WAREHOUSE LOGISTICS MEETING · TAVOLO CYBERSECURITY

La cybersecurity entra nella filiera

Sintesi della tavola rotonda: NIS2, CRA e software per la logistica

17 novembre 2026 | Moderatore: **Sandro Sana** | In collaborazione con Induvation

IL CONTESTO

Due normative, un unico mercato che cambia

Al tavolo sedevano soprattutto aziende che sviluppano software WMS e TMS e ne curano la manutenzione, da remoto o in presenza. In tre giri di confronto abbiamo discusso di come la NIS2 e il Cyber Resilience Act (CRA) stiano cambiando il loro mercato, raccogliendo sulla lavagna opportunità, ostacoli e quick win.

Le due normative guardano lo stesso problema da due lati diversi. La NIS2 riguarda come lavorate: siete fornitori di aziende che devono proteggere la propria filiera. Il CRA riguarda cosa vendete: il software che producete diventa un prodotto da progettare, documentare e aggiornare in modo sicuro. Per una software house della logistica le due cose arrivano insieme.

IL TEMA TRASVERSALE

Si rischia di essere esclusi da una fornitura per motivi normativi, non per la qualità del prodotto.

TEMA 1 · D.LGS. 138/2024

NIS2 e sicurezza della filiera

Come lavorate: le richieste di sicurezza che arrivano dai clienti

COSA È EMERSO

Essere in filiera non vuol dire essere soggetto NIS2

- **In filiera significa nel perimetro.** Far parte della filiera di un soggetto NIS2 non vi rende a vostra volta soggetti NIS2. Vi porta però dentro il suo perimetro di sicurezza: il cliente deve gestire il rischio dei propri fornitori, e quel rischio siete anche voi.
- **Nessun questionario universale.** Ogni soggetto chiede evidenze di sicurezza secondo criteri propri. Lo stesso fornitore riceve domande diverse da clienti diversi, spesso con formati e livelli di dettaglio non confrontabili.

- **WMS e TMS sono forniture ICT rilevanti.** Un software che governa magazzino e trasporti, mantenuto anche da remoto, tocca il cuore operativo del cliente. Le richieste saranno quindi tra le più stringenti.
- **Molti di voi sono già in lista.** A maggio i soggetti NIS2 hanno stilato l'elenco dei fornitori rilevanti. È molto probabile che le aziende presenti ci siano già, e che possano diventare oggetto diretto della normativa nei prossimi anni.

DALLA LAVAGNA

OPPORTUNITÀ	OSTACOLI	QUICK WIN
Leva commerciale	**Società di un gruppo "piccola" entra in NIS2 come "essenziale"**	**Checklist / audit interno sicurezza**
Essere adeguati e dimostrarlo distingue dai concorrenti	**Non è chiaro se l'azienda entra nella NIS2**	**Plan per rientrare in normativa**
	Rischio di entrare nella prossima NIS2	*Documentazione che attesti la postura di sicurezza*
	Mancanza di struttura	

In grassetto i post-it scritti sulla lavagna; in corsivo gli spunti emersi nella discussione.

LE MIE CONSIDERAZIONI

La dimensione non si misura da soli. Per stabilire se un'azienda è piccola, media o grande si considerano anche le imprese collegate e associate del gruppo, salvo i correttivi previsti. Una società "piccola" può così ritrovarsi nel perimetro, anche come soggetto essenziale. Il primo passo è un'analisi di applicabilità fatta bene, non un'impressione.

"Non siamo NIS2" non chiude la questione. Anche chi è fuori dal perimetro riceverà richieste dai clienti che ci sono dentro. E il perimetro si aggiorna: chi oggi è escluso può rientrarci domani per crescita, acquisizioni o nuove attività. Conviene prepararsi come se si fosse già dentro.

L'accesso remoto è il punto più delicato. Per chi fa assistenza su WMS e TMS, il cliente guarderà soprattutto lì: MFA, utenze nominative e non condivise, accessi remoti tracciati e autorizzati, backup verificati, aggiornamenti puntuali. Sono anche le prime domande dei questionari.

Rispondere una volta sola, e bene. Contro la frammentazione dei questionari serve un dossier di sicurezza pronto: referente, regole, evidenze, procedura di gestione degli incidenti. Lo stesso materiale si riusa con ogni cliente e, quasi naturalmente, porta verso la certificazione ISO/IEC 27001.

La struttura minima è una persona. La mancanza di struttura si affronta prima di tutto nominando un responsabile delle richieste di sicurezza dei clienti, con un mandato chiaro della direzione. Senza un punto di riferimento le richieste si perdono tra commerciale, sviluppo e assistenza.

Guardate anche a monte. Anche voi avete fornitori: hosting, cloud, librerie, partner. Se uno di loro si ferma, cosa si blocca da voi e dai vostri clienti? Chiederselo prima è parte della risposta che darete ai vostri clienti.

TEMA 2 · REG. (UE) 2024/2847

Cyber Resilience Act e prodotti digitali

Cosa vendete: il software come prodotto sicuro, documentato e aggiornato

COSA È EMERSO

Più sicurezza nel codice, più costi da governare

- **Il software diventa un prodotto con marcatura CE.** Il CRA si applica ai prodotti con elementi digitali: terminali, scanner, sensori IoT e anche il software. Devono essere sicuri fin dalla progettazione e restare aggiornati per tutto il periodo di supporto.
- **I costi crescono.** Sicurezza del codice, penetration test, gestione delle vulnerabilità e documentazione tecnica hanno un costo che prima non era a budget.
- **Le piccole software house sono le più esposte.** Con strutture ridotte e margini già stretti, il rischio concreto è vedere i margini assottigliarsi ulteriormente.
- **Chi si prepara prima vende meglio.** Una roadmap di marcatura CE dimostrabile è già oggi un argomento commerciale verso chi è ancora agli inizi.

