factory SOFTWARE
A Sonepar Company

AVEVA SELECT ITALY

WHITE PAPER

Il Cyber Resilience Act

Perché le organizzazioni industriali dovrebbero prestare attenzione

Capire CRA e NIS2: due regolamenti UE che stanno ridisegnando i rapporti tra fornitori e operatori e ridefinendo le responsabilità della cybersecurity industriale.

Indice

1. Introduzione

L'email dell'ufficio Acquisti sembrava abbastanza di routine:

Il rinnovo del contratto con il fornitore richiede un'attestazione di sicurezza aggiornata. Si prega di confermare che tutti i sistemi rispettino la nostra attuale policy di cybersecurity.

Il responsabile di impianto te l'ha inoltrata senza aggiungere una parola, solo un punto interrogativo. Come manager IT/OT delle operazioni di produzione, sai bene cosa significa. Fissi lo schermo, poi apri il registro degli asset con un senso di urgenza. Il sistema SCADA è stato installato nel 2011. Lo storico dati è del 2008. I gateway edge sono arrivati insieme a una linea di confezionamento acquisita con un'operazione di M&A tre anni fa: non sei nemmeno certo di chi fosse il fornitore originale. Metà dei server OPC in funzione nello stabilimento sono stati configurati da appaltatori che ormai non ci sono più e si basano ancora su DCOM.

Chiami il fornitore:

Potete confermare che i nostri sistemi rispettano gli attuali standard di cybersecurity?"

Il tecnico del supporto è cortese, ma poco risolutivo:

Non possiamo davvero pronunciarci su come avete configurato l'ambiente. Nel 2011 abbiamo fornito delle linee guida di sicurezza, ma non sappiamo quali modifiche abbiate fatto da allora. Se volete che verifichiamo il vostro ambiente, è un incarico a parte.

Riattacchi e ti rendi conto che: nessuno sa davvero chi sia responsabile di mantenere questi sistemi al sicuro. Il fornitore li ha realizzati. Il tuo team li ha messi in produzione. Le Operations li hanno modificati. L'IT gestisce la rete su cui girano. E adesso l'Ufficio Acquisti chiede un'attestazione che nessuno è in grado di rilasciare con certezza.

Questo scenario si sta ripetendo proprio ora in molte realtà industriali

Due nuove normative UE stanno imponendo chiarezza in rapporti che per decenni sono rimasti comodamente sfumati. Il **Cyber Resilience Act (CRA)** stabilisce cosa devono consegnare i fornitori. La **Direttiva NIS2** definisce cosa devono garantire gli operatori. Insieme, stanno ridisegnando il confine delle responsabilità nella cybersecurity industriale.

2. Due normative, due responsabilità

La confusione è comprensibile: entrambe le norme parlano di cybersecurity, entrambe arrivano dall'UE ed entrambe hanno scadenze ravvicinate. Ma si rivolgono a soggetti diversi e impongono obblighi diversi.

CRA

Cyber Resilience Act
Il problema del fornitore (quindi anche il nostro)

Stabilisce requisiti obbligatori di cybersicurezza per i prodotti digitali venduti nell'Unione europea, inclusi software industriali e dispositivi connessi. Il regolamento diventa applicabile verso la fine del 2027. I fornitori devono progettare prodotti con la sicurezza integrata, mantenere la sicurezza per tutta la vita del prodotto, garantire trasparenza sulla composizione del software e, in molti casi, ottenere la marcatura CE che includa garanzie di cybersicurezza.

NIS2

Direttiva NIS2
La sfida dell'operatore

La Direttiva sulla sicurezza delle reti e dei sistemi informativi (aggiornata a NIS2 nel 2023) impone agli operatori di servizi essenziali e importanti, tra cui manifattura, energia, acqua e infrastrutture critiche, di adottare misure di cybersicurezza adeguate, segnalare gli incidenti rilevanti e dimostrare resilienza. Se gestisci impianti industriali in settori coperti dalla NIS2, la conformità è un obbligo di legge.

3. Perché la conformità al CRA semplifica la conformità alla NIS2

NIS2 impone agli operatori di adottare "misure tecniche e organizzative adeguate e proporzionate" per gestire i rischi di cybersicurezza. La direttiva non indica tecnologie o configurazioni specifiche: definisce i risultati che devi raggiungere. La direttiva richiede di mappare le vulnerabilità, implementare controlli stringenti, governare patch e aggiornamenti, e mitigare gli incidenti in modo tempestivo, dimostrando piena conformità alle autorità di vigilanza.

Prova a farlo con sistemi industriali progettati prima che la sicurezza by design diventasse la norma: ti ritroverai con il livello di sicurezza previsto dal fornitore, a cui si aggiungono le modifiche introdotte dal tuo team e le vulnerabilità emerse dopo la messa in esercizio.

