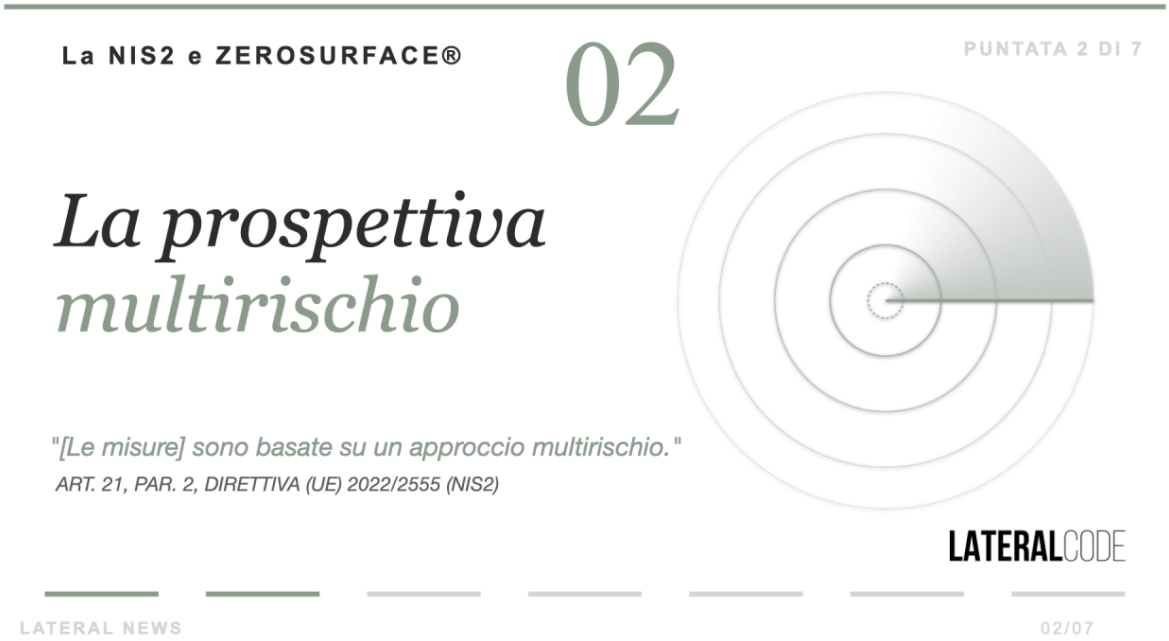
Tutti i rischi, non uno alla volta

La NIS2 e ZeroSurface® — Puntata 2 di 7

9 giugno 2026



La settimana scorsa abbiamo letto quattro parole. Questa settimana ne leggiamo due: "*approccio multirischio.*"

Stanno nell'articolo 21, paragrafo 2, della Direttiva (UE) 2022/2555 (la NIS2, per gli amici) nel punto in cui la direttiva smette di descrivere e comincia a prescrivere. È l'incipit dell'elenco delle misure obbligatorie:

> *"Le misure di cui al paragrafo 1 sono basate su un approccio multirischio mirante a proteggere i sistemi informatici e di rete e il loro ambiente fisico da incidenti."*

"Approccio multirischio" è la traduzione ufficiale italiana dell'espressione inglese "*all-hazards approach*". E *all-hazards* significa, letteralmente, tutti i rischi: non solo gli attacchi informatici malevoli, ma anche errori umani, guasti sistemici, eventi fisici, interruzioni di alimentazione, accessi non autorizzati. La direttiva lo dice esplicitamente nello stesso paragrafo, citando l'ambiente fisico dei sistemi accanto ai sistemi stessi.

Cosa significa, davvero

Il legislatore non si ferma qui. Nel Considerando 78, Direttiva (UE) 2022/2555, aggiunge un passaggio che pesa: le misure di gestione del rischio ***"dovrebbero prevedere un'analisi sistemica, tenendo conto del fattore umano, onde avere un quadro completo della sicurezza del sistema informatico e di rete"***.

Mettete insieme le due richieste.

Da un lato, tutti i rischi. Dall'altro, **un'analisi sistemica** che restituisca un quadro completo. Non è una coincidenza: sono due facce dello stesso principio. Il legislatore non vuole che si affronti una minaccia alla volta. Vuole che si guardi al **sistema** come a un tutto unico, e che **lo si protegga in quanto tale**.

È una richiesta apparentemente ovvia. È, in realtà, il punto più disatteso dell'intera direttiva.

La domanda scomoda

Il modello dominante della cyber security **è l'esatto contrario di un approccio sistemico**: è un approccio additivo. Una minaccia, uno strumento.

- Malware? Antivirus.
- Traffico ostile in rete? Firewall.
- Saturazione del servizio? Anti-DDoS.
- Attacco applicativo? WAF.
- Endpoint compromesso? EDR.

