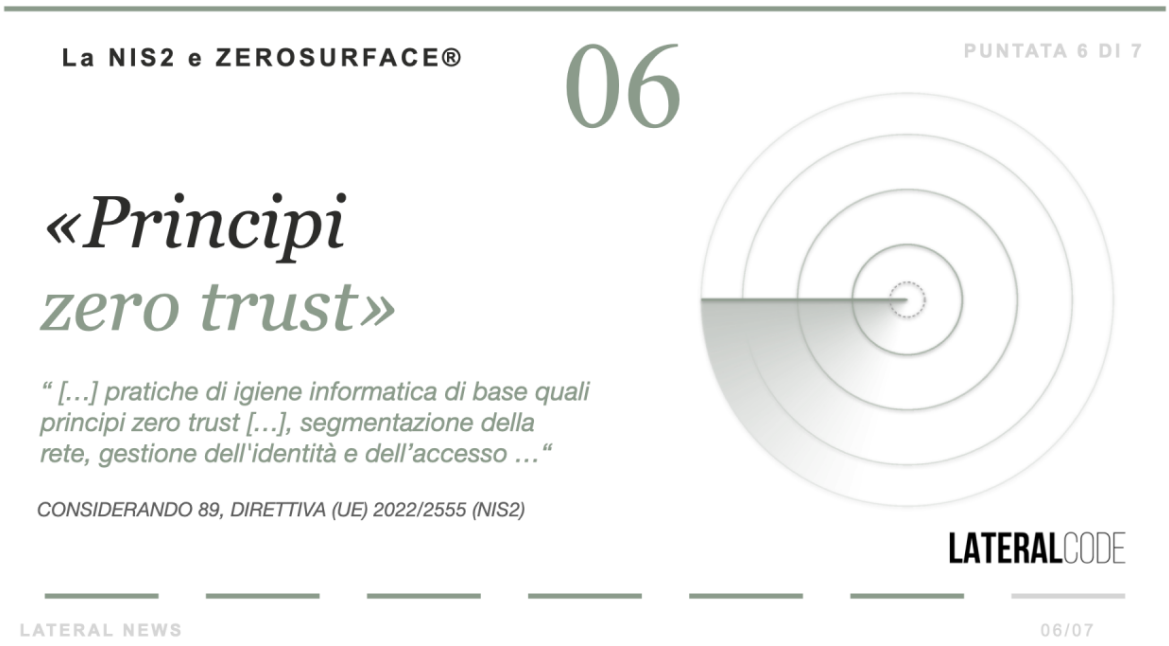
Non fidarsi di nessuno non basta se tutti possono bussare

La NIS2 e ZeroSurface® — Puntata 6 di 7

7 luglio 2026



Per cinque settimane abbiamo letto la NIS2 fermandoci su un punto per volta; questa settimana ci fermiamo su due termini che la direttiva scrive esattamente come li conoscete: **zero trust** e **segmentazione**.

L'articolo 21, paragrafo 2, alla lettera g) chiede *"pratiche di igiene informatica di base e formazione in materia di cibersicurezza"*. Cosa siano quelle pratiche lo precisa il Considerando 89 che elenca i *"principi zero trust"* e la *"segmentazione della rete"* accanto ad *aggiornamenti del software, gestione dell'identità e dell'accesso, formazione del personale...*

Ora fermatevi un istante su tre parole: **pratiche di base**. Il legislatore non colloca lo *zero trust* in cima all'edificio della sicurezza ma lo mette alle fondamenta, tra le cose che si danno per acquisite, cioè un punto di partenza; è un giudizio che merita **attenzione**, perché lo *zero trust* viene spesso raccontato come l'approdo, come il traguardo di una strategia. **E invece la Direttiva lo tratta come il punto di partenza.**

E guardate che non è una lettura isolata: il regolamento di esecuzione (UE) 2024/2690, che dettaglia i requisiti tecnici delle misure per alcune categorie di soggetti, colloca di nuovo i

principi *zero trust* e la segmentazione della rete tra le pratiche di **igiene di base**. La stessa collocazione, quindi, **ma ribadita da un atto tecnico e vincolante.**

Cosa dice, davvero

Lo *zero trust* è, in sostanza, "solo" un principio: *non fidarti di nessuno, verifica sempre, non concedere fiducia per il solo fatto che una richiesta arrivi dall'interno del perimetro, controlla ogni accesso ogni volta.*

La segmentazione, a ben vedere, ne è la controparte architetturale: *dividi la rete in zone così che una compromissione in un settore non dilaghi negli altri.* È una buona disciplina e la direttiva fa bene a metterla tra le fondamenta.