Applicare le patch richiede test approfonditi e, spesso, il fermo della produzione. La gestione delle vulnerabilità dipende dalla rapidità con cui il fornitore rilascia gli aggiornamenti. La risposta agli incidenti, infine, presuppone che tu abbia piena visibilità su ciò che è realmente in esecuzione nei tuoi sistemi.

I fornitori conformi al CRA rendono tutto questo molto più semplice. Quando la sicurezza è integrata fin dall'inizio, parti da una base più solida. Quando i fornitori adottano processi chiari di gestione delle vulnerabilità, sai quali rischi stai realmente governando. Quando mettono a disposizione dati trasparenti sulla composizione del software, capisci da cosa dipende la tua supply chain. Quando si impegnano a garantire finestre di supporto definite con aggiornamenti di sicurezza, puoi pianificare la gestione del ciclo di vita in modo strutturato.

La sfida della gestione delle patch

Prendiamo la gestione delle patch. NIS2 si aspetta che le vulnerabilità note vengano corrette in tempi rapidi. Ma negli ambienti industriali aggiornare non è affatto banale: servono finestre di test, fermi produzione, procedure di rollback e verifiche operative.

Un fornitore con una conformità CRA davvero matura rilascerà patch con indicazioni chiare per i test, vincoli di compatibilità noti e procedure di rollback documentate. Al contrario, un fornitore che riduce il CRA a un mero adempimento burocratico si limiterà a rilasciare le patch senza alcun supporto all'integrazione, lasciando l'onere del rischio interamente sulle tue spalle.

Trasparenza della Supply Chain

Il requisito di trasparenza della supply chain porta vantaggi ancora più evidenti. NIS2 si aspetta che tu gestisca il rischio legato a terze parti. Ma come valuti quel rischio se non sai quali componenti di terzi sono integrati nei prodotti dei tuoi fornitori?

Il CRA obbliga i fornitori a documentare le dipendenze della propria supply chain e a garantire che tali componenti rispettino i requisiti di sicurezza. Quella documentazione diventa il tuo punto di partenza per la valutazione del rischio di supply chain secondo NIS2.

Conta anche la relazione inversa. Le organizzazioni che dimostrano una solida conformità alla NIS2 spingeranno i fornitori a migliorare la propria postura CRA. Quando definisci requisiti di sicurezza chiari negli acquisti, quando pretendi trasparenza sulla sicurezza del prodotto, quando chiedi ai fornitori (noi compresi!) responsabilità sul supporto lungo il ciclo di vita, stai creando pressione di mercato per pratiche migliori da parte dei vendor.

4. Cosa richiede davvero il CRA ai fornitori

Quattro requisiti fondamentali determinano tutto ciò che viene dopo. I prodotti con elementi digitali devono essere progettati con la cybersecurity integrata fin dall'inizio, non aggiunta successivamente, dopo la messa in esercizio. I fornitori devono garantire la sicurezza per l'intero ciclo di vita del prodotto, rilasciando tempestivamente le patch, gestendo le vulnerabilità e documentando gli incidenti di sicurezza. Devono inoltre assicurare la massima trasparenza sulla composizione del software, indicando componenti, librerie e dipendenze di terze parti.Per molti prodotti sarà inoltre richiesta la marcatura CE, che non attesterà più soltanto la conformità ai requisiti di sicurezza, ma anche il rispetto di specifici requisiti di cybersecurity.

Il requisito sul ciclo di vita è il più importante

Il requisito relativo al ciclo di vita è quello che ha il maggiore impatto sulle operazioni industriali. A differenza del software consumer, che ha un ciclo di vita di pochi anni, i sistemi industriali rimangono in funzione per decenni. Uno storico installato nel 2008, con ogni probabilità, sta ancora raccogliendo dati oggi. Un sistema HMI del 2012 potrebbe continuare a governare la linea di produzione più critica. Per questo motivo, la sicurezza non può limitarsi alla fase di rilascio del prodotto, ma deve essere garantita per tutta la sua vita operativa.

Il CRA obbliga i fornitori a definire con chiarezza le finestre di supporto e a mantenere gli aggiornamenti di sicurezza per tutta la loro durata. È un cambiamento netto rispetto alla realtà attuale, dove "fine supporto" spesso significa "in bocca al lupo, arrangiati."

Per gli operatori alle prese con i requisiti NIS2, finestre di supporto chiare da parte dei fornitori risolvono un problema cronico. Non puoi mantenere misure di sicurezza adeguate su sistemi che i fornitori non supportano più. Il CRA ti dà più potere contrattuale: chi vuole vendere nell’UE deve impegnarsi su periodi di supporto definiti. Questo impegno facilita la conformità alla NIS2 garantendo che gli aggiornamenti di sicurezza restino disponibili per tutto il ciclo di vita operativo.

