LATERAL NEWS — LATERALCODE

Proteggere gli Ospedali con ZeroSurface®: Risposta Sistemica alle Iniziative Europee

Non bastano lucchetti: se una qualcosa è raggiungibile, è attaccabile. Anche il tuo ospedale!

20 gennaio 2025

Introduzione

Recentemente, la Commissione Europea ha proposto la creazione di un **centro paneuropeo di cybersecurity** per proteggere gli ospedali dagli attacchi informatici, un'iniziativa che sottolinea la crescente necessità di soluzioni innovative per affrontare minacce sempre più sofisticate. Gli ospedali, infatti, rappresentano bersagli critici per ransomware, attacchi Distributed Denial of Service (DDoS) e violazioni di dati sensibili, mettendo a rischio sia la continuità operativa sia la vita dei pazienti.

Se da un lato la proposta del centro di *cyber security* è un passo interessante (benché, nei contenuti, lasci molto molto perplessi!), dall'altro porta con sé un valore assai limitato senza un contestuale ripensamento radicale delle tecnologie di protezione. In questo contesto, **ZeroSurface®** offre un approccio sistemico che **elimina le vulnerabilità alla radice**, ridisegnando completamente la sicurezza delle infrastrutture critiche come quelle sanitarie.

Le Minacce Attuali agli Ospedali

1. Ransomware

Gli attacchi ransomware rappresentano una delle minacce più gravi per gli ospedali, con richieste di riscatto che spesso paralizzano i sistemi e bloccano l'accesso a dati essenziali. Le reti sanitarie, con numerosi dispositivi continuamente connessi e dati sensibili, offrono un ampio terreno di attacco per i criminali informatici.

ZeroSurface® risponde **eliminando completamente le superfici d'attacco esterne**. I ransomware inoculati attraverso vettori esterni semplicemente non possono raggiungere i sistemi protetti, neutralizzando il rischio alla radice.

2. DDoS

Gli attacchi DDoS mirano a rendere inaccessibili i servizi critici sovraccaricando le risorse di rete. Per gli ospedali, questo significa interruzione dei sistemi di emergenza e dei servizi di cura, con conseguenze potenzialmente fatali.

Grazie all'irraggiungibilità garantita da ZeroSurface®, i sistemi non possono essere sovraccaricati perché non esposti.

Nessun attacco DDoS può colpire un'infrastruttura che non è accessibile agli attori non autorizzati.

3. Esfiltrazioni e violazioni di dati

Le informazioni mediche sono tra i dati più preziosi e vulnerabili, spesso oggetto di furti e vendita sul dark web. Tuttavia, ZeroSurface® garantisce un **isolamento bidirezionale**: nulla entra e nulla esce dal sistema protetto se non tra il target e l'utente autenticato. Questo non solo previene qualsiasi forma di esfiltrazione, ma sterilizza anche eventuali backdoor presenti nel sistema.

4. Phishing

Il phishing, una delle tecniche più utilizzate dagli attaccanti, punta a ingannare gli utenti affinché forniscano credenziali riservate.

Tuttavia, **ZeroSurface® rende inefficace questa pratica** grazie alla sua progettazione che prevede, in fase di autenticazione, un **"URL funzionale"** che è parte integrante delle credenziali: in altre parole, l'attaccante, non potendo costruire un sito a quell'indirizzo (che è esso stesso una credenziale che **ha bisogno di operare proprio da quell'indirizzo** e da nessun altro), si troverà nell'impossibilità di accedere all'autenticazione.

Il Ruolo del NIS2

La normativa NIS2, entrata in vigore per rafforzare la sicurezza delle reti e dei sistemi informativi in Europa, richiede standard più elevati per la protezione delle infrastrutture critiche, tra cui gli ospedali. **ZeroSurface® è pienamente conforme ai requisiti del NIS2 (in realtà va anche oltre)**, offrendo una soluzione che garantisce:

- **Protezione continua** contro le minacce emergenti (di fatto non c'è "nulla da proteggere" poiché irraggiungibile).
- **Semplificazione della conformità normativa** grazie all'isolamento bidirezionale, alla gestione e al tipo di credenziali (come detto), alla struttura distribuita e asimmetrica, alla mancanza di dati sensibili associati o associabili
- **Riduzione dei rischi operativi** eliminando le superfici d'attacco e garantendo l'operatività anche in caso di attacco (anche di tipo Supply Chain o 0-day) poiché la protezione rimane invariata in qualsiasi stato operativo si trovi il target o l'infrastruttura ZeroSurface®

Valore per gli Ospedali

Adottare **ZeroSurface®** significa trasformare la sicurezza in un vantaggio competitivo e operativo:

- **Continuità operativa garantita**: Protezione totale contro DDoS e ransomware esterni.
- **Conformità normativa senza complessità**: ZeroSurface® semplifica la protezione dei dati sensibili, rispondendo alle esigenze di normative come il GDPR (ZeroSurface® è pienamente rispondente alle previsoni di *Privacy by Default* e *Secure by Design*) e il NIS2.
- **Riduzione dei costi SOC e IT**: Meno interventi reattivi, meno downtime, maggiore efficienza.

Conclusione

La proposta di un centro paneuropeo di *cybersecurity* per gli ospedali è un'iniziativa preziosa, ma poco incisiva se non affiancata a tecnologie che possano affrontare in modo profondamente diverso le minacce informatiche.

ZeroSurface® rappresenta questa innovazione, offrendo una sicurezza intrinseca che elimina i rischi alla radice.

Scopri di più su ZeroSurface®, scarica il PDF: https://lateralcode.it/wp-content/uploads/2025/01/LC-ZS-_mil_compressed.pdf

Link all'articolo originale: https://www.quotidianosanita.it/cronache/articolo.php?articolo_id=126950

Lateral News — Articoli, idee e riflessioni sullo sviluppo tecnologico e sulla sicurezza informatica non “mainstream”

lateralcode.it