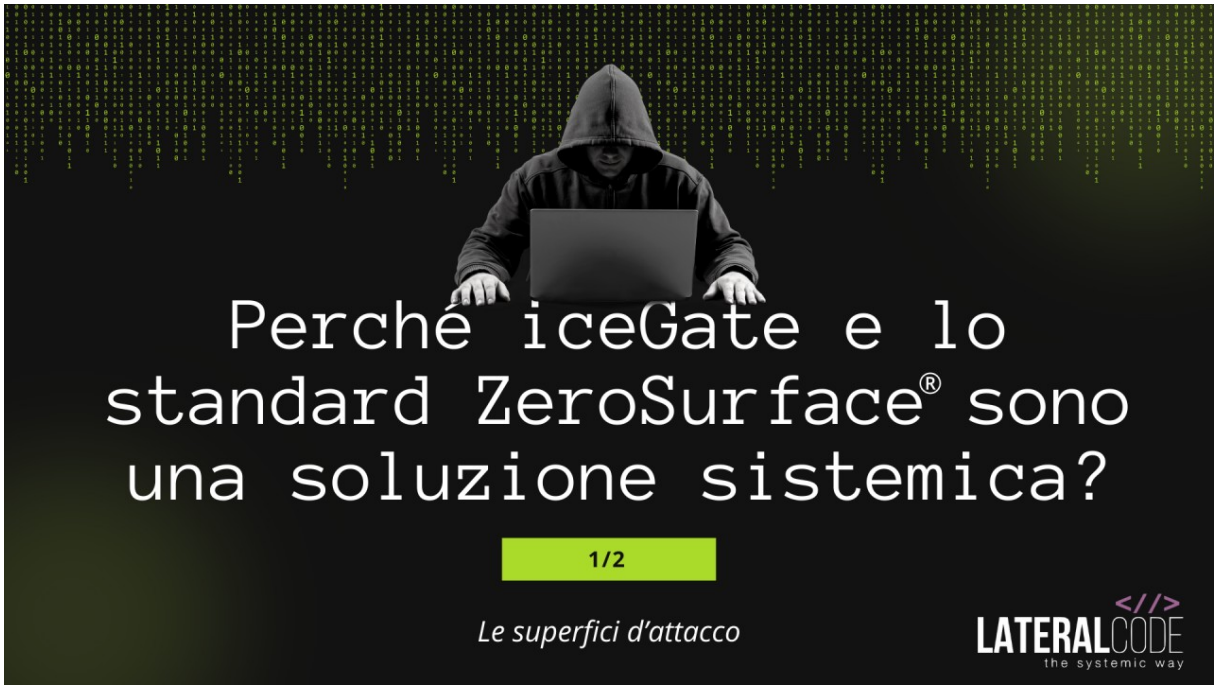
LATERAL NEWS — LATERALCODE

Perché iceGate e lo standard ZeroSurface® sono una soluzione sistemica? (1/2)

29 gennaio 2024



Questo articolo in due parti riprende alcuni dei principi che avete letto nelle edizioni precedenti e ne introduce di nuovi; oltre a ciò, è utile per comprendere ancora meglio come si colloca la tecnologia ZeroSurface® nel panorama della sicurezza informatica di oggi.

Per rispondere alla domanda che fa da titolo è utile iniziare chiarendo in cosa consista, all'interno di un sistema dinamico complesso, una **soluzione fondamentale** (se avete letto gli articoli passati dovreste saperlo): un modo molto semplice di farlo è pensare al suo opposto, ovvero una **soluzione sintomatica**.

Se ho mal di testa o mal di stomaco, spesso ingurgito una pillola e il male passa. Ho curato il problema? Sono guarito? Ovviamente no: ho curato il sintomo, l'ho tamponato, l'ho fatto sparire, ma **la causa primaria del dolore è ancora in giro**, ballonzolante nel mio organismo.

In un sistema dinamico complesso (qual è anche il corpo umano) esistono soluzioni sintomatiche (la pillola) e soluzioni dette **"fondamentali"**, quelle cioè che **affrontano ed eliminano le cause**, anzi, le catene di causa-effetto-causa, che sottostanno alla generazione dei problemi (le fondamenta appunto) le quali si palesano poi attraverso i sintomi.

Come intuite, l'individuazione di soluzioni fondamentali può essere un'attività particolarmente impegnativa, tanto più quanto più è complesso il sistema in esame: per fortuna la **dinamica dei sistemi** e **il pensiero sistemico** ci vengono in soccorso con le loro leggi e i loro strumenti di ricerca e intervento.

Bene, in ambito di sicurezza informatica iceGate e la tecnologia ZeroSurface® affrontano una causa primaria e per questo sono una soluzione sistemicamente fondamentale (per completezza va detto che lo sono anche per altre ragioni di cui abbiamo già parlato e per altre di cui parleremo).

UN PASSO AVANTI

Bene, ma allora che caratteristiche deve avere, tra le altre, una soluzione sistemica?