Effetti a catena nella supply chain

Il requisito di trasparenza della supply chain genera effetti a catena in tutto il settore. Se il tuo fornitore SCADA utilizza una libreria di comunicazione di terze parti, anche quella libreria deve rispettare i requisiti del CRA. Se non li rispetta, il fornitore deve sostituirla oppure rischia la non conformità. Questo porta alla luce dipendenze rimaste invisibili per anni e impone scelte sul debito tecnico che molte organizzazioni hanno rimandato.

5. Cosa richiede davvero la NIS2 agli operatori

La NIS2 definisce un quadro di gestione del rischio, anziché imporre un elenco di controlli specifici. Le organizzazioni interessate devono valutare i propri rischi di cybersicurezza, adottare misure proporzionate per gestirli e rafforzare nel tempo il proprio livello di sicurezza.

La direttiva individua aree specifiche su cui concentrarsi:

Analisi del rischio e politiche di sicurezza dei sistemi informativi

Gestione degli incidenti

Continuità operativa e gestione delle crisi

Sicurezza della catena di fornitura

Gestione e divulgazione delle vulnerabilità

Misure per valutare l’efficacia del vostro approccio

I dettagli cambiano da uno Stato membro all'altro: ogni Paese recepisce la NIS2 tramite norme nazionali che adattano i requisiti al contesto locale. Ma le aspettative di fondo restano le stesse: devi dimostrare di gestire attivamente il rischio cyber, che le misure adottate siano proporzionate alla reale esposizione al rischio e che tu sappia reagire in modo efficace quando si verificano incidenti.
Per gli operatori industriali, alcuni requisiti creano sfide immediate.

Le aspettative sulla sicurezza della supply chain implicano visibilità sulle pratiche dei fornitori, sulle dipendenze da terze parti e sul livello di sicurezza dei componenti che stai integrando. La gestione delle vulnerabilità richiede processi per individuarle, valutarle e correggerle, e dipende dal fatto che i fornitori forniscano informazioni e patch in tempi utili. La risposta agli incidenti presuppone che tu disponga di capacità di monitoraggio, procedure di escalation definite e della possibilità di contenere e ripristinare gli eventi di sicurezza.

I fornitori conformi al CRA supportano i tuoi requisiti NIS2

La **sicurezza della supply chain diventa più semplice** quando:
- i fornitori documentano le dipendenze dei loro componenti.

La **gestione delle vulnerabilità è più rapida** quando:
- i fornitori mantengono processi chiari di segnalazione e rilascio delle patch.

La **risposta agli incidenti è più efficace** quando:
- i fornitori mettono a disposizione documentazione di sicurezza dettagliata e un supporto tempestivo.

6. Che cosa significa una risposta solida da parte del fornitore

Non tutti i fornitori affronteranno la conformità al CRA allo stesso modo. Alcuni si limiteranno a soddisfare gli obblighi minimi previsti dalla normativa. Altri, invece, coglieranno il CRA come un'opportunità per migliorare in modo più profondo lo sviluppo dei prodotti, la gestione del loro ciclo di vita e i servizi di assistenza. La differenza è importante, perché il software industriale non si valuta solo in base alle funzionalità che offre. Conta anche la qualità della relazione con il fornitore, la capacità di garantire stabilità operativa nel tempo e l'efficacia nella gestione del rischio.

AVEVA ha delineato pubblicamente il proprio approccio all'EU Cyber Resilience Act, includendo l'impegno verso pratiche di security-by-design e la sicurezza lungo tutto il ciclo di vita.

Per le indicazioni più recenti e ufficiali, consulta la posizione pubblica di AVEVA sul CRA.

Per gli operatori che gestiscono la conformità NIS2, l'impegno tempestivo dei fornitori riduce il rischio. È possibile pianificare gli upgrade alle versioni conformi al CRA durante le normali finestre di manutenzione, invece di dover correre ai ripari a fine 2027. Si possono allineare gli aggiornamenti del fornitore ad altri interventi di sicurezza, anziché trattarli come progetti di compliance isolati. E si può dimostrare alle autorità di vigilanza che si sta gestendo in modo proattivo il rischio della supply chain, anziché reagire alle scadenze.

Opzioni di assistenza a lungo termine

L'introduzione delle opzioni di Long-Term Servicing risolve un problema ricorrente per gli operatori industriali e supporta direttamente la conformità NIS2. AVEVA ora offre due percorsi di supporto: Standard Term Servicing con tre anni di supporto attivo più due anni di supporto esteso, e Long-Term Servicing con cinque anni di supporto attivo più due anni di supporto esteso. Questo garantisce ai team operativi finestre di upgrade prevedibili e una maggiore stabilità operativa, in linea con il modo in cui i sistemi industriali funzionano davvero.

