Post-Mortem: Analisi di un disservizio di rete autoindotto da filtri perimetrali

Post-Mortem: Analisi di un disservizio di rete autoindotto da filtri perimetrali

Esiste una linea sottile tra la corretta postura di sicurezza informatica e l'eccesso di filtraggio euristico. Questa soglia viene spesso superata all'interno dei firewall perimetrali quando regole di "web reputation" e filtri IP non contestualizzati collidono con le architetture CDN distribuite.

Di seguito viene documentata l'analisi post-mortem di un incidente reale verificatosi all'interno di un'infrastruttura d'ufficio, dove l'isolamento perimetrale ha involontariamente disconnesso i servizi interni essenziali.

La genesi del disastro: "Questo IP ha una brutta faccia"

Tutto inizia con una telefonata o un ticket di prima mattina. "*Non funziona più il Nextcloud interno.*" "*Strano, i server sono su, la RAM è al 20%, i dischi respirano. Da fuori va?*" "*Sì, da cellulare si apre. Da dentro l'ufficio va in timeout.*"

L'analista di turno, armato di `curl -vL` e santa pazienza, fa due verifiche e scopre l'arcano. Il dominio risolve verso un indirizzo IP appartenente a una nota e mastodontica CDN globale (chiamiamola, a caso, *NuvolaDiTempesta*). E quell'IP specifico, da dentro la rete aziendale, risponde solo con un desolante silenzio. I pacchetti partono, ma non tornano indietro.

Perché? Semplice: il sistema di "threat intelligence" del firewall perimetrale ha rilevato che su quell'IP, tre giorni prima, c'era un sito coreano che distribuiva malware. E quindi, con la rapidità e

l'acume di un elefante in un negozio di cristalli, ha messo l'IP in blacklist.

Peccato che quell'IP appartenga a una CDN che gestisce circa il 20% del traffico web mondiale.

Il paradosso delle CDN spiegato ai refrattari

A questo punto si apre il dibattito teologico con i gestori del perimetro. "*Abbiamo bloccato l'IP perché ha cattiva reputazione*", dicono tronfi dall'alto delle loro policy.

Ora, provate a spiegare a questa gente che le CDN funzionano con IP condivisi e dinamici. È come bloccare l'intera autostrada del Sole perché dieci minuti fa è passata una macchina rubata.

- Se blocchi un IP di una CDN, non stai bloccando l'hacker. Stai bloccando anche i tuoi stessi servizi ospitati dietro quella CDN.
- Stai bloccando i portali delle banche che i tuoi dipendenti devono usare.
- Stai bloccando le pagine di documentazione tecnica.
- E soprattutto, domani la CDN assegnerà a quel servizio un altro IP del suo immenso pool, e il blocco diventerà inutile per la sicurezza ma resterà utilissimo per rompere i coglioni.

La risposta standard a questa obiezione di solito è: "*Eh, ma se togliamo il blocco, poi l'hacker ci buca. La sicurezza prima di tutto*".

Sicurezza. Ovvero, l'arte di rendere i sistemi così inutilizzabili che nemmeno gli utenti legittimi possono lavorarci. Il sogno bagnato di ogni sysadmin pigro: un server spento e scollegato dalla rete. Lì sì che il livello di sicurezza è del 100%.

Il delisting fai-da-te e la provocazione politica

Quando la discussione tocca questi livelli di surrealismo, la frustrazione può spingere a risposte estreme.

C'è chi suggerisce che dovresti essere tu, gestore del servizio, ad andare dalla CDN a chiedere il "de-listing" dell'IP. Certo, chiami il

supporto di un colosso da miliardi di dollari per dirgli: "*Senta, scusi, il mio firewall locale ha bloccato un vostro IP a caso, potete cambiarlo?*". Ti ridono in faccia in quindici lingue diverse.

Ed è qui che scatta la mossa disperata: la **provocazione politica**.

Se chi gestisce la rete ti dice che l'unico modo per essere sicuri è blindare tutto fino al blackout, tu gli rispondi con un sorriso: "*Sapete che c'è? Avete ragione. Spostiamo tutti i nostri servizi di sicurezza fuori dal vostro datacenter. Compriamo una bella VPS da venti euro su un provider tedesco e gestiamoci tutto da lì*".

La reazione è immediata. La sola idea che il team di sicurezza decida di scappare all'esterno perché non si fida dell'infrastruttura interna è un siluro politico micidiale. È il crollo della credibilità dell'intero reparto IT.

In pochi minuti, magicamente, le regole del firewall vengono riviste, i blocchi IP degradati a controlli intelligenti e il servizio riprende a funzionare.

Non abbiamo vinto con la logica, né con la tecnica. Abbiamo vinto usando la paranoia del management contro la pigrizia dei sistemisti.

[Che il talpone sia con voi]

Fluxer Icon

Canale di discussione e supporto

Canale di discussione e supporto. Per confrontarti su configurazioni o altro entra su fluxer.dreadful.work (https://fluxer.dreadful.work/invite/dreadful).