Guida autonoma e cybersecurity, quali prospettive per il 2020?

Fino a qualche decennio fa sembrava solo un topos della fantascienza, ma oggi le auto a guida autonoma stanno diventando sempre di più una realtà.

Guida autonoma: i leader del mercato

Da **Uber** a **Google** e – ovviamente – **Tesla capitanata** da **Elon Musk** stanno investendo e sperimentando intensamente su queste tecnologie.

Il colosso del Car sharing e l'indiscusso leader nel mercato delle auto elettriche più in chiave di "affiancamento" alla figura del guidatore, mentre Google ha puntato direttamente sulla guida autonoma.

Ma ovviamente, come con ogni nuova tecnologia "disruptive", sono nati molti dubbi sulla sicurezza di questa, soprattutto perché introducendole nei veicoli ha di fatto introdotto un'altra dimensione nella sfera della sicurezza tipica dell'automobile: alla parte di sicurezza attiva e passiva si è aggiunta quella della cybersecurity.

Dall'infrastruttura alla manutenzione, i rischi fisici e

Cyber

Naturalmente non è oro tutto ciò che luccica, come ogni dispositivo connesso e dotato di un processore, i rischi i rischi relativi alla cybersecurity sono dietro l'angolo.

La guida autonoma fa affidamento a software e hardware per tracciare i suoi percorsi (*pathfinding*).

Maggiore sarà il numero di questi veicoli sulla strada maggiore sarà la superficie d'attacco a disposizione dei Criminal Hacker, d'altronde come qualsiasi dispositivo interconnesso questi veicoli devono gioco-forza fare affidamento su altri device, server e servizi per funzionare correttamente; tutti potenziali access point se non correttamente monitorati e difesi da un efficace perimetro di cybersecurity.

Questo è uno dei grandi scogli nell'implementazione di questi veicoli: presa singolarmente la tecnologia funziona, ma il contesto dove deve operare è tutt'altro che pronto.

Quando all'inizio del secolo scorso le automobili hanno cominciato a diffondersi le strade non erano pronte né tantomeno adeguate ad accoglierle, allo stesso modo oggi le Smart car sono pronte (o quasi), ma l'infrastruttura necessaria a supportarle non è ancora matura.

Guida autonoma: l'impatto della cybersecurity

Questo impatta sia il lato strettamente operativo che quello della cybersecurity. Operativamente la guida autonoma richiederà sempre più massicciamente infrastrutture di rete più affidabili, con fortissimi requisiti di ridondanza e abilità di operare in Real time a seconda delle necessità, nonché una copertura totale del territorio.

Le auto senza conducente hanno già sistemi incredibilmente sofisticati, tra cui computer ad alte prestazioni e un numero crescente di sensori **ADAS** (Advanced Driver Assistance System) come telecamere ad alta risoluzione, **RADAR** e **LIDAR**, nonché grandi schermi 4K/8K e i display head-up (HUD).

Questi sistemi genereranno enormi quantità di dati, che richiederanno un supporto fisico sofisticato: da Data node ad alta velocità a cavi e collegamenti…

È stato stimato che le prossime generazioni di queste vetture arriveranno a inviare 25 gigabyte di dati al cloud ogni ora. Tale mole di dati, ovviamente, comprende anche una grandissima quantità di informazioni sensibili come itinerari di viaggio, storio dei luoghi visitati.

Mantenere intatto questo patrimonio e proteggerlo adeguatamente sarà – a livello di privacy e *Data Integrity* – una delle prime sfide da affrontare per le case automobilistiche e i provider che stanno testando queste tecnologie.

Un'ulteriore area potenzialmente critica è legata alla sicurezza di tutti i sensori che controllano l'area di *obstacle avoidance,* ovvero quelli che analizzano la strada e l'ambiente circostante per reagire a possibili ostacoli o situazioni di emergenza.

Questi lavorano in base a degli algoritmi e sono programmati per rispondere a un vastissimo ventaglio di situazioni, ma cosa potrebbe accadere se l'algoritmo – non sufficientemente protetto e salvaguardato dal punto di vista del suo cybersecurity Framework – venisse corrotto da un Criminal Hacker per non rispondere a pericoli incombenti sulla strada?

Come se non bastasse c'è un ulteriore grandissimo punto di domanda che riguarda il discorso aggiornamenti, croce (per i cybersecurity Provider) e delizia (per i Criminal Hacker) dell'ambito cybersecurity.

Ovviamente per strumenti così innervati di tecnologie l'aggiornamento dei firmware diventa assolutamente critico, allo stesso livello della manutenzione che al momento svolgiamo per la nostra auto.

Ma questo non deve limitarsi alla sola auto a guida autonoma, tutta l'infrastruttura di supporto deve essere costantemente aggiornata; ogni singolo server, ogni singolo endpoint. Un compito sicuramente impegnativo.

Anche lato user finale dobbiamo tenere in considerazione quanto potrebbe impattare la scarsa awerness nei confronti dei Cyber rischi.

