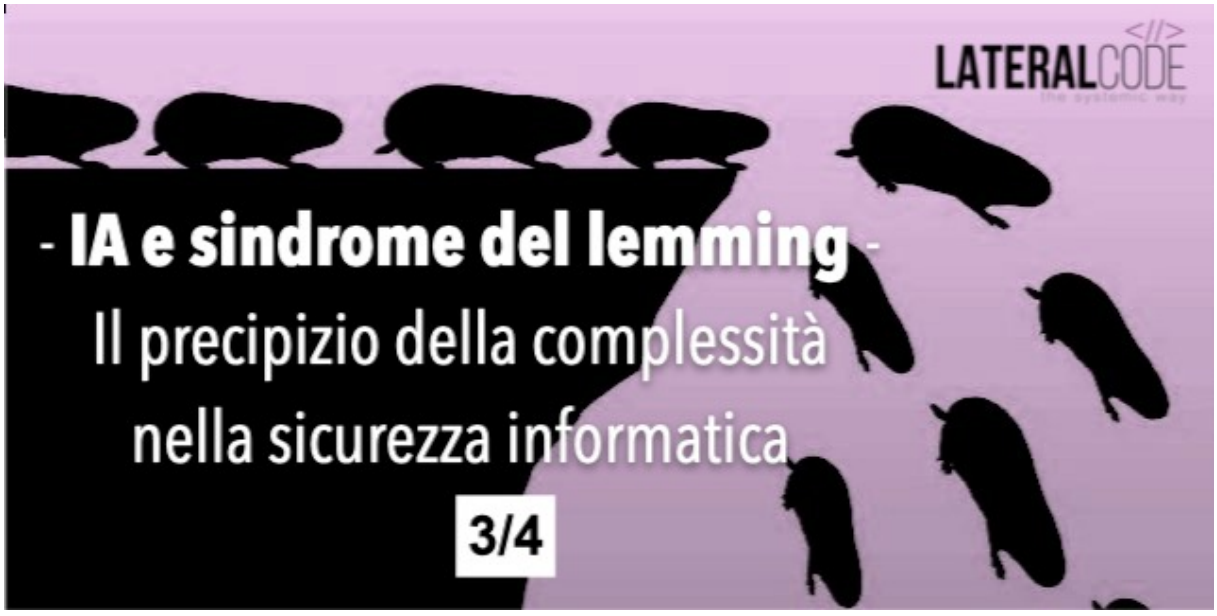
LATERAL NEWS — LATERALCODE

IA e sindrome del lemming: il precipizio della complessità (3/4)

25 luglio 2023



Fatevi coraggio, siamo nella seconda metà del percorso; vedrete che alla fine unirete i puntini!

Per proseguire ho bisogno però di introdurre un'altra definizione, quella di **equilibrio**:

> *L'equilibrio di un sistema è l'obiettivo intrinseco che esso persegue per perpetuare e proteggere se stesso producendo continui feedback tra un componente e l'altro*

Bene. Un principio con cui dobbiamo far pace è che un equilibrio non è "buono" o "cattivo" in sé. Il sistema non ha i nostri valori, le nostre preoccupazioni o le nostre **esigenze**, lui "vive" e basta, autonomamente, ed è l'unica cosa che gli "interessa"; solo in un **secondo momento** arriviamo noi che, da osservatori, giudichiamo se quell'equilibrio ci è gradito oppure no, come abbiamo fatto nel giudicare gli scambi tra Bob e Alice, per capirci.

Nel pensiero sistemico, di fronte a una condizione problematica e indesiderata (per noi, ripeto, **non per il sistema**) occorre tenere perciò un'attenzione e un comportamento del tutto particolari.

THINK DIFFERENT, ACT DIFFERENT

Metto qui tre criteri di esempio, già molto eloquenti.

1. Domanda sistemica: cosa sta impedendo al sistema di raggiungere un diverso equilibrio?

Non domandiamoci - Cosa devo fare per cambiare le cose? - ma chiediamoci invece quali precondizioni sono necessarie affinché le cose “cambino per energia intrinseca” al sistema, connaturata e spontanea, volgendo così a nostro favore le sue “abitudini” più profonde e difficili da sradicare. In altre parole, più immettiamo o “sovrapponiamo” in un sistema, più resistenze e comportamenti imprevisti provochiamo. Questa legge è ineluttabile.

2. Indicazione preferenziale: intervento sottrattivo.

Un operatore sistemico, dunque, cerca sempre di evitare interventi additivi, rinuncia cioè all’inserimento di ulteriori regole e alla forzatura di nuovi componenti: la sua scelta ricade piuttosto sull’eliminazione degli elementi distorsivi o inutilmente ridondanti.

Perciò, come sopra, non domandatevi “come modificare” il sistema o quali nuove prescrizioni introdurre ma anzi cosa potete “eliminare”, quali elementi o relazioni (cioè vincoli) sottrarre. Va da sé che ciò significa prima imparare a “pensare per sistemi”.

