

Dai, chiedimi ancora come funziona!

2 settembre 2024



Pensa alle volte in cui hai acquistato un'auto o hai cercato anche solo di fartene un'idea: quante volte hai sentito la tua voce dire "sì, ma come funziona?" Forse mai.

Certo, potresti rispondermi che in fondo la domanda non avrebbe molto senso perché se hai la patente (o anche no) sai come funziona un'auto, tutto sommato. Però non è così.

Sai guidarla, quasi certamente. Sai che funzione hanno ruote, motore, sterzo, cilindri, freni... Quel che non sai è "come" intimamente funzionino molti dei suoi componenti, specie quelli meno visibili o soggetti alla "creatività ingegneristica" come centraline, circuiti di feedback, meccaniche all'avanguardia, parti brevettate e via dicendo e, in fondo, non te ne interessi neanche se non marginalmente.

Però se ti parlo di ZeroSurface[®], beh, allora... "come funziona"??

Vediamo le differenze tra le due situazioni e perché questa domanda è del tutto inutile, fuori luogo e indicativa di un approccio sbagliato alla risoluzione dei tuoi problemi di sicurezza.

Il caso dell'auto

Quando acquisti un'auto, come per tutti gli altri casi in cui compri qualcosa, segui alcuni processi decisionali e rispetti certi "tuoi" criteri.

Puoi comprare per abitudine, per necessità, per convenienza, per emulazione, per moda, per gratificazione e via dicendo...

Il punto interessante però, è ciò che NON fai. E vuoi sapere cosa NON fai? Puoi arrivarci da solo: è sufficiente che pensi al fatto che a quell'auto tu affidi LETTERALMENTE la vita. Pensaci: non dipende solo da come guidi o da come guidino gli altri o dalle condizioni della strada. Dipende moltissimo da quell'auto.

Cosa dovresti chiedere davvero? Cosa dovresti voler sapere, prima di tutto? Eppure quante volte hai chiesto realmente "sì, ma COME funziona?" con in mente la tua incolumità? No, no, non mentire! Non ho detto che non chiedi quanto sia sicura, ho detto che non chiedi "come" fa a esserlo!

Tu chiedi COSA fa, non COME lo fa! E questo ti basta.

Perché ti basta?

Ti basta perché di auto ne costruiamo da decenni, non sono nulla di nuovo, sono "tecnica nota" (tu credi).

Ti basta perché ti fidi del costruttore.

Ti basta perché hai esperienza (a qualunque livello) di quel tipo di "oggetto".

Ti basta perché ti fidi di chi te la vende o di qualcuno che ne sa più di te.

Ti basta perché "...sì, vabbè, figurati se adesso fanno una macchina che non frena bene o che prende fuoco da sola!"

E magari ti basta perché ci hai fatto un giro di prova e ti ha dato un senso di affidabilità e sicurezza.

Aggiungi a questa lista ciò che vuoi...

Il caso delle soluzioni di sicurezza

Prova a dire che non hai comprato in passato (o non compreresti oggi) una soluzione di sicurezza informatica attraverso uno o più dei filtri decisionali scritti qui sopra.

Dimmi che non hai comprato Cisco o Fortinet per uno o più di quei motivi; però, quante volte hai chiesto "sì, ma come funziona"? E se lo hai fatto, cosa volevi sapere realmente? Volevi davvero sapere come funzionasse il cuore di quel sistema? E seppure fosse, davvero ti aspettavi che la risposta del costruttore ti svelasse i suoi "segreti industriali"?

Certo, si trattava di costruttori noti, un po' come succede con le auto, quindi ti fidi. Oppure di soluzioni talmente diffuse che "...beh, ma se succede qualcosa a me vuol dire che deve

succedere a mezzo mondo, figurarsi...” (la mia risposta a una simile affermazione sarebbe come sparare sulla Croce Rossa, tuttavia suggerisco ugualmente la lettura di questo post: *Dai, chiedimi ancora chi altri usa iceGate!*)

Insomma del “come” funziona non te ne importa concretamente nulla!