1. Una soluzione sistemica deve essere **STRUTTURALE** ma anche **ECOLOGICA**. "Con il termine "ecologica" si richiama la **sostenibilità** degli effetti dell'intervento, non soltanto in senso ambientale o naturale. L'adozione di una misura ecologica deve infatti garantire la **conservazione** di quanto già funzionale ed efficiente esista nel sistema a tutti i livelli ed evita quei provvedimenti che, pur centrando l'obiettivo prefissato, abbiano come conseguenza un qualsivoglia danno collaterale. Quando installiamo iceGate non interveniamo mai sull'architettura destinataria della nostra protezione, non modifichiamo mai protocolli o strutture: la rete "cliente" resta esattamente quella che è stata fino a quel momento, solo che diventa sicura.

2. Una soluzione sistemica deve essere **GENERATIVA**. In questo caso l'azione è volta a scoprire "cosa" impedisce al sistema di perseguire un diverso e più favorevole equilibrio: l'operatore agisce cioè per **creare all'interno del sistema in esame le condizioni capaci di generare autonomamente l'effetto complessivo cercato**. Per fare ciò egli non disdegna misure di tipo sottrattivo anziché additivo o integrativo; in altre parole si procede all'eliminazione degli elementi distorsivi o ridondanti piuttosto che introdurre ulteriori regole o nuovi componenti che non farebbero altro che aumentare la complessità totale e l'imprevedibilità. Noi riteniamo che l'eccessiva sovrapposizione di layer e la convivenza e l'integrazione di troppe soluzioni "sintomatiche" all'interno dei sistemi creino una grave **fragilità intrinseca** dovuta al fenomeno delle **emergenze sistemiche**.

3. Una soluzione sistemica deve essere **EVOLUTIVA**. In questo caso, oltre a portare il sistema all'equilibrio desiderato, l'operatore lo conduce a un livello di evoluzione che favorisce condizioni grazie alle quali si autoproteggerà da eventuali ricadute: è per questo motivo che diciamo che **"iceGate è progettato e realizzato per proteggerti anche da minacce future, ancora non scoperte"**. Proseguite nella lettura e vi sarà chiaro il perché.

UN PASSO INDIETRO

In un'edizione di novembre, a proposito della rincorsa sempre in atto tra hacker e sistemi di protezione, leggete: *“Questo ennesimo circolo di rinforzo è davvero distruttivo, 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 che ospiti lo scontro.”*

Ora la domanda è: **qual è questo “terreno di scontro”?** I computer? La rete? I database? Le applicazioni? I firewall? Per certi versi potremmo rispondere “sì” a ogni ipotesi (e in tutta evidenza a molte altre) però non sarebbe una risposta sistemica.

Affinché un malintenzionato possa “entrare” dove non dovrebbe e fare danni è infatti necessario che ci siano **accessi disponibili** (per quanto poi blindati a piacimento con i servizi e le soluzioni che conosciamo come VPN, Strong Authentication, Identity Provider, tunnel di vario tipo e foggia ecc.). Ma il punto è proprio questo. In ciascuna di queste soluzioni esiste SEMPRE una **superficie d’attacco disponibile** il che trasforma i sistemi di sicurezza in **sistemi di speranza**, la speranza cioè che qualcuno non trovi un modo per rompere quelle "catene" e quei "lucchetti". Una differenza sostanziale dunque, tutt’altro che linguistica: **chiamare le cose con il loro nome è il primo passo per prendere decisioni più consapevoli**.

Ci sarà sempre qualcuno con un ariete più forte della blindatura della tua porta.

RITORNO AL FUTURO

Bene, tutto chiaro, tutto teoricamente ineccepibile, ma piuttosto accademico, almeno in apparenza, non trovate? Come possiamo infatti pensare di raggiungere un server se questo non fornisce una qualche visibilità o un qualche ingresso, per quanto dissimulato o protetto? D’altro canto, se così non fosse, non sarebbe neanche “in internet” e quindi di fatto non si porrebbe neppure il problema, ma ciò negherebbe il concetto stesso di rete.

Ebbene, iceGate risolve l‘enigma e vince la sfida dell’apparente illogico: **con lo standard ZeroSurface® è finalmente possibile che un server o una rete siano raggiungibili dall’esterno senza che questi espongano accessi, siano visibili, disponibili o raggiungibili**.

Questo è dunque il primo dei motivi per i quali iceGate, e solo iceGate, può definirsi una **soluzione sistemica fondamentale** al problema della sicurezza perimetrale, poiché sottrae ad attaccanti e difensori il terreno su cui scontrarsi.

Fine dei giochi, andate a giocare da un’altra parte.

TIRIAMO QUALCHE SOMMA

Se è vero che **non esistono accessi da difendere**, non esistono neanche porte e perciò neanche serrature in cui iniettare la colla per fare dispetto al padrone di casa e impedirgli di entrare: avete capito cosa intendo, vero? I danni ai sistemi non sono solo di tipo intrusivo (sicurezza, integrità e riservatezza dei dati) ma anche di indisponibilità dei servizi, come il **DDoS** insomma.

Con iceGate, il DDoS diventa un ricordo polveroso, un mito del passato: riposi in pace anche lui.

Non solo: poiché l'isolamento garantito da iceGate è **bidirezionale** ne consegue che anche le **esfiltrazioni diventano impossibili** e le **backdoor vengono sterilizzate**.

In ultimo (*but not least*), grazie al sistema di **autenticazione asimmetrica a url funzionali** anche il **phishing diviene impossibile**.

Per i miracoli, invece, ci stiamo attrezzando.

Gianluigi Merlino

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

lateralcode.it