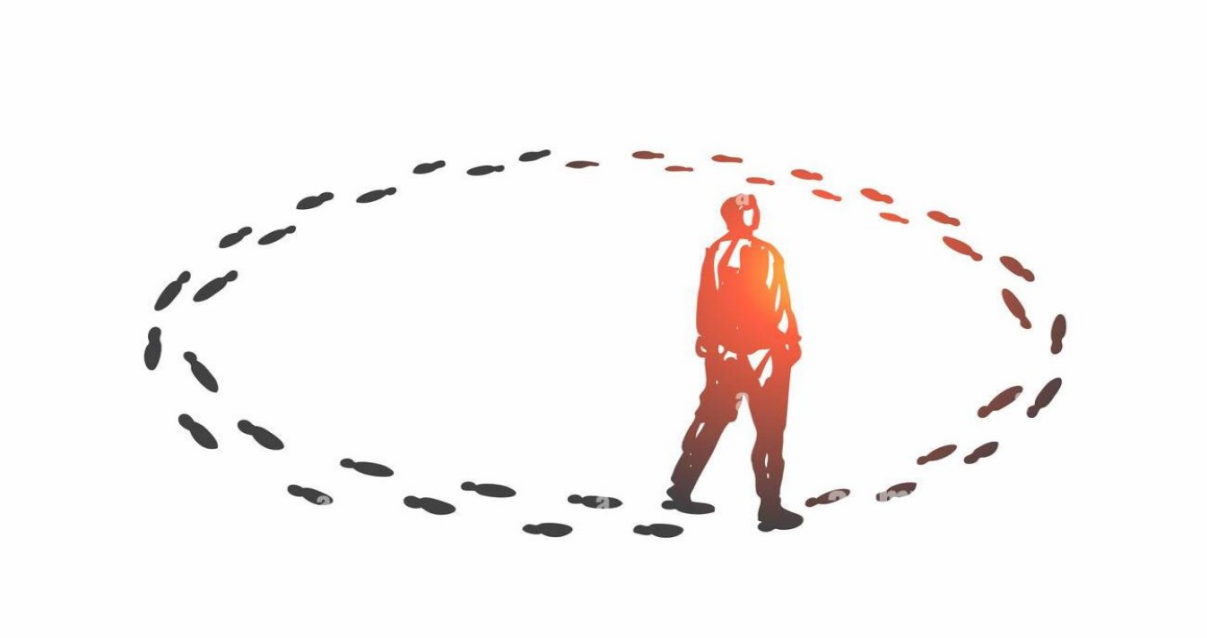
Circoli causali e archetipi sistemici nella sicurezza informatica: se non ti occupi di loro, loro si occuperanno di te.

3 ottobre 2023



In questa newsletter abbiamo spesso parlato di **sistemi**, **complessità dinamica** e di approccio sistemico al problema della sicurezza informatica, che poi è quello che adottiamo qui in Azienda.

In un post di luglio scorso vi abbiamo inoltre posto un quesito: “Quanti dei progressi nella tecnologia difensiva alimentano quella offensiva?”. Dietro questa domanda, molto più che solo provocatoria, si celano dinamiche troppo spesso ignorate.

I circoli causali e gli archetipi sistemici (principi base per capirci)

Una volta compreso cosa si intenda per sistema (e dopo la lettura dei nostri articoli spero inizi a essere chiaro) è utile iniziare a rappresentarne il senso attraverso uno dei tipici linguaggi dell’osservazione sistemica che sono i **diagrammi a circoli causali**, **stock** e flussi. Qui, per adesso, ci limitiamo a disegnare diagrammi circolari non solo per evitare di complicarci troppo la vita ma anche perché sono più che sufficienti allo scopo.

Un possibile circolo causale è quello detto “di rinforzo”, “di accrescimento” o di “feedback positivo” poiché tende **all’amplificazione nel tempo di un fenomeno** o di una grandezza (da cui l’icona della valanga). È tanto intuitivo quanto subdolo e ignorato:

Se la grandezza A è, mettiamo, **la capacità offensiva degli hacker** e la grandezza B è **la capacità di difendersi degli attaccati** tutto è molto chiaro (i segni + e – stanno a indicare che la grandezza alla fine della freccia cresce in maniera rispettivamente diretta o inversa rispetto a quella che si trova all’origine). Ingannevolmente, potremmo pensare che se le cose stessero (solo) così ci potremmo anche stare: in fondo si tratterebbe di una situazione in cui il livello di scontro fra contendenti **ugualmente forti**(?) sale continuamente e che i danni che gli attaccati subiscono sarebbero “limitati” alla **parentesi temporale** loro necessaria per prendere le contromisure nei confronti dei nuovi tipi di attacchi (che poi questa parentesi possa essere pericolosamente lunga è un altro paio di maniche!). Ovvio che se ragionassimo così rischieremmo di scollarci dalla realtà dei fatti.

Perciò proseguiamo, ma per farlo dobbiamo **inserire un semplice concetto** senza il quale non possiamo neanche iniziare a pensare in termini di sistema: **il ritardo**.

Lo vedremo fra un attimo perché prima dobbiamo spendere due parole sugli archetipi.

Un archetipo è una struttura sistemica ricorrente che produce andamenti caratteristici nel tempo

In altre parole, esistono **schemi causali** di eventi e comportamenti riconoscibili che **si ripetono a prescindere dal tipo di ambiente** in cui sono inseriti, come dire che possiamo trovare un archetipo all’opera in uno studio, per es., demografico e trovarlo poi, tale e quale in uno studio biologico, tecnologico, sociale, militare ecc.

