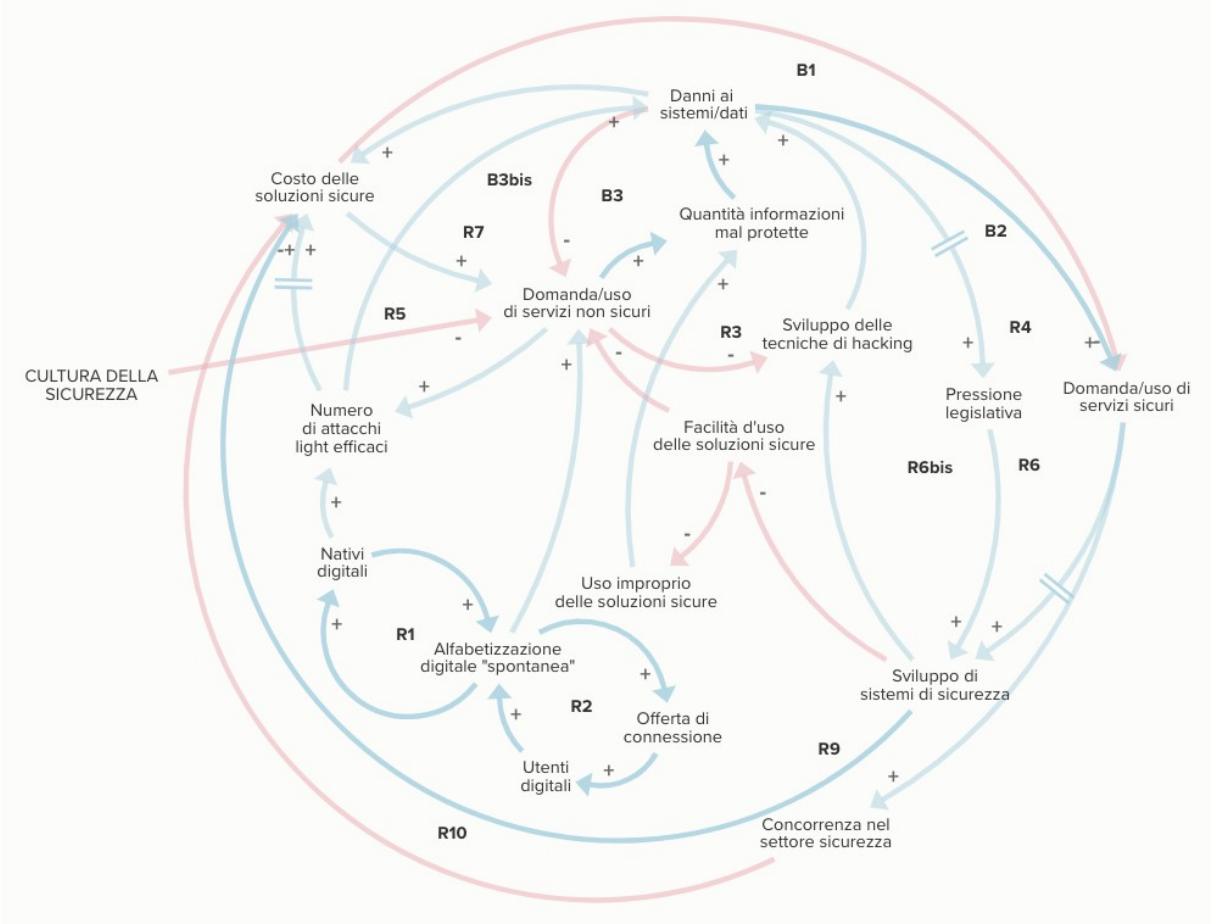
LATERAL NEWS — LATERALCODE

Osservazione sistemica e sicurezza informatica oggi: divertiamoci con un esempio (4/4).

5 dicembre 2023

Ok, siamo arrivati alla fine, che poi è sempre un nuovo inizio...

Il diagramma con cui ci siamo salutati l'ultima volta può sembrare complesso ma in realtà lo abbiamo tracciato indulgendo a notevoli semplificazioni le quali, tuttavia, non mi pare sottraggano utilità all’esercizio: lo scopo, in questo articolo, è quello di stimolare osservazioni e riflessioni fuori dal coro, quanto basta per spingere a uno studio del tema da un punto di vista diverso.



Il mantra di ogni buon ingegnere della sicurezza dovrebbe essere: “La sicurezza non è un prodotto, ma un processo”. È più che progettare una forte crittografia in un sistema: è progettare l’intero sistema in modo tale che tutte le misure di sicurezza, inclusa la crittografia, lavorino insieme. — Bruce Schneier

Su e giù per le curve

In questa osservazione, avrete notato che esiste un elemento “esogeno”, un elemento cioè che non sembra nascere come comportamento emergente o come conseguenza naturale e significativa del sistema (almeno per come lo abbiamo disegnato e stanti le premesse): la CULTURA DELLA SICUREZZA. In altre parole la "Cultura della Sicurezza" è un fattore che dobbiamo considerare pianificato e introdotto nel sistema scientemente, dall’esterno (se mi consentite la licenza dato che non si è mai esterni a un sistema); si tratta di un’inoculazione di informazioni ordinate che altrimenti non emergerebbero spontaneamente dal sistema lasciato a se stesso.