DALLA LAVAGNA

OPPORTUNITÀ	OSTACOLI	QUICK WIN
Software sicuro e pronto “CE”	**Rischio maggiore per aziende “piccole”**	*Roadmap di marcatura CE dimostrabile*
Fatturato aggiuntivo per canoni di manutenzione	**Penetration test con AI e costo**	*Periodo di supporto dichiarato*
Approccio al business model SaaS		

In grassetto i post-it scritti sulla lavagna; in corsivo gli spunti emersi nella discussione.

LE MIE CONSIDERAZIONI

Le date sono già qui. Dall’11 settembre 2026 i fabbricanti devono segnalare le vulnerabilità attivamente sfruttate e gli incidenti gravi. L’11 dicembre 2027 il regolamento si applica per intero. Chi rilascerà nuove versioni dopo quella data deve partire ora.

Patch gratuite, evoluzioni a canone. Gli aggiornamenti di sicurezza vanno resi disponibili senza costi per tutto il periodo di supporto e, dove possibile, separati da quelli funzionali. Le minor release evolutive restano invece un servizio che si può proporre a canone. Attenzione: per i prodotti realizzati su misura per un cliente business, le parti possono accordarsi diversamente, e i contratti vanno riletti con questo occhio.

Il periodo di supporto va dichiarato. Il fabbricante deve indicare per quanto tempo garantirà gli aggiornamenti di sicurezza, di norma almeno cinque anni. È una scelta che pesa sul modello economico ed è una delle prime domande che vi farà un cliente informato.

SaaS: fuori dal CRA, ma attenzione alla NIS2. Un servizio SaaS puro, senza componenti installate presso il cliente, non è un prodotto ai sensi del CRA. Ma i fornitori di servizi cloud rientrano tra i settori della NIS2. Spostarsi sul SaaS può quindi trasferire gli obblighi da una normativa all’altra: è

una scelta da valutare caso per caso, non una scorciatoia.

Il costo si può contenere. Nella maggior parte dei casi un software WMS o TMS non rientra tra i prodotti “importanti” o “critici” e può seguire la valutazione interna di conformità, senza organismo notificato. Per micro e piccole imprese il regolamento prevede inoltre misure di supporto e una documentazione tecnica semplificata.

Penetration test e AI. Gli strumenti basati su AI possono abbassare il costo dei test continui e aiutare a trovare prima le vulnerabilità più comuni. Non sostituiscono però il test manuale sui punti critici né la responsabilità del fabbricante: vanno usati per testare più spesso, non per testare meno.

Il marchio cambia il ruolo. Chi rivende con il proprio marchio o modifica in modo sostanziale un prodotto altrui ne diventa fabbricante, con tutti gli obblighi. Chi distribuisce deve invece verificare marcatura CE, dichiarazione UE di conformità, istruzioni e dati di fabbricante e importatore.

IN SINTESI

Da obbligo a vantaggio competitivo

NIS2 e CRA non sono solo un costo di conformità. Per chi sviluppa software per la logistica, chi si muove per primo e sa dimostrare la propria sicurezza può trasformarle in un vantaggio competitivo: la conformità diventa un argomento di vendita, non solo un requisito da soddisfare. Chi aspetta, invece, rischia di scoprirlo al momento di una gara o di un rinnovo contrattuale.

IL FOGLIO CONSEGNATO AI PARTECIPANTI

10 cose da portare a casa

TEMA 1 · D.LGS. 138/2024

NIS2 e sicurezza della filiera

1 **Anche se non siete NIS2, i clienti potrebbero esserlo.**
Devono gestire il rischio dei loro fornitori: le richieste arriveranno anche a voi.

2 **Questionari, clausole e audit.**
MFA, utenze nominative, accessi remoti controllati, backup verificati, aggiornamenti.

3 **Un dossier di sicurezza pronto.**
Referente, regole, evidenze, procedura incidenti: rispondete una volta sola, e bene.

4 **Una persona che risponde.**
Un responsabile delle richieste di sicurezza dei clienti, con il mandato della direzione.

5 **Sapere da chi dipendete.**
Se un vostro fornitore si ferma, cosa si blocca da voi? Chiedetevelo prima.

TEMA 2 · REG. (UE) 2024/2847

Cyber Resilience Act e prodotti digitali

1 **Riguarda i prodotti con elementi digitali.**
Terminali, scanner, sensori IoT, software: sicuri dalla progettazione e aggiornati nel tempo.

2 **Due date da segnare.**
11/09/2026: segnalazione di vulnerabilità sfruttate e incidenti. 11/12/2027: piena applicazione.

3 **Chi distribuisce verifica.**
Marcatura CE, dichiarazione UE di conformità, istruzioni, dati di fabbricante e importatore.

4 **Chiedete il periodo di supporto.**
Prima di comprare o rivendere: fino a quando arriveranno gli aggiornamenti di sicurezza?

5 **Il vostro marchio cambia tutto.**
Rivendete con il vostro marchio o modificate in modo sostanziale? Diventate fabbricanti.

“Sicurezza crea libertà.”

SANA SANDRO

Sandro Sana · Consulente Cybersecurity, NIS2 & CRA
sandro@sanasandro.it · +39 335 615 2678 · www.sanasandro.it