Ma guardate cosa danno per scontato, tutt'e due: **presuppongono un sistema che resta raggiungibile, sul quale si dispongono controlli per verificare ogni richiesta e contenere ciò che passa.**

Lo *zero trust*, per dirla semplice, ti dice di diffidare di ogni bussata, ma la bussata può comunque arrivare. La segmentazione, poi, limita gli spostamenti ma le zone restano raggiungibili al loro interno. Si è dunque passati dal fidarsi "del dentro" al non fidarsi di nessuno ed è un progresso reale, innegabilmente; il mondo, però, può ancora bussare **e le giornate si spendono a verificare ogni bussata e a contenere ciò che entra.**

La domanda scomoda

Ora prendiamo sul serio il principio *"non fidarsi di nessuno"* e portiamolo fino in fondo: ***se davvero non ci si fida di nessuno, perché tenere una porta che tutti possono raggiungere per poi doverne diffidare, verificarla e contenere ciò che la attraversa?***

> *La forma più compiuta della sfiducia non è controllare ogni bussata: è una porta che l'estraneo non può nemmeno raggiungere per bussare.*

E allora cosa è più coerente con il *"non fidarsi di nessuno"*?

Cosa intende davvero la direttiva

La direttiva mette lo *zero trust* tra le fondamenta perché è, appunto, **la disciplina della sfiducia**, preziosa e da acquisire, e quindi diventa importante quel che si costruisce sopra quelle fondamenta.

ZeroSurface®, la tecnologia italiana coperta da brevetto depositato che fa da filo conduttore a questa serie, porta il principio della sfiducia alla sua **conseguenza strutturale**. Un sistema ZeroSurface® tiene, per costruzione, l'intero mondo in blacklist, in qualunque stato operativo si trovi: nessuno è ammesso e il bersaglio resta irraggiungibile anche mentre gli utenti autorizzati stanno operando. Non è una fiducia negata di continuo, richiesta dopo richiesta, ma

un’assenza di fiducia intrinseca alla struttura che quindi non va presidiata perché è condizione stessa del sistema.

Vale anche per la segmentazione perché segmentare serve a limitare il movimento laterale, cioè a contenere chi è già entrato. ZeroSurface® **agisce prima**: se il bersaglio non è raggiungibile, il movimento laterale non ha da dove cominciare perché manca l’ingresso da cui propagarsi. Attenzione: questo non abolisce lo *zero trust* né la segmentazione, e non sono approcci in conflitto che anzi possono lavorare nella stessa squadra.

Ma tra i due c’è un’asimmetria che occorre rendere esplicita. **ZeroSurface®** mantiene la propria promessa (*"il bersaglio non esiste"*), indipendentemente dal fatto che sopra vi si applichino o meno principi *zero trust*. Lo *zero trust* invece, per mantenere la propria (*"non fidarsi di nessuno"*) non dovrebbe interagire con nessuno che non fosse autenticato ***prima***, altrimenti **resta una superficie su cui la fiducia si negozia ogni volta**, verifica dopo verifica, e una superficie negoziabile non è mai *fiducia zero*, è solo *fiducia ridotta*.

> *Detta altrimenti: ZeroSurface® può fare a meno dello zero trust e restare comunque ciò che promette di essere. Lo zero trust, per diventare compiutamente ciò che promette di essere, ha bisogno di ZeroSurface®.*

Ed è anche per questo che in un impianto a superficie zero molto di ciò che lo *zero trust* deve verificare senza sosta, e molto di ciò che la segmentazione deve contenere, **semplicemente non si presenta.**

> *Lo zero trust è una sfiducia da mantenere ogni momento. ZeroSurface®, la superficie zero, è una sfiducia che non ha bisogno di essere mantenuta.*

Il punto della Puntata 6

La NIS2 mette lo *zero trust* e la segmentazione tra le pratiche di base ed è il posto giusto: sono le fondamenta, non il tetto. Adottarle è sano e va fatto, ma le fondamenta pongono una domanda su ciò che vi si costruisce sopra. Se il principio è non *"fidarsi di nessuno"* la sua forma più compiuta non è verificare ogni estraneo che si presenta ma è fare in modo che l’estraneo non possa presentarsi. **La direttiva chiede la disciplina della sfiducia: la sua conseguenza più piena è una sfiducia che diventi struttura.**

Lateralcode s.r.l.
-- Martedì prossimo la 7ª e ultima puntata --
