Un fattore in più

La NIS2 e ZeroSurface® — Puntata 5 di 7

30 giugno 2026

Per quattro settimane abbiamo letto la NIS2 fermandoci, ogni volta, su un punto preciso. Questa settimana ci fermiamo su una misura che conoscete tutti e che quasi tutti avete già adottato.

L'articolo 21, paragrafo 2, alla lettera j) chiede l'"uso di soluzioni di autenticazione a più fattori o di autenticazione continua". È la misura che in azienda chiamate semplicemente MFA: alla password si aggiunge un secondo fattore, un codice, un'app, un token, un dato biometrico. Un'ottima pratica e la direttiva fa bene a chiederla.

L'autenticazione a più fattori rende più difficile fingersi qualcun altro. Se un attaccante ruba la vostra password, senza il secondo fattore non entra: di fatto un innalzamento reale del costo dell'attacco.

Cosa dice, davvero

L’autenticazione a più fattori e l’autenticazione continua, che la lettera j) mette sullo stesso piano, sono due modi di irrobustire l’accesso. Ma condividono lo stesso presupposto implicito: che ci sia un accesso esposto da irrobustire. Sia che verifichiate l’identità con più fattori all’ingresso, sia che la ricontrolliate di continuo durante la sessione, state comunque lavorando su un varco che resta lì, raggiungibile. Ed è esattamente su questo presupposto che si apre la domanda scomoda.

La domanda scomoda

L’autenticazione a più fattori protegge il momento dell’autenticazione, e fin qui non ci piove. Ma il punto in cui quell’autenticazione avviene rimane lì, esposto, visibile, raggiungibile da chiunque. In pratica state blindando la serratura di una porta che tutti, comunque, possono vedere e raggiungere, e quel che ci faranno, beh....

Sia come sia, una porta raggiungibile, per quanto blindata, resta una porta su cui bussare: si può tempestare l’utente di richieste finché, per sfinimento, ne approva una (MFA fatigue); si può intercettare il codice usa e getta con una pagina civetta; si può colpire il servizio di autenticazione stesso, che è software, e come ogni software ha le sue falle (o, più banalmente, lo si può saturare). Il numero dei fattori non cambia il fatto che il punto d’accesso sia in piazza.

> *Un fattore in più rende più difficile varcare la porta. Ma non la toglie.*

Non basta. In un’architettura tradizionale il punto di autenticazione è sempre riconducibile, in modo diretto o indiretto, al bersaglio che protegge. C'è sempre un filo che lega l’autenticazione all’obiettivo: trovato il primo, si seguono le briciole di Pollicino fino al secondo. Quindi, di nuovo, l’autenticazione a più fattori irrobustisce il primo anello della catena, ma la catena resta.

> *"Serve più una serratura migliore su una porta che tutti vedono o una porta che non è possibile raggiungere?"*

Cosa intende davvero la direttiva

Il punto, perciò, non è scegliere meglio tra le due opzioni della lettera j) perché danno entrambe per scontata una cosa: esiste un varco esposto su cui lavorare.

ZeroSurface®, la tecnologia italiana coperta da brevetto depositato che fa da filo conduttore a questa serie, non si propone come terza tecnica da mettere in fila; e qui non si afferma che chi ha scelto l’MFA abbia sbagliato.

Qui si parla di un altro piano: *ZeroSurface*® elimina il varco su cui quelle tecniche è richiesto che si lavori.

Lo fa in due modi.

1. Tiene il punto di autenticazione lontano dal bersaglio, non al bordo della rete e non riconducibile al sistema protetto, così la catena di briciole si spezza.
2. Rende il bersaglio irraggiungibile.

Va aggiunto, per inciso, che *ZeroSurface*® non rifiuta i fattori multipli, anzi, è esso stesso multifattore. Semplicemente, non si ferma lì.

C'è poi una conseguenza che merita di essere esplicitata per intero.

L'autenticazione continua, contemplata e/o richiesta dalla Direttiva, si realizza di solito come una verifica ripetuta a intervalli durante la sessione: un controllo in più che presuppone, come dicevamo, un varco da presidiare. *ZeroSurface*®, invece, non ripete un controllo ma mantiene una condizione. L'irraggiungibilità del bersaglio non muta mai, in nessuna fase del funzionamento, ma resta identica per tutta la sessione, ovviamente anche mentre i servizi sono in uso. Il livello di sicurezza non cala mai, dal primo istante all'ultimo.

> *L'autenticazione continua si ottiene dalla struttura, non dal presidio continuo.*

Il punto della Puntata 5

L'autenticazione a più fattori è giusta, utile, e la NIS2 fa bene a richiederla. Adottatela. Ma non scambiate una serratura migliore per una casa che non si può trovare. La lettera j) offre due strade per irrobustire l'accesso e tutt'e due danno per scontato che ci debba essere un accesso esposto.

Ma la condizione più solida è quella in cui non c'è MAI un ingresso da difendere.

Lateralcode s.r.l.
