La sicurezza fin dalla progettazione

La NIS2 e ZeroSurface® — Puntata 7 di 7

14 luglio 2026

La settimana scorsa abbiamo separato due condizioni che vengono spesso confuse: "fidarsi di meno" e "non averne bisogno". Lo zero trust e la segmentazione, infatti, hanno a che fare con intrusi che sono già dentro o a ridosso di un perimetro raggiungibile; **ZeroSurface®** toglie la raggiungibilità a monte, e buonanotte ai suonatori.

> *“Perciò combattere e vincere cento battaglie non è prova di suprema eccellenza: la suprema abilità consiste nel piegare la volontà del nemico senza combattere.” - Sun Tzu*

Con questa puntata chiudiamo la serie "La NIS2 e ZeroSurface®" tornando dove eravamo partiti: azzerare la superficie ma fin da subito...

Cosa dice davvero

La NIS2 non impone a tutti i soggetti un obbligo generale e uniforme di sicurezza fin dalla progettazione, il famoso *secure by design*. La locuzione esplicita **compare in due considerando** ben delimitati, entrambi rivolti ai fornitori di comunicazione elettronica: il Considerando 104, Direttiva (UE) 2022/2555 (NIS2), afferma che *"I fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico dovrebbero attuare la sicurezza fin dalla progettazione e per impostazione predefinita"*; il Considerando 98, resta nello stesso ambito quando richiama i *"principi di sicurezza e tutela della vita privata per impostazione predefinita e fin dalla progettazione"*, accanto a concetti di sicurezza incentrati sui dati come la cartografia, la segmentazione, la marcatura, la politica di accesso e la gestione degli accessi.

Per l'insieme dei soggetti essenziali e importanti, invece, il principio che regge l'intera architettura della direttiva è un altro, ed è quello del **Considerando 105**: *"Un approccio proattivo alle minacce informatiche è una componente essenziale delle misure di gestione dei rischi di cybersicurezza"*. Proattivo, non reattivo (prendiamolo con la stessa intenzione di come è stato scritto benché, sistemicamente, la proattività non esista).

È la stessa direzione che il Regolamento di esecuzione (UE) 2024/2690 **traduce in requisito** di sviluppo sicuro per i soggetti pertinenti, quando al punto 6.2.2, lettera b), chiede di *"applicare principi per la creazione di sistemi sicuri e principi di programmazione sicura a tutte le attività di sviluppo dei sistemi informativi, quali la promozione della cybersicurezza fin dalla progettazione e delle architetture zero trust"*.

La domanda scomoda

Ora mettiamo in fila le due cose, con una precisazione necessaria. La locuzione *"sicurezza fin dalla progettazione"* resta un obbligo confinato ai fornitori di comunicazione elettronica dei Considerando 98 e 104: per tutti gli altri soggetti non è che valga in versione più debole, semplicemente non compare.

Quello che vale per tutti è altro, con un proprio fondamento testuale che punta però nella stessa direzione:

- l'approccio proattivo del Considerando 105
- l'impianto generale di gestione del rischio dell'articolo 21
- il rinvio alla protezione dei dati fin dalla progettazione del GDPR, richiamato dal Considerando 51 a proposito dell'uso di tecnologie innovative come l'IA nella cibersicurezza

Tre vie autonome, non un'eco indebolita delle prime due. E allora la domanda è questa: *quando la direttiva, nel suo complesso, chiede un approccio proattivo alla gestione del rischio, sta chiedendo un impianto pensato così fin dall'origine, o un controllo aggiunto sopra un*

bersaglio che, di suo, resta raggiungibile?

Cosa intende davvero la direttiva

“Fin dalla progettazione” non è un prodotto da installare né un livello da sovrapporre ma è **una proprietà di come il sistema è pensato**, decisa nel momento in cui il sistema viene disegnato e non alla fine, a esposizione già avvenuta. Non è un caso che la stessa direttiva, al Considerando 51, rinvii esplicitamente ai *"requisiti di protezione dei dati fin dalla progettazione e predefiniti di cui al regolamento (UE) 2016/679"*, chiedendo che siano **"pienamente rispettati"**. Il “fin dalla progettazione” del GDPR e quello della NIS2 appartengono alla stessa famiglia: la sicurezza e la protezione dei dati come **conseguenza dell'architettura**, non come rammendo applicato dopo. La direzione dell'intera direttiva, dalla gestione dei rischi dell'articolo 21 ai concetti incentrati sui dati del Considerando 98, è questa: spostare la sicurezza dal dopo al prima.

> *“Fin dalla progettazione” non è un prodotto da installare né un livello da sovrapporre ma è una proprietà di come il sistema è pensato, decisa nel momento in cui il sistema viene disegnato e non alla fine a esposizione già avvenuta.*

Il punto della Puntata 7

ZeroSurface®, la tecnologia italiana coperta da brevetto depositato che fa da filo conduttore a questa serie, è quella direzione portata al suo limite: ***l'irraggiungibilità non è un controllo che si possa aggiungere a un bersaglio esposto ma è una proprietà strutturale del disegno.***

Il target non è filtrato o nascosto ma semplicemente non esiste, non è un riferimento raggiungibile: questa è sicurezza fin dalla progettazione nel senso più letterale possibile, **perché la sicurezza non viene dopo l'architettura: coincide con essa!**

Lo si vede nel modo in cui in **ZeroSurface®** l'informazione è distribuita. Nessun nodo è unico o centrale, nessun nodo è direttamente riconducibile a un altro, nessun nodo contiene mai informazioni complete. Ogni nodo custodisce solo frammenti non parlanti, non significativi e non riconducibili né a clienti né a utenti. La violazione di un singolo nodo non restituisce dati sensibili perché in quel nodo non c'è nulla di ricomponibile o riferibile. La sicurezza, così, è intrinseca al sistema stesso: è garantita dalla sua architettura, dal suo *design*, appunto.

È lo stesso principio evocato dal Considerando 98 portato però fino alla minimizzazione strutturale: nemmeno i sistemi di Lateralcode associano le credenziali agli utenti poiché non ne hanno bisogno.

> La sicurezza non viene dopo l'architettura: coincide con essa!

E qui la serie si chiude dove si era aperta. All'inizio, eravamo partiti da un'osservazione della direttiva stessa, al Considerando 96, Direttiva (UE) 2022/2555 (NIS2), secondo cui *"la superficie di attacco continua ad ampliarsi"*. Puntata dopo puntata abbiamo letto le misure della NIS2 come modi diversi di difendere meglio quella superficie, fino a oggi, dove affermiamo che la forma più radicale della *"sicurezza fin dalla progettazione"* è progettare un sistema che una superficie da difendere non ce l'ha. **ZeroSurface®** fa esattamente questo: rende il bersaglio strutturalmente irraggiungibile. Non sostituisce lo sviluppo sicuro né gli obblighi della direttiva **ma ne è l'espressione più conseguente.**

Togliere la superficie, non irrobustirla.

Lateralcode s.r.l.

Con questa puntata la serie "La NIS2 e ZeroSurface®" si chiude. Torneremo con un'appendice riepilogativa che mette in fila le minacce neutralizzate da questa architettura e le collega, una a una, ai considerando della direttiva da cui siamo partiti.
