LATERAL NEWS — LATERALCODE

La Dinamica dei Sistemi nella cyber security e perché le strategie tradizionali falliscono

25 ottobre 2024

Se state leggendo questo articolo appartenete, al minimo, a una di queste categorie:

- Siete responsabili della sicurezza in un’organizzazione
- Vi occupate di cyber security come consulenti o professionisti
- Siete decisori che devono valutare investimenti in sicurezza informatica

In ogni caso, vi siete mai chiesti perché, nonostante i continui investimenti in **soluzioni sempre più sofisticate**, gli attacchi informatici continuano ad aumentare sia in frequenza che in complessità?

La risposta è tanto semplice quanto scomoda (taaaanto scomoda, e chi-vuol-capire-capisca):

> *state affrontando un problema sistemico con soluzioni lineari*

Il Paradosso della Complessità

Prendiamo un esempio concreto. Quando un'azienda subisce un attacco informatico, qual è la risposta tipica?

1. Rafforzare le misure di sicurezza esistenti
2. Aggiungere nuovi layer di protezione
3. Implementare sistemi di monitoraggio più sofisticati
4. Aumentare il budget per la sicurezza
5. Pregare (e piangere se è andata parecchio male)

Ognuna di queste azioni segue una logica lineare *causa-effetto*: se c'è un problema, aggiungiamo una soluzione. Se la soluzione non basta, ne aggiungiamo un'altra. E un'altra ancora.

Si chiama analisi, o come direbbe Krishnamurti:

> *frammentazione.*

Ma cosa succede realmente? **Ogni nuovo layer di sicurezza aumenta la complessità del sistema.** E con la complessità aumentano:

- Le potenziali vulnerabilità
- I punti di possibile fallimento
- La difficoltà di gestione
- I costi di manutenzione
- Le incompatibilità tra sistemi

L'effetto del paradosso

Ecco dunque la verità, *quella (taaanto) scomoda*: più complesso diventa il vostro sistema di difesa, più diventa vulnerabile.

È come costruire un castello sempre più alto e intricato, dimenticando che ogni nuova torre, ogni nuovo passaggio segreto, ogni nuovo sistema di difesa può diventare un punto di ingresso per gli attaccanti, un nuovo fronte da sorvegliare, difendere e prevedere nei turni di guardia.

Tranquilli, sull'altro lato il castello è integro!

I metodi tradizionali seguono questo approccio additivo:

- Più firewall
- Più sistemi di autenticazione
- Più layer di controllo
- Più regole e policy
- Più strumenti di monitoraggio

Però la dinamica dei sistemi ci insegna che:

> *la somma delle parti non equivale al tutto.*

Un sistema complesso sviluppa comportamenti emergenti che non possono essere previsti analizzando i singoli componenti (rieccola, la verità taaanto scomoda…).

La Rivoluzione Necessaria

È qui entra in gioco **ZeroSurface®**.

Invece di aggiungere complessità, la nostra tecnologia:

- *Elimina tutte le superfici d'attacco*
- *Semplifica l'architettura di sicurezza*
- *Toglie i punti di vulnerabilità*
- *Minimizza le dipendenze tra sistemi*

- *Non interagisce con la struttura ospite*

In altre parole, non costruiamo un castello più alto e complesso: lo rendiamo

irraggiungibile => (quindi) indisponibile => (quindi) invisibile => (quindi) inattaccabile.

Con tutte le sue funzionalità invariate!

Lo ZeroSurface® è fatto a forma di uovo

Come sempre è una questione di scelta: la vostra

Potete continuare a seguire l'approccio tradizionale, aggiungendo strato su strato di "protezione" e sperando che la prossima soluzione sia quella definitiva (pregare è una strategia come un'altra).

Oppure potete abbracciare un **cambio di paradigma** (REALE) e comprendere che la vera sicurezza non sta nell'**accumulo di difese**, ma nell'**eliminazione delle minacce**.

Come disse (forse) Einstein:

> *Non possiamo risolvere i problemi allo stesso livello di pensiero che abbiamo usato quando li abbiamo creati*

È tempo di pensare in modo diverso alla sicurezza informatica.

È tempo di pensare in termini sistemici (in realtà siete già in ritardo).

O anche no: potete sempre continuare a pregare.

Gianluigi Merlino

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

lateralcode.it