Dobbiamo tenere presente che forse solo adesso ha cominciato a fare breccia nella coscienza comune che per utilizzare pc e smartphone e mantenere sicuri i propri dati ci sia bisogno di un certo livello di consapevolezza; l'introduzione delle auto a guida autonoma potrebbe rimandarci all'anno 0 da questo punto di vista.

Quante volte è capitato che le case produttrici ordinassero un recall di un certo modello per correggere un possibile difetto e venissero ignorate (anche solo da un piccolo substrato dei propri clienti)? Nel caso delle Auto a guida autonoma questa negligenza potrebbe avere conseguenze ben più gravi, come tra l'altro hanno avuto già modo di dimostrare negli Stati Uniti.

I precedenti

Come accennato sono già stati fatti test e ricerche su quanto sia compromettibile e quale sia il livello di controllo che può estrapolare un eventuale attaccante che ottiene accesso ai sistemi informatici di un'auto.

Nel 2017 due ricercatori di un'università americana erano riusciti a dimostrare come fosse facilmente possibile dirottare e prendere il controllo dei veicoli di alcuni famosi

brand come Jeep, Ford e Toyota – veicoli "tradizionali" e non certo con il livello di digitalizzazione che possiedono i prototipi di veicoli a guida autonoma.

Nonostante questo erano riusciti a fermare completamente l'auto in marcia sfruttando una vulnerabilità del sistema di infotainment per accedere al CAN-BUS.

Nel mondo reale questo significa che potenzialmente un *threat actor* potrebbe anche arrivare a dirottare il veicolo o costringerlo a girare o frenare all'improvviso per causare disordini o peggio.

Se le auto di oggi sono "semi connesse" e possono essere già così impattate è facile comprendere come le preoccupazioni per un veicolo a guida autonoma che è completamente basato sul principio dell'interconnessione e con una superfice d'attacco così ampia.

Errare è umano

Forse più che un'problema di immaturità tecnologica dell' "auto senza conducente" stiamo sottovalutando le necessità infrastrutturali che questa richiede sia dal punto di vista fisico che Cyber.

Ciononostante, non si può negare che il mondo ha disperatamente bisogno di ridurre la percentuale di errore che l'uomo commette alla guida. Non stiamo solo parlando degli incidenti stradali, ma banalmente anche di ingorghi e di code.

Facendo un parallelo con il mondo dell'aviazione (caso Boeing escluso) è innegabile come l'automazione dei controlli e l'ingresso di tecnologie come i *glass cockpit* e i sistemi di pilota automatico sempre più avanzati hanno aumentato di *n* volte la sicurezza del trasporto su ala. Non sono semplici speculazioni, i ricercatori del Dipartimento dei Trasporti degli Stati Uniti hanno stimato che le auto a guida autonoma

potrebbero ridurre le fatalità dovute agli incidenti sulla strada fino al 94%.

Intervenire a monte

Con miliardi di euro di investimenti in questi progetti da parte di aziende grandi e piccole è abbastanza sicuro che abbiamo da tempo superato il punto di non ritorno, questi mezzi saranno tra poco tra noi.

Prima che l'Uber e la Tesla di turno riescano però a realizzare il loro sogno di flotte di auto autonome c'è la necessità di assicurarsi che tutto il comparto sia allineato sulle necessità di rafforzare il Framework di cybersecurity.

Al momento questa necessità sembra ancora latere, basti pensare che anche la semplice porta ODB – usata universalmente da tutti i meccanici per inserire i loro strumenti di diagnostica – è vulnerabile sia ad attacchi fisici che Cyber.

Citando quanto detto da uno dei ricercatori che ha effettuato i testi sulla Cyber Resilience delle auto: "*I veicoli autonomi sono all'apice di tutte le cose terribili che potrebbero andare male con la tecnologia*".

Un'esagerazione forse, ma come con tutte le tecnologie, dopo una fase di "grazia" dobbiamo fare i conti con i compromessi.

Quali rischi

Le auto autonome hanno buone probabilità di "salvarci" da alcune delle nostre peggiori abitudini. Ma prima di poterlo fare, gruppi privati e pubblici devono sviluppare standard di sicurezza informatica solidi per il settore automobilistico, al contrario c'è il rischio che queste diventino un'arma a doppio taglio e un rischio concreto non solo per la sicurezza dei nostri dati personali, ma anche per la nostra incolumità fisica.

Esistono già dei *must have* imprescindibili per fare fronte alle future minacce: dall'imporre aggiornamenti di firmware tempestivi e obbligatori al taylorizzare i framework in base alla classe e tipologia di veicolo (basti pesare alla differenza oggettiva tra un tir e una semplice auto anche solo in termini di danno potenziale) oltre alla necessità di implementare un protocollo sicuro di comunicazione tra veicolo e veicolo e tra veicolo e infrastrutture e/o device.

Lo scetticismo nei confronti delle nuove tecnologie è giusto. Ma nel caso delle auto senza conducente, a patto di riuscire a costruire un framework di sicurezza solido, potremmo essere davanti a un vero e proprio stravolgimento – in positivo – di come pensiamo e viviamo il trasporto personale.

https://www.key4biz.it/guida-autonoma-e-cybersecurity-quali-prospettive-per-il-2020/284734/