La NIS2 e ZeroSurface® — Appendice

22 settembre 2026



Il rientro dalle ferie non fa sconti a nessuno.

Il decreto legislativo 4 settembre 2024, n. 138 (e le successive determinazioni ACN), che ha recepito la NIS2 in Italia, fissa a diciotto mesi dalla notifica di inserimento nell'elenco dei soggetti NIS il termine per la piena operatività delle misure di sicurezza di base. Per la maggior parte dei soggetti notificati tra marzo e aprile 2025 quel termine cade a ottobre 2026. **Signori, il mese prossimo!**

Non è un dettaglio amministrativo tra i tanti che ci ammorbano ma la scadenza in cui le buone intenzioni maturate durante l'anno diventano, oppure no, misure operative **dimostrabili**. Ed è anche il momento in cui torna utile **l'appendice che avevamo promesso** chiudendo la serie: una mappa che mette le sei minacce da cui una “difesa” deve proteggerci a fianco dei punti della NIS2 che le nominano.

> Sei voci, quelle che nel nostro materiale ricorrono da sempre, quelle da cui **ZeroSurface®** mette al riparo: *intrusione nei sistemi, DDoS, minacce future e 0-day, esfiltrazioni e backdoor, attacchi supply chain, phishing.*

Una sola precondizione

Ormai dovreste saperlo (e se non lo sapete, mooolto male): c'è un filo che le tiene insieme e lo abbiamo tirato in ballo già nella seconda puntata intitolata **"La prospettiva multirischio"**. Sono minacce diverse (ciascuna destinata al proprio strumento di difesa, se consideriamo un modello a pila) ma tutte, per fare danno, **hanno bisogno della stessa cosa**: che il bersaglio sia raggiungibile. È la precondizione che accomuna categorie altrimenti lontane: eliminatela e non dovrete più contrastare una minaccia alla volta poiché verrà meno il terreno su cui l'intero gruppo si muove.

È in questa chiave, e non su una promessa di invulnerabilità, che va misurato quanto segue, che poi è anche la lettura che rende operative e non solo cartacee le misure che il termine di ottobre chiede di dimostrare.

Ed eccole qua le sei minacce, una a una...

Intrusione nei sistemi

È il caso base, quello da cui la serie è partita. Il Considerando 96, Direttiva (UE) 2022/2555 (NIS2), osserva che *"la superficie di attacco continua ad ampliarsi"*: più servizi esposti, più vie per entrare. Qui è tutto molto intuitivo: un tentativo di accesso non autorizzato ha sempre bisogno di una via per arrivare al sistema. Bene, **ZeroSurface®** non irrobustisce la difesa di quella via ma la **rimuove**: obiettivo non raggiungibile e fine della storia *(ovvio, il servizio continua a funzionare per chi deve, altrimenti dove sarebbe il bello?)*.

DDoS

Qui è facile fraintendere. Il Considerando 79, Direttiva (UE) 2022/2555 (NIS2), colloca tra i beni da proteggere *"la disponibilità ... dei servizi offerti"*. Un attacco volumetrico che satura la banda a monte è un problema di capacità della rete e naturalmente **ZeroSurface®** non si occupa di questo (e non ne ha bisogno). Ciò che fa è un'altra cosa: **rende il servizio protetto non indirizzabile né raggiungibile**. La sua disponibilità non dipende dall'assorbire l'attacco ma dal fatto che l'attacco non trova un bersaglio a cui rivolgersi.

Minacce future e 0-day

L'articolo 21, paragrafo 2, lettera e), chiede la sicurezza dello sviluppo e "*la gestione e la divulgazione delle vulnerabilità*". Tutto giusto ma una vulnerabilità ignota è, per definizione, quella per cui oggi non esiste neanche una correzione: come dire, non puoi "chiudere una porta" di cui ignori l'esistenza. **ZeroSurface®** non si mette in cerca delle falle che nessuno ha ancora trovato (ancora una volta: non ne ha bisogno) ma **toglie la precondizione che le rende sfruttabili**: tutta un'altra storia. Una falla, nota o ignota, diventa una violazione solo se esiste una via per raggiungerla. Se quella via non c'è la falla può anche restar lì, inutilizzabile: la "*patcheremo*" poi con calma (o magari no, tanto non cambia nulla).