Ogni layer risponde a un rischio. La somma dei layer dovrebbe, nelle intenzioni, coprire "tutti i rischi".

> *Ma la somma di tante risposte parziali non è un approccio sistemico: è una pila.*

E le pile hanno due problemi.

1. Il primo è che ogni *layer* copre il rischio per cui è stato progettato, e nulla più (ciò che cade tra due layer non è coperto da nessuno).
2. Il secondo è ancora più insidioso: **ogni layer aggiunto aumenta la complessità, e la complessità è essa stessa un rischio**. Più strumenti significano più configurazioni, più integrazioni, più superfici, più punti di rottura, più comportamenti emergenti. **A un certo punto, la difesa diventa parte del problema che dovrebbe risolvere**.

Allora la domanda è:

> *una pila di strumenti “monorischio” può davvero soddisfare un requisito che chiede tutti i rischi e un’analisi sistemica? O è strutturalmente, per come è fatta, una collezione di risposte parziali che si spaccia per un tutto?*

Cosa fa, invece, un approccio sistemico

Partiamo da una prima distinzione d’obbligo. L’approccio multirischio della NIS2 abbraccia anche il mondo fisico (incendi, inondazioni, guasti elettrici, accessi non autorizzati ai locali) e su quel fronte la risposta giusta è fatta di estintori, ridondanza, gruppi di continuità, vigilanza, controllo degli accessi ecc. Nessuna tecnologia di rete vi protegge da un allagamento, e sarebbe disonesto sostenere il contrario.

Ma la quota più grande, più dinamica e più imprevedibile di quel ventaglio di rischi non vive nei locali: vive sulla rete. E lì arriva la vera domanda: **come si protegge ciò che, semplicemente, può sempre essere raggiunto?**

> *Un approccio sistemico non aggiunge una difesa per ogni minaccia di rete ma **cambia la condizione che le rende tutte possibili**. È una differenza di natura, non di grado.*

Prendete la categoria più ampia di questi rischi vale a dire **tutto ciò che richiede, per concretizzarsi, che qualcuno possa raggiungere il bersaglio**: intrusione, esfiltrazione, movimento laterale, saturazione, sfruttamento di vulnerabilità note e ignote, perfino l’errore umano e l’azione malevola, che il Considerando 79 elenca tra i rischi, hanno quasi sempre bisogno della raggiungibilità per fare danno. Sono minacce diverse, con strumenti di difesa diversi nel modello a pila. **Ma condividono un’unica precondizione: che il bersaglio sia raggiungibile.**

> *Rimuovete quella precondizione, e l’intera categoria collassa in un colpo solo, non perché ogni minaccia sia stata contrastata individualmente, ma perché è venuto meno ciò che le accomunava.*

Vale anche per un rischio che la NIS2 mette nero su bianco nello stesso articolo 21: **la sicurezza della catena di approvvigionamento** (Art. 21, par. 2, lett. d). Un fornitore compromesso, un aggiornamento avvelenato, un servizio gestito violato sono vettori che, per colpirvi, devono comunque raggiungere il vostro sistema. **Se il sistema non è raggiungibile, il vettore non ha dove arrivare**. Ma su questo torneremo in un’altra puntata.

Questo è ciò che intende il legislatore quando chiede un’analisi sistemica: guardare a ciò che i rischi hanno *in comune*, non trattarli uno per uno.

ZeroSurface®, la tecnologia italiana, coperta da brevetto depositato, che fa da filo conduttore a questa serie, è esattamente questo: **una logica che agisce sulla struttura, non sui sintomi.**

Rende il bersaglio irraggiungibile e così facendo **neutralizza in un'unica mossa una categoria di rischi che il modello a pila affronta con dieci strumenti diversi.**

Il punto della Puntata 2

L'articolo 21, paragrafo 2, chiede un approccio **multirischio**. Il Considerando 78 chiede un'**analisi sistemica** (praticamente un ossimoro, ma transeat...) per un quadro completo. Due richieste, una direzione: **guardare alle cause, al sistema, non ai sintomi.** Il mercato, però, non sostiene questa cultura: sviluppa e vende soluzioni sintomatiche.

La domanda che ogni soggetto NIS2 dovrebbe porsi è dunque:

> *"la mia difesa è sistemica o è solo una pila molto alta di risposte parziali?"*

Perché "*all-hazards*" non è la somma di tanti rischi affrontati separatamente. E la direttiva, a saperla leggere, lo dice con chiarezza.

— Lateralcode s.r.l.

Martedì prossimo la 3a puntata - Continueremo a leggere la NIS2 due volte: prima nella sua lettera, poi nelle sue conseguenze.