3. Obiettivo comune: evolutivo ed ecologico.

Portare un sistema all’equilibrio desiderato significa condurlo a un livello di evoluzione che favorisca condizioni grazie alle quali si autoproteggerà da eventuali ricadute (intervento evolutivo). Ciò a cui puntiamo è una condizione di efficienza che conservi quanto di buono già esiste evitando che, nel tentativo di cambiare quanto non ci piace, si “butti via il bambino con l’acqua sporca” e si danneggino le interazioni già funzionali (ecologia dell’intervento).

I CANONI DEL PROGETTO ICEGATE - ZEROSURFACE®

Nel rispetto di tali premesse (e di alcune altre che per brevità ometto poiché non aggiungerebbero significati utili in questo articolo) ecco i requisiti che alla vigilia del progetto avevamo stabilito per un **sistema di sicurezza informatica** realizzato in chiave sistemica, gli stessi che poi ne hanno guidato lo sviluppo.

A - La soluzione avrebbe dovuto:

1. essere facilmente **integrabile**

2. essere semplice da usare, **indipendente** da dispositivi, sistemi operativi, ambienti e infrastrutture.

3. essere **compatibile con ogni altro sistema di sicurezza**, rinforzandolo in misura determinante.

4. lavorare a **basso livello dello stack OSI**. Più il livello fosse stato basso più la soluzione sarebbe stata **trasversale** e non avrebbe aumentato la complessità; oltre a ciò avrebbe dovuto sfruttare “un’abitudine profonda” del sistema stesso (in questo caso scegliemmo il protocollo IP).

5. **eliminare completamente** le superfici d'attacco in ogni condizione operativa, fossero esse in forma diretta, indiretta, seriale, concentrata o triangolata: nessuna soluzione di sicurezza perimetrale rispettava infatti, fino a quel momento, un simile criterio poiché un punto di accesso, per quanto ridotto e/o protetto, era esposto **sempre** e comunque (e infatti i risultati si vedono).

B - La soluzione NON avrebbe dovuto:

1. aumentare la complessità **totale** né dei sistemi locali né della rete in genere.

2. operare come **identity provider** né farne uso (gravissima fragilità logica del sistema e focolaio di interesse per gli attacchi)

3. contenere **dati sensibili e/o associati** di clienti e/o utenti, cioè un vero **Secure by Design** e **Privacy by Default**, per la gioia dell'amato GDPR e soprattutto per preservarne l'integrità assoluta (il concetto è semplice: se non tratto dati sensibili, non mi possono essere rubati).

Certo, un progetto di questo tipo era **estremamente ambizioso**, sembrava persino utopistico stanti le tecnologie correnti.

Pensate, per esempio alla sfida rappresentata dai punti A5 e B3 dove uno comprometteva l'idea stessa di una rete connessa (nessuna superficie esposta -> nessuna apertura -> nessuna connessione possibile) e l'altro privava il progetto persino della possibilità di "distinguere i buoni dai cattivi"…

- Risultato: oggi la tecnologia ZeroSurface® è un brevetto internazionale depositato.

CONCLUSIONE E ULTIMO SFORZO (per oggi)

Vi sarà ormai chiaro che il contrario di "complesso", quindi, non è "facile", semmai è "semplice", solo che **realizzare la semplicità** è opera assai faticosa e… "difficile".

"Qualsiasi sciocco può fare qualcosa di complesso; ci vuole un genio per fare qualcosa di semplice." (Pete Seeger)

La complessità **può** e **deve** essere affrontata in termini **sistemici** ma per farlo occorre saper pensare **sistemicamente**; purtroppo, è più probabile veder volare un unicorno fucsia che trovare progetti, ricerche e approcci **sistemici** in tema di sicurezza informatica (e non solo lì, ahinoi).

Nel caso in questione, fintanto che avessimo avuto **superfici da difendere** avremo avuto bisogno anche di **lucchetti, blindature, guardie armate** (intelligenti?), sistemi di analisi (ops "sistemi", ops "analisi") e sovrastrutture **sempre più complesse**.

Vedete, fintanto che svilupperemo simili schieramenti difensivi esisterà sempre **un'analogo progresso** nei metodi di attacco, tanto più pericolosi quanto più complesso sarà il sistema

attaccato perché produttore di **emergenze** potenzialmente devastanti e **afflitto da fragilità** tutte da scoprire.

Insomma, la solita rincorsa degli uni sugli altri, una **escalation** (guarda caso uno degli **archetipi sistemici**) che sarebbe comica se non fosse spaventosa.

La prossima volta chiuderemo finalmente con i lemming, l'IA e la responsabilità dei ruoli in questo gioco delle parti (e devo anche mantenere fede all'impegno di spendere due parole sulla ***Privacy by Default*** che ho preferito espungere da questa puntata… prendetemi a male parole nei commenti).

Alla prossima!

Gianluigi Merlino
