Non potete chiudere una porta che non sapete di avere

La NIS2 e ZeroSurface® — Puntata 4 di 7

23 giugno 2026

Per tre settimane abbiamo letto la NIS2 soffermandoci ogni volta su una o due parole. Questa settimana ci fermiamo su un "elenco" un po' più corposo e, in particolare, su due stralci in cui il legislatore richiama alcuni concetti senza giri troppo intorno.

L'articolo 21, paragrafo 2, è il punto in cui la direttiva elenca le misure minime obbligatorie. Alla lettera e) chiede la *"sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità"*. Tradotto: occuparsi delle vulnerabilità lungo tutto il ciclo di vita di un sistema, non solo quando lo si scrive ma anche quando lo si compra, lo si integra e lo si mantiene.

Poco oltre, la direttiva diventa ancora più esplicita.

Il Considerando 90, Direttiva (UE) 2022/2555, trattando i rischi della catena di approvvigionamento (la famigerata *supply chain*), cita tra i fattori di rischio le ***"vulnerabilità nascoste o backdoor"***. Il legislatore sa che certe falle non sono errori da correggere ma porte lasciate aperte di proposito che arrivano spesso da dove non state guardando: **i componenti che acquistate e i fornitori da cui dipendete.**

Cosa dice, davvero

La direttiva, dunque, non si ferma ai **vostri** sistemi. Il paragrafo 3 dello stesso articolo chiede di **tenere conto delle vulnerabilità specifiche di ogni fornitore** e della qualità complessiva delle sue pratiche di sicurezza, comprese le procedure di sviluppo. E il Considerando 90 arriva a nominare i fattori di rischio **non tecnici**:

- la dipendenza dal fornitore
- il *lock-in* tecnologico
- l'influenza di un paese terzo.

Il messaggio, letto per intero, è particolarmente *sgradevole*:

> *le vulnerabilità potenzialmente più pericolose sono quelle che non avete introdotto voi e che non potete vedere.*

La domanda scomoda

La gestione delle vulnerabilità, così come la pratichiamo di solito, poggia sul presupposto silenzioso che una falla si possa **prima trovare e poi correggere**. Si trova, si valuta e si applica la patch. È (quasi) un buon metodo per le vulnerabilità note ma

1. una *backdoor* è, per definizione, ciò che non vedete e
2. uno *zero-day* è la falla per cui, oggi, una *patch* non esiste ancora.

Peggio: i fatti documentati mostrano che, in certi casi, nemmeno l'aggiornamento basta a sfrattare chi è già entrato e mantiene il proprio accesso (ne abbiamo parlato qui).

> *Il modello **trova-e-correggi** è una rincorsa in cui partite sempre un passo indietro.*

In definitiva: non si corregge ciò che non si conosce e non si chiude una porta di cui si ignora l'esistenza.

Così la domanda diventa: *come si gestisce una vulnerabilità di questo tipo, cioè che*

- ***non si sa di avere***
- ***dentro un componente che non avete scritto***
- ***fornito da chi non controllate?***

Cosa intende davvero la direttiva

L'unica via d'uscita, ci pare evidente, è dunque spostare la domanda e NON *cercare-di-più-sperando-di-trovare*.

> *Possiamo essere d'accordo sul fatto che una vulnerabilità, nota o ignota, vostra o del vostro fornitore, diventa un problema alla sola condizione che esista una via (qualunque) per raggiungere il bersaglio?*

Bene, allora è la **raggiungibilità** a dare alla falla il terreno su cui operare: toglietela, e la falla resta lì, inutile e inutilizzabile.

ZeroSurface®, la tecnologia italiana coperta da brevetto depositato che fa da filo conduttore a questa serie, non promette di trovare le falle che non vedete (lavoro improbo e mal concepito) ma qualcosa di diverso: **rende il bersaglio irraggiungibile.**

Una *backdoor* che nessuno può contattare dall'esterno e che non trova una via per uscire, resta inerte: continua a esistere ma non serve a niente.

Attenzione a non fraintendere. Questo non sostituisce la cura del codice né la verifica dei fornitori che la direttiva continua giustamente a richiedere, rimuove però la precondizione che **trasforma una falla nascosta in una violazione**. Ed è proprio l'effetto che il Considerando 90 insegue quando si preoccupa di *backdoor* e dipendenza dai fornitori: **rendere quei rischi ininfluenti invece di doverli scovare a uno a uno**.

> *Una difesa non deve conoscere ogni minaccia per renderla inoffensiva: le basta togliere il terreno su cui la minaccia si muove.*

Il punto della Puntata 4

La NIS2 chiede di gestire le vulnerabilità e di sorvegliare la catena di approvvigionamento, fino alle *backdoor* nascoste nei prodotti che comprate. È giusto e necessario, e va fatto. Ma c'è una differenza tra rincorrere ogni falla, nota e ignota, e rendere irrilevante il fatto stesso che esista. La direttiva chiede la prima cosa. Non vieta la seconda ma, semmai, a saperla leggere, la indica.

Certo, non sapeva che **oggi è tecnicamente possibile** ma a colmare questa potenziale lacuna ci ha pensato nel passaggio sullo "*stato dell'arte*" (Considerando 81) di cui abbiamo parlato la scorsa settimana.

Lateralcode s.r.l.