Ricordatevi tre punti importanti:

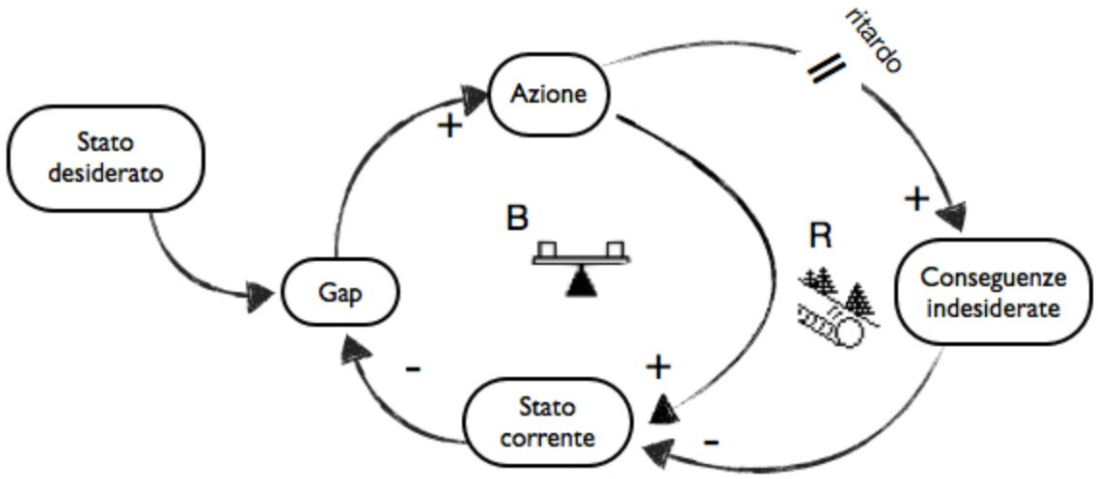
1. Gli archetipi sono in **numero limitato** ma consentono, singolarmente o in combinazione con gli altri, di rappresentare **l'intera realtà dinamica** che ci circonda.

2. Essendo strutture che si ripetono **sono stati studiati a fondo** e quindi la loro conoscenza ci consegna una capacità di interpretazione e un'efficienza di intervento che solo un pensatore sistemico può vantare. Tutti gli archetipi vantano infatti **esclusive proprietà** come comportamenti attesi, resistenze, punti di leva ecc.; insomma sono "organismi noti" di cui conosciamo bene le malattie e le cure profonde.

3. Possono essere usati in almeno **quattro modi** diversi: A. come filtri di osservazione, B. come modelli di struttura, C. come teorie dinamiche o D. come strumenti per la previsione dei comportamenti.

E finalmente eccoci a noi

Un archetipo che ci interessa qui è il **FtF — Fixes that Fail** (Soluzioni che Falliscono): osservate la sua rappresentazione grafica.



Leggiamolo insieme: naturalmente noi siamo i buoni e abbiamo uno **stato desiderato** (per es. starcene in pace a fare il nostro lavoro senza preoccuparci dei continui attacchi).

Questo stato è però diverso da quello reale perciò mettiamo in atto comportamento volti a ridurre il **gap**. Se tenessimo conto del solo circolo B (di bilanciamento) la cosa sembrerebbe anche funzionare: adottiamo cioè **azioni** che → migliorano lo stato corrente il quale → diminuisce il gap con lo stato desiderato che quindi → richiede minori interventi fino al punto in cui non servì fare altro.

Tuttavia sappiamo bene che le cose stanno diversamente e il circolo R (di rinforzo) è lì a rappresentarle: con un **ritardo più o meno sensibile(!)** si presentano **conseguenze indesiderate** (pensate alla scoperta, tardiva per definizione, di nuove vulnerabilità o all'affinamento delle tecniche d'attacco stimolato proprio dal circolo B, alle incompatibilità, alle **patch** che non risolvono ma "crashano" i sistemi… o a tutto quanto scriviamo nelle altre

edizioni di questa newsletter). In ultima analisi, le azioni poste in essere nel primo circolo **alimentano esattamente ciò contro cui le adottiamo**.

Nel suo celeberrimo *The Fifth Discipline*, Peter Senge indica per questo archetipo una "Descrizione", un "Segnale d'Allarme" e un "Principio di Gestione".

- **Descrizione**: una soluzione, apparentemente efficace a breve termine, ha conseguenze impreviste a lungo termine che possono richiedere un utilizzo anche maggiore della stessa soluzione (si è sempre fatto così)
- **Segnale tempestivo di allarme**: sembrava che prima funzionasse, perché non funziona adesso?
- **Principio di gestione**: mantenere la concentrazione sul lungo termine. Trascurare la soluzione a breve termine, se possibile, oppure utilizzarla soltanto per «guadagnare tempo» mentre si lavora sui rimedi a lungo termine.

Peter e lo ZeroSurface®

La nostra soluzione di sicurezza perimetrale **iceGate** è realizzata su profonde radici sistemiche e lo standard **ZeroSurface®** su cui si basa permette, a chi lo adotta, di **rispondere in pieno alle raccomandazioni di Senge** oltre che a evitare le conseguenze indesiderate del **FtF**; va da sé che un approccio di questo tipo, di lungo periodo, richiede da parte dei **decisori** una certa pianificazione, **disposizione al cambiamento**, preparazione e lungimiranza.

> *Il cambiamento è una legge naturale ineluttabile. Quello di cui dobbiamo preoccuparci è l'atteggiamento mentale con cui affrontiamo il cambiamento.*
> *— N. Hill e W.C. Stone*

Crediamo che ciò sia non solo auspicabile ma imprescindibile poiché le leggi del sistema non sono eludibili, in alcun modo, **perciò o ci occupiamo di loro o loro si occuperanno di noi**.

Gianluigi Merlino

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

lateralcode.it