******** Breve nota ********

A voler essere precisi, le cose, da un punto di vista sistemico, starebbero in maniera diversa. L'azione ortodossa, infatti, sarebbe quella di creare le condizioni necessarie e sufficienti (pur sempre con inoculazioni "esterne") affinché il comportamento desiderato emerga spontaneamente perché solo in questo modo possiamo aspettarci che quello stesso comportamento sia incarnato nel

sistema stesso e abbia quindi minori rischi di rigetto. In questo articolo, tuttavia, non abbiamo lo spazio per studiare un simile intervento sociale e culturale poiché andremmo, con tutta evidenza, fuori tempo. Concediamoci perciò anche questa semplificazione e prendiamo ciò che c'è di buono nel grafico.

******** Fine della nota ********

1. Eccoci dunque a una prima semplice indicazione: aziende, scuole, istituzioni devono farsi seriamente carico di formare l'utenza sul tema della cyber security e sulle possibili contromisure, comprese, se non addirittura prima delle altre, quelle di carattere comportamentale (e loro sì in maniera sistemica creando le giuste condizioni!).

2. Il secondo punto inerisce ancora alla cultura della sicurezza ma in questo caso nel senso di "ricerca e innovazione": una soluzione che fosse più semplice da usare, integrabile in tutti i sistemi, che necessitasse di poca manutenzione e che fosse meno vorace in termini di risorse potrebbe affacciarsi sul mercato con un'offerta competitiva, più efficace e meno disincentivante rispetto a quelle cui siamo abituati, troppo spesso appannaggio di grandi strutture che possono destinarvi budget consistenti. Che debba fare il suo lavoro e che mantenga ciò che promette lo do per scontato...

3. Osservando il grafico, si scopre che una riduzione dei prezzi può inopinatamente favorire, alla lunga, la R&S e l'ingresso di nuovi competitor nel mercato, innescando così un circolo virtuoso (a quel punto anche di carattere culturale poiché la competizione si sposterebbe giocoforza su quel terreno liberandoci in parte dalla necessità dell'inserimento "esterno" di cui parlavo).

4. I rovinosi circoli R6 e R6bis. Se sul fronte degli aspetti legislativi sembra che possiamo fare poco, almeno nel breve, dall'altro possiamo invece domandarci se può esistere una soluzione di sicurezza informatica che non alimenti la crescita e lo sviluppo delle tecniche di hacking e cracking o che, almeno, le rallenti di molto. Come ho già accennato qui e in altre occasioni sulla nostra pagina (e temo che avremo modo di dirne ancora), il panorama dell'offerta in tema di sicurezza, pur ampio, è piuttosto piatto; in altre parole le soluzioni proposte sono spesso rivisitazioni o ricombinazioni fantasiose e composite di logiche e tecniche note. Dell'IA, capitolo a parte (e assai scivoloso) non parlo qui: ne abbiamo già parlato in altri post e continueremo a farlo.

La tendenza diffusa rimane però quella del muscle hardening, della stratificazione ad alto livello (quando la scelta più efficiente e sistemica sarebbe invece quella di lavorare al livello OSI più basso possibile) e all'irrobustimento, in chiave analoga, dei dispositivi anti intrusione, il che non aiuta e di certo non cambia le carte in tavola: ci sarà sempre qualcuno con un ariete più forte della blindatura della tua porta! Ecco allora che soluzioni di sicurezza che avessero le caratteristiche tratteggiate al punto 2 cambierebbero anche questa sezione dello scenario.

E il punto di vista diverso?

Nella seconda puntata di questo articolo ho scritto di “una continua rincorsa degli uni sugli altri, un braccio di ferro apparentemente destinato a continuare in eterno, almeno fino a quando ci sarà un terreno [o un portone blindato] che ospiti lo scontro”. Bene, provate a immaginare se non ci fosse più un portone da sfondare, se cioè non ci fosse più quel tipo di terreno a ospitare il solito scontro: una soluzione che spezzasse questo circolo rivoluzionerebbe il sistema!

Ecco, è su questi criteri che LATERALCODE ha concepito, progettato e realizzato iceGate e la tecnologia ZeroSurface®

Conclusione

Come potete immaginare ho scritto questo articolo su un editor di testo: se ora lo state leggendo significa che anche voi siete davanti a un altro schermo, grande o piccolo che sia (se lo avete stampato non siete green).

Bene, ora domandatevi quante delle cose che sapete, che fate e che avete, "passano" attraverso lo schermo di un pc, di uno smartphone, di un tablet. Alcune hanno un’importanza marginale, probabilmente come questo stesso articolo, ma…

...quante di quelle più importanti si trovano depositate, custodite e quindi “affidate” a un computer piazzato in qualche parte del mondo?

Mi riferisco a cose come documenti di proprietà, di identità, dati personali e riservati, email, messaggistica, conti correnti, carte di credito, profili di mercato, credenziali di accesso, documenti della P.A., fiscali, contabili, aziendali e via dicendo: la nostra vita, così come la intendiamo adesso, non è più conservata al sicuro fra le “nostre mura” ma in “casa di altri”, e cioè sui server di tutte le aziende che ce ne forniscono il servizio, che ci permettono l’uso di quei dati e che ci promettono di proteggerli.

Spesso va bene, altre volte no; e quando va male, va male di brutto.

"Sì, ok, ma figurati se deve capitare proprio a me…"

Gianluigi Merlino

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

lateralcode.it