiando. Si tratta di un vero e proprio trend mondiale.

FlowerJS, come funziona il Workflow engine di Spindox

Da queste realizzazioni, 2 anni fa, è nato di FlowerJS, il Workflow engine di casa Spindox interamente sviluppato da Stackhouse.

FlowerJS è un software inquadrato nei BPM Engine (o workflow Engine) per lo sviluppo di progetti di medio/grandi dimensioni, che permette di poter sviluppare codice attraverso diagrammi di flusso ordinati.

Come funziona?

FlowerJS è stato integrato intanto come plugin per Visual Studio Code, creato ad hoc per evitare allo sviluppatore lo stress di dover utilizzare altro sistema di sviluppo. È flessibile, il che vuol dire che è possibile utilizzare FlowerJS per diverse tecnologie. Al momento è operativo sullo stack di ReactJS, NodeJS, ma stiamo implementando Angular, Java e varie altre tecnologie.
FlowerJS permette di sviluppare intere parti di codice attraverso UI e diagrammi di flusso, e facilita il lavoro dello sviluppatore, che a questo punto dovrà esclusivamente occuparsi del "singolo" componente e delle sue customizzazioni.
Per i meno esperti: attraverso il mouse è possibile creare diagrammi di flusso su come funziona l'applicativo, solo che, invece di progettarlo e basta, come accade con "Figma", il motore genera anche il codice, creando l'applicativo stesso. In ogni flusso è possibile inserire i componenti che servono.
Esempio:

- Creo il diagramma del Login.
- Inserisco i componenti che mi servono (text-pwd etc etc).
- Se ho necessità di componenti particolareggiati, li posso comunque sviluppare ed inserire in FlowerJS ed utilizzare anche in diverse porzioni di codice.

Ed ecco che per sviluppare qualcosa ho ottimizzato i tempi.

Che cosa riserva il futuro?

L'errore più comune è quello di pensare che i sistemi lowcode "sostituiranno" gli sviluppatori, cosa che non può accadere. Quello che invece succederà è che i sistemi lowcode, come FlowerJS, aiuteranno gli sviluppatori, dandogli maggiore controllo e permettendo di ottenere i risultati che si raggiungono con i metodi tradizionali in minor tempo.
Tramite FlowerJS, con le ultime evolutive, è possibile mantenere il controllo del Front-end e del Back-end contemporaneamente.
È possibile testare tutto, o parte, del software e si possono anche replicare e scalare sia componentistiche singole che interi flussi.
Lo sviluppatore ha piena libertà, nessun vincolo, ma solo opportunità. Grazie a FlowerJS si ha "pieno controllo" dello sviluppo, semplicità assoluta nel creare delle evolutive.
In più grazie a FlowerJS anche gli "junior" alle prime armi potranno comunque rendersi maggiormente utili ed imparare non solo le basi del codice, ma anche le basi progettuali su come si "organizza un software" e la sua architettura
Ed ecco che il futuro non prevede l'eliminazione dello sviluppatore, ma la sua evoluzione e soprattutto la crescita su base numerica. Attraverso FlowerJS, per una persona con poca esperienza, è più facile comprendere anche le tecnologie di riferimento.
Ad oggi ancora troppi errori vengono commessi in fase di programmazione, fogli interi di codice, codici infiniti, software monolitici impossibili da evolvere.

Mentre il futuro ormai è scritto:

1) Micro componenti.
2) Micro servizi.
3) LowCode e BPM Engine per la loro organizzazione.
4) Sviluppatori sempre più facilitati e specializzati.
5) Meno disordini e bug.
6) Tanto codice di qualità in più.

Lo sviluppatore è il lavoro del futuro, il Lowcode aprirà le porte ad una più ampia platea di persone riducendo i problemi dovuti all'inesperienza.

Le caratteristiche di FlowerJS sono le seguenti:
1) Plug-In VScode.
2) FlowChart System per lo sviluppo di Front-end/Back-end.
3) Cloud Dashboard di sviluppo.
4) Codice testato,100% coverage.

FlowerJS è a disposizione per tutti gli sviluppatori Spindox, che volessero semplificarsi la vita. Al momento è stato utilizzato ed operativo su diversi di software a livello industriale, l'efficacia è garantita, e la semplicità d'uso anche.

Il futuro

Ci rimane ancora qualcosa di bello da fare. È meraviglioso il futuro, Stefa'

La grande Bellezza (2013)
Paolo Sorrentino


LIB.T

OVER DATA.

Un magazine di proprietà
di Spindox sui temi
dell'artificial intelligence
e della tech culture.

Contact us

info@spindox.it
www.spindox.it

spindox
DIGITAL SOUL