

La superficie d'attacco

La NIS2 e ZeroSurface® — Puntata 1 di 7

2 giugno 2026

La NIS2 e ZEROSURFACE®

01

PUNTATA 1 DI 7

La superficie d'attacco

"La superficie d'attacco continua a espandersi."

CONSIDERANDO 96, DIRETTIVA (UE) 2022/2555 (NIS2)



LATERALCODE

LATERAL NEWS

01/07

Considerando 96, Direttiva (UE) 2022/2555 (NIS2)

Quattro parole.

Stanno nel *Considerando 96 della Direttiva (UE) 2022/2555*, la NIS2, quasi a metà del preambolo, in mezzo a centinaia di paragrafi su settori critici, soggetti essenziali, autorità competenti, obblighi di notifica ecc. Se le leggete velocemente passano inosservate ma se le rileggete, cambiano peso:

"La superficie d'attacco continua a espandersi."

Non è un'opinione tecnica né un'osservazione di mercato: è una **constatazione del legislatore europeo**, scritta nera su bianco in un atto vincolante. Noi crediamo che stia dicendo qualcosa che ritiene strutturale al problema e che la direttiva vuole affrontare.

Cosa significa davvero

La superficie d'attacco è la somma di tutti i punti di un sistema che un attaccante può **tentare di toccare**. Porte aperte, endpoint esposti, servizi raggiungibili, interfacce di gestione, API pubbliche, gateway, VPN, terminali, dispositivi IoT, oggetti che parlano con altri oggetti: ogni *cosa che esiste e che è raggiungibile* è una porzione di superficie d'attacco.

Più cose esistono, più la superficie cresce. Più la superficie cresce, più aumenta la probabilità che almeno uno di quei punti sia vulnerabile, oggi o tra sei mesi, a una tecnica nota o a una ancora non scoperta.

Il legislatore, dicevamo, ne prende atto. E nello stesso Considerando aggiunge un esempio: *“i servizi di comunicazione interpersonale indipendenti dal numero, come i servizi di messaggistica, stanno diventando vettori di attacco diffusi”*. Traduzione: ogni volta che inventiamo un nuovo modo di far comunicare due endpoint, abbiamo creato un nuovo pezzo di superficie. E la stiamo creando più velocemente di quanto riusciamo a proteggerla.

Badate bene, questa non è solo un'istantanea: è un processo in corso. La direttiva non chiede di *“fermare l'espansione”* ma piuttosto di costruirci sopra una postura (no dai, *“postura”* no, non si può sentire!) di sicurezza adeguata.

La domanda scomoda

Ecco il punto che, secondo noi, viene troppo spesso eluso.

Se la superficie d'attacco continua a espandersi, la cyber security contemporanea sta affrontando il problema giusto?

Il modello dominante è semplice.

- Aumenta la superficie? Più layer di difesa.
- Più endpoint? Più agent.
- Più ingressi? Più firewall.
- Più traffico? Più sonde di rilevamento.
- Più rete? Più segmentazione.
- Più utenti? Più MFA.

È una corsa armata e la direzione di marcia è chiara: ogni anno spendiamo di più per difendere una superficie che va sempre più ingrandendosi.

C'è una scuola di pensiero che dice: *“Questa è la normalità, è il prezzo del progresso digitale, da pagare per essere connessi”*.

Ma c'è anche un'altra scuola, la nostra, che dice qualcosa di essenziale:

“se la curva delle minacce cresce più velocemente di quella delle difese, e tutto fa pensare che sia esattamente quanto accade, allora non stiamo perdendo qualche battaglia (sempre più spesso) ma stiamo combattendo la guerra sbagliata.”

Davvero vi domandate ancora **“come posso proteggere meglio la mia superficie d’attacco”**? Perché non vi chiedete invece: **“Deve necessariamente esistere”**?

Cosa cambia se la superficie non c’è

Immaginate un sistema irraggiungibile per chi non è autenticato. Non “protetto”, non “nascosto dietro un firewall”, ma “irraggiungibile”. **Irraggiungibile** nel senso letterale del termine. Una porta che non solo è chiusa ma che non esiste. Pensate a una scansione di rete che restituisca sempre “*host seems down*” anche mentre un utente legittimo sta lavorando dentro il sistema... **e anche se fatta da quello stesso utente!**

*In un sistema così, le quattro parole del Considerando 96 cambiano natura. La superficie d’attacco non si espande. Non perché qualcuno la stia comprimendo ma perché, per definizione, non esiste finché qualcuno autorizzato **non la istanzia temporaneamente** per sé e solo per uno specifico compito.*

Questa non è teoria.

Esiste una tecnologia che lo fa, ed è italiana. Si chiama **ZeroSurface[®]**, è coperta da brevetto depositato ed è il filo conduttore di questa serie. Ne parleremo meno come prodotto e più come **logica architettonica**, perché è soprattutto questo o dovrebbe diventarlo per tutti voi.

Il punto della puntata 1

Le strategie attualmente dominanti accettano come inevitabile questa espansione delle superfici e si limitano a inseguirla. La NIS2 chiede misure **proporzionate allo stato dell’arte** ma, ATTENZIONE:

*lo stato dell’arte non è ciò che fanno tutti o che il mercato è abituato a propinarci ma è ciò che **OGGI È POSSIBILE FARE**.*

E una delle cose che oggi è possibile fare, **e che fino a pochi anni fa non era nemmeno concettualizzata**, è far smettere alla superficie d’attacco di esistere.

Ma se è possibile, allora un’architettura ZeroSurface[®] è una delle opzioni in tabella e, anzi, è il punto di partenza. E se è in tabella, va valutata. A questo punto ecco l’altra domanda:

“Se è valutabile e non la sto valutando, sono conforme?”. O meglio: “Sono conforme alla migliore conformità disponibile o alla conformità che il mercato mi propone di acquistare da sempre?”

Lateralcode srl
