LATERAL NEWS — LATERALCODE

Cyber Security: rispondete a questa sola domanda, poi decidete.

30 maggio 2023

LA DOMANDA E LA PREMESSA

La domanda è la seguente.

In termini di **pura sicurezza** preferireste avere:

*A) un sistema fragile che non “parla” con **nessuno***

*B) un sistema forte che “parla” con **tutti**?*

Vi lasciamo qualche secondo per pensare. *Tic tac…*

Bene, quale che sia la vostra risposta, è del tutto ovvio che nel caso A) il livello di sicurezza è incomparabilmente più elevato e questo perché un sistema, per quanto fragile o permeabile, non corre alcun rischio se non “parla con nessuno” e la sua fragilità rimane solo potenziale, **teorica**, sulla carta; per questo immaginiamo che la maggioranza, se non la totalità di voi, avrà scelto proprio questa opzione (d’altronde, vale ripeterlo, **un sistema non connesso alla rete è certamente più sicuro** rispetto all’altro, e ci mancherebbe il contrario).

PRIME CONSIDERAZIONI (e prime difficoltà)

Se la premessa è corretta, allora ne discende che in un sistema la sicurezza non è figlia dell'essere intrinsecamente "fragile" o "forte", ma dell'essere connesso oppure no e in che modo, e più avanti sarà ulteriormente chiaro(*).

Fin qui è facile. Tuttavia non vi sarà sfuggito un ovvio "ma": se è vero che un sistema disconnesso dalla rete, indipendentemente dal suo livello di forza, è fantastico in termini di sicurezza, purtroppo è anche **inutilizzabile**.

Ecco il motivo del **compromesso** di cui siamo schiavi **da sempre**: per pubblicare applicazioni, reti, interfacce, API e servizi vari abbiamo dovuto esporli, farli parlare tra loro o con il resto della rete. In altri termini, i sistemi DEVONO essere raggiungibili e disponibili, fosse anche solo per permettere loro di **decidere da cosa difendersi** oppure no, di chi fidarsi e di chi no.

Ma è proprio questo il problema: così facendo li esponiamo (sia tecnicamente che concettualmente) anche al rischio di non riconoscere il cattivo di turno (cosa che avviene con sconfortante regolarità) e di farsi ingannare da qualche abile travestimento.

Il quadro già caustico prende ulteriori tinte fosche se solo ricordiamo che tutti (TUTTI!) i sistemi di sicurezza che installiamo per mitigare il problema ne soffrono a loro volta, **soluzioni Zero Trust comprese!**

In un sistema la sicurezza non è figlia dell'essere intrinsecamente "fragile" o "forte", ma dell'essere connesso oppure no e in che modo

Notato quanto si parli sempre di robustezza dei sistemi in chiave di forza "muscolare" e quanto la ricerca si concentri sullo sviluppo di quella caratteristica? Non è mai considerata la possibilità che un sistema possa funzionare anche da disconnesso (il che, fino a "ieri", era anche comprensibile, va ammesso).

SFIDA SENZA FINE A BRACCIO DI FERRO

Altra semplice ma poco frequentata domanda: (*)come possiamo valutare l'adeguatezza del livello di forza di un sistema se non conosciamo a priori l'entità di quella che ci attaccherà? Non possiamo, ed è per questo che i contendenti di siffatta battaglia, chi attacca e chi difende, sono sia vittime che creatori dell'Escalation (non a caso un archetipo sistemico) cui pongono quotidianamente rimedio alimentandola!

Presente i sistemi di sicurezza "real time"? Quelli che bruciano enormi risorse nel tentativo di capire, a ogni secondo che passa, se quello stormire di foglie è sospetto oppure no? Ecco, tutti figli di questo approccio.

RAGIONARE DIVERSAMENTE

Bene: ragionare in termini sistemici (il nostro payoff, come sapete, è "the sistemic way") significa, tra le molte altre cose, sviluppare soluzioni che eliminino le cause, non i sintomi, evitando al contempo l'insorgere dei comportamenti emergenti tipici delle soluzioni complesse.

Pensate, solo per fare un esempio, alle **backdoor**: secondo noi rappresentano il livello di fragilità **intrinseco** di un sistema rispetto alla capacità degli attaccanti. Di fatto parlare di superficie di attacco e di **backdoor** è esattamente la stessa cosa: la prima è evidente dall'esterno, la seconda è evidente dall'interno.

L'eliminazione **totale** e **costante** delle superfici esposte ha poi un altro vantaggio sistemico, quello di rappresentare un **potente effetto leva**.

Una condizione di **ZeroSurface™** garantisce infatti protezione da:

- Intrusioni
- Attacchi DDoS
- Minacce Zero-Day
- Esfiltrazioni e backdoor
- Inoculazioni di malware (ransomware compresi)
- Phishing
- Attacchi Supply Chain

Non è poco, per una sola mossa.

Ragionare in termini sistemici significa sviluppare soluzioni che eliminino le cause, non i sintomi

IL BELLO DI POTER SCEGLIERE (e soluzione)

Fino a ieri sembrava impossibile, un paradosso, ma oggi possiamo finalmente **scegliere** se un sistema debba essere connesso o disconnesso pur **mantenendo inalterata** la fruibilità del servizio che offre!

A questo punto sarebbe curioso parlare con chi, potendo scegliere, preferisse restare sempre connesso e disponibile.

La risposta sensata alla domanda iniziale è dunque una e una sola: "Un sistema non connesso". Semplicemente.

Ecco, ora sta a voi **scegliere** se disconnettervi e, se non lo fate, alla fine **saprete di chi sarà stata la responsabilità**.