Esfiltrazioni e backdoor

Il Considerando 90, Direttiva (UE) 2022/2555 (NIS2), mette tra i rischi non tecnici le "*vulnerabilità nascoste o backdoor*". Una *backdoor* è, per definizione, ciò che non vedete. **ZeroSurface®** non la scova (indovinate un po? tanto per cambiare non ne ha bisogno) ma la rende inerte. In l'isolamento bidirezionale, una *backdoor* che dall'esterno nessuno può contattare e che non trova una via per uscire continua a esistere ma non serve a niente. Va da sé, dunque, che ciò vale anche per l'esfiltrazione, che è la violazione della "*riservatezza dei dati*" richiamata dal Considerando 79.

Attacchi supply chain.

L'articolo 21, paragrafo 2, lettera d), impone la "*sicurezza della catena di approvvigionamento*", e il Considerando 85, Direttiva (UE) 2022/2555 (NIS2), ricorda i casi in cui i responsabili di atti malevoli hanno compromesso un soggetto "*sfruttando le vulnerabilità che interessano prodotti e servizi di terzi*". Un fornitore compromesso, un aggiornamento avvelenato, un servizio gestito violato restano vettori che per colpirvi devono comunque **raggiungere** il vostro sistema: se il sistema non è raggiungibile, il vettore non ha dove arrivare. Ormai lo avete capito: **ZeroSurface®** non sostituisce la verifica dei fornitori che la direttiva richiede ma rende ininfluente l'esito.

Phishing

Il Considerando 89, Direttiva (UE) 2022/2555 (NIS2), lo cita accanto alle "*tecniche di ingegneria sociale*", e lo fa nel giusto contesto, cioè quello della formazione e della sensibilizzazione delle persone. **ZeroSurface®** non elimina il *phishing* come tecnica (che noia vero?) ma toglie valore a ciò che il phishing cerca di (o riesce a) carpire. L'autenticazione poggia su un ***URL funzionale*** non parlante, senza ridirezionamento e senza rilascio di token; non si può indovinare né raccogliere da un sito civetta o, peggio ancora, pensare di costruirci sopra un sito avvelenato. L'URL è parte integrante delle credenziali da usare insieme con le *iceKey*: in altre parole possono anche rubare le chiavi ma non c'è modo di ricreare la serratura.

*Nota: qui la logica che c'è dietro è forse un po' meno intuitiva perciò, se volete approfondire, potete leggere **questo numero** di Lateral News.*

La domanda scomoda

Tra qualche settimana qualcuno, in molte organizzazioni italiane, **dovrà dimostrare** che le misure di sicurezza di base richieste dal decreto 138/2024 sono operative, non solo pianificate.

E allora la domanda è questa:

> *le misure che state per dimostrare riducono ciascuna minaccia una alla volta, con uno strumento diverso per ognuna, o tolgono la precondizione che tutte hanno in comune?*

Vedete, arrivare al termine di ottobre **con dieci contromisure sintomatiche** non è la stessa cosa che arrivarci avendo tolto il terreno su cui tutte, insieme, si muovono.

Il punto dell'appendice

Il modello a pila le affronta con strumenti diversi, uno per minaccia. La lettura sistemica guarda invece a ciò che hanno in comune: la raggiungibilità del bersaglio. **ZeroSurface®**, brevetto depositato, agisce lì, sulla **STRUTTURA** e non sui **SINTOMI**.

Sei minacce, sei punti della direttiva, una sola precondizione.

Lateralcode s.r.l.

Qui "La NIS2 e ZeroSurface®" si chiude per davvero. Sette letture (in realtà otto con la puntata zero) e un'appendice, tenute insieme da una sola domanda ferma dall'inizio: ***e se il bersaglio non fosse mai raggiungibile?***