Ripeto:

tu compri ciò che fa, non come lo fa

E c'è di più.

Pensa che, anche considerando questo punto di vista, il tuo comportamento resta ancora incoerente poiché se è vero, come nel nostro esempio, che compri la sicurezza del veicolo, in realtà lo fai comprando ciò che ti hanno “detto” altri (risultati di crash test, certificazioni, articoli, passaparola, commerciali ecc)!

Con quell'auto che stai per comprarti non ci sei mai andato a sbattere a 60 km/h contro un muro... per vedere l'effetto che fa!

Eppure la compri.

Il caso dello ZeroSurface[®]

Lo ZeroSurface[®] è **tecnica non nota**.

LATERALCODE forse non la hai mai sentita o solo di sfuggita.

E quindi credi che la tua domanda “Sì, ma come funziona?” sia giustificata. Non è così.

Innanzitutto otto anni di sviluppo non si raccontano nello spazio di un articolo, di una risposta verbale o in uno sheet o un paper (sì, molti lo fanno e ci danno il contentino, perché se credi che in ciò che leggi ci sia quello che ti serve veramente di sapere allora sei il re di Fantasilandia); soprattutto, però, sei vittima del più elementare dei cortocircuiti. Mi spiego.

Lo ZeroSurface[®] è una soluzione che lavora a metà tra i livelli 2 e 3 dello stack OSI (e già questo suona strano, un po' come il binario 9 e 3/4 di Harry Potter... ma andiamo oltre) e ciò che garantisce è la protezione da infiltrazioni, attacchi supply chain, DDoS, esfiltrazioni e backdoor, phishing e attacchi Zero-Day, tutto in una volta.

Per la sua progettazione sistemica, **non interagisce con i tuoi sistemi e le tue reti** (che rimangono esattamente quelli che sono, senza bisogno di modifiche!), non è un SIEM (ma li protegge), non è un WAF (ma li protegge), non è una VPN (ma le protegge), non è un Identity Provider (ma li protegge), non è “pass through”, non è un security hub (ma li protegge), non triangola, non usa dati associati o sensibili (!), non è Zero Trust (ma lo protegge), non è real time, non è IA. Se te ne volessi liberare (vai a sapere perché) basterebbero pochi minuti, e la tua rete tornerebbe istantaneamente a quella che era (e buona fortuna).

Quello che fa dovresti saperlo, altrimenti non saresti qui (e in ogni modo puoi scoprirlo in un secondo in rete): diciamo solo, brevemente, che è quanto di più vicino tu possa avere a **una rete air gap ma che ti permette di comunicare lo stesso!**

Il problema (in parte all'origine del cortocircuito) è che **ti sembra troppo bello per essere vero.**

Sia come sia... vuoi sapere come funziona???

Dai, non scherziamo.

E quindi cosa dovresti fare?

C'è una cosa, molto più utile che tu puoi fare: "metterti al volante" e andare a sbattere a 120 km/h... per vedere l'effetto che fa.

Chiedi di usare la tua futura auto sulla TUA pista, non sulla nostra (leggi: nell'ambiente che preferisci); ingaggia i piloti più spericolati (leggi: tuoi tecnici di fiducia, hacker russi o cinesi, tu stesso, chiunque tu voglia).

Poi chiedi quello che chiederesti NORMALMENTE. Chiedi le garanzie che ti servono.

Scopri COSA FA per te, non COME lo fa.

Hai paura di qualcosa? Comprensibile. Ma se hai capito COSA FA e ritieni che ti serva (difficile immaginare il contrario), allora poni le domande giuste: capirai quel che ti manca di capire (davvero) e potrai decidere.

Abbandona le categorie di pensiero e di soluzioni cui sei abituato ed evolvi il tuo ruolo e la tua funzione.

Gianluigi Merlino

Lateral News — Articoli, idee e riflessioni sullo sviluppo tecnologico e sulla sicurezza informatica non "mainstream"

lateralcode.it