Tu pensi in bianco o in nero?

26 febbraio 2025

La sicurezza informatica è una questione di colori. A essere precisi due in particolare, il **bianco** e il **nero**: due modi opposti di affrontare il problema.

NdA: ok, d'accordo, i puristi obietteranno che il nero e il bianco (il primo soprattutto) non sono colori, ma solo espressioni "al limite" della luce, per altro mai pienamente raggiungibili. Se promettete di finire il post prima di allontanarvi, vi mettiamo qui un utile articolo di Adobe sull'argomento: https://shorturl.at/SEp4D (e se lo dice Adobe…).

Dicevamo: due modi opposti di affrontare il problema…

Il **nero**, il dominio del "**black**", è il paradigma classico, quello che l'industria della cyber security ha sempre adottato. Il suo archetipo è la ***blacklist***, con il carico concettuale che si porta dietro, declinato in tutte le soluzioni abituali, anche le più insospettabili.

Il black:

- Osserva ogni accesso
- Analizza i comportamenti
- Confronta ciò che sta accadendo con le minacce conosciute
- Aggiorna le difese, rincorrendo il nuovo attacco

• Decide chi bloccare (sperando di non sbagliare)

Il problema? Questo sistema:

• Blocca solo ciò che è già noto o… ciò che è “sospetto” (sperando di non sbagliare)

• (oppure) Lascia passare il nuovo, finché non diventa noto

• È complesso, costoso, inefficiente.

Nel frattempo, gli attaccanti giocano d’anticipo: cambiano metodo, eludono i controlli, sfruttano i tempi di reazione. La sicurezza basata sul black non protegge, prova solo a contenere i danni.

Poi c’è il **bianco**, il dominio del “**white**”, il paradigma inverso, quello che nella cyber security ha molte meno espressioni (il suo archetipo è la *whitelist*) la più evoluta delle quali è ovviamente lo ZeroSurface®.

Il white:

• Non giudica

• Non filtra

• Non perde tempo con chi sta fuori

• Non insegue le minacce

• Non dialoga con nessuno

Nel dominio del white non c’è… nulla da cui difendersi.

Nel regno del bianco, quindi, non si valuta continuamente chi escludere e non è qualcosa su cui ci sia margine di discussione: o sappiamo già chi sei (e allora, dovunque tu sia, in qualunque momento, prego, accomodati), oppure non puoi neanche avvicinarti, in realtà non puoi neanche trovarci!

Se sei stato autenticato (**dinamicamente** e **ASIMMETRICAMENTE**… qui non si parla di una semplice *whitelist*!), passi. Altrimenti siamo su due diversi piani dell’esistenza: per noi tu non esisti, noi non esistiamo né esisteremo mai per te e non ci sono porte a cui bussare. In ultimo, ricorda che tutto questo vale sia per le persone che *machine to machine*, a diversi livelli, **API** comprese.

■ **Ora, quale delle due sembra una vera sicurezza?**

Essere costretti a **rincorrere gli attaccanti**, oppure rendere il loro lavoro **inutile fin dall’inizio**?

La domanda, alla fine, non è se vuoi una sicurezza più forte, ovvio che tu la voglia!

● **La domanda è: stai ancora pensando in nero?**