Dal punto di vista NIS2, finestre di supporto ben definite risolvono il problema dei "sistemi non supportati". Non puoi mantenere misure di sicurezza adeguate su sistemi che i fornitori non supportano più. Con opzioni LTS chiaramente definite, puoi pianificare la gestione del ciclo di vita in modo sistematico: distribuire sulla linea LTS, stabilizzare e ottimizzare, operare per cinque anni con aggiornamenti di sicurezza, pianificare l'upgrade successivo durante la finestra di supporto esteso. Questo approccio strutturato alla gestione del ciclo di vita è esattamente ciò che la NIS2 si aspetta.

Trasparenza della supply chain

La revisione della supply chain è il lavoro più complesso e, al tempo stesso, il più importante. AVEVA ha esaminato oltre 3.000 componenti esterni integrati nel proprio software, valutando uno per uno la preparazione rispetto al CRA, e ha iniziato a sostituire i componenti i cui fornitori non intendono adeguarsi. Così si evita che i clienti si portino dietro vulnerabilità nascoste provenienti da librerie abbandonate o framework deprecati.

ESEMPIO PRATICO

La tecnologia alla base di InTouch Access Anywhere verrà dismessa perché il suo fornitore non intende perseguire la conformità al CRA. Invece di lasciare i clienti esposti o nell'incertezza, AVEVA sta pianificando in modo proattivo alternative sicure e percorsi di aggiornamento.

Questo rigore nella gestione della supply chain supporta direttamente i tuoi obblighi NIS2 in materia di sicurezza della catena di fornitura. Quando i fornitori rivedono sistematicamente le proprie dipendenze e verificano che i componenti rispettino i requisiti di sicurezza, riducono il rischio associato alle terze parti. La sostituzione proattiva dei componenti non conformi, anziché attendere l'emergere di nuove vulnerabilità, dimostra quell'approccio alla gestione del rischio che la NIS2 si aspetta anche dalle organizzazioni soggette alla direttiva. Inoltre, una comunicazione chiara dei cambiamenti, accompagnata da indicazioni per la migrazione, facilita il percorso di conformità invece di introdurre nuove criticità.

Sviluppo Secure-by-Design

Anche il passaggio a pratiche di sviluppo secure-by-design è fondamentale. AVEVA oggi integra pratiche di codifica sicura, threat modeling, scansioni continue delle vulnerabilità e processi di risposta agli incidenti più efficaci lungo tutto il ciclo di vita dello sviluppo. Non si tratta solo di superare gli audit di conformità. Si tratta di creare prodotti in cui la sicurezza è parte integrante, non un'aggiunta successiva.

7. Cosa significa per te

Le scadenze normative sembrano sempre lontane, finché all'improvviso diventano urgenti. Le organizzazioni che iniziano a prepararsi fin da ora eviteranno le corse dell'ultimo minuto. Ecco su cosa dovrebbero concentrarsi i diversi team, tenendo presente che la conformità alla NIS2 è una responsabilità della tua organizzazione, mentre quella al CRA ricade sui tuoi fornitori. Entrambe, però, richiedono la tua attenzione.

Per il team OT

Parti dall'inventario. È fondamentale mappare con precisione quali sistemi sono in funzione, le relative versioni, i fornitori di riferimento e le scadenze del supporto. I sistemi legacy spesso sono privi di documentazione. Gli stabilimenti acquisiti possono usare stack tecnologici diversi. Sistemi "ombra" creati da ingegneri in buona fede potrebbero non comparire in alcun registro ufficiale degli asset. Create l'inventario subito.

Una volta completato l'inventario, definisci il tuo perimetro NIS2. Quali sistemi rientrano nei servizi essenziali o importanti? Quali fornitori li mettono a disposizione? Quali sistemi stanno arrivando a fine supporto? Questa analisi mette in luce dove siete più esposti e dove la conformità CRA dei fornitori pesa di più sulle vostre operazioni.

Avvia subito un confronto con i fornitori. Chiedere quali sono i loro piani di conformità al CRA, le tempistiche previste e i percorsi di migrazione. Ma informarvi anche su come intendono supportare i tuoi requisiti NIS2. Come gestiscono la divulgazione delle vulnerabilità? Qual è il loro processo di risposta agli incidenti? Che livello di visibilità offrono sui componenti della supply chain? In che modo supportano le tue esigenze di monitoraggio della sicurezza? I fornitori che rispondono con chiarezza e competenza a queste domande vi mettono nelle condizioni di affrontare la conformità con maggiore serenità. Quelli che evitano di rispondere o forniscono indicazioni vaghe stanno introducendo un rischio che ricadrà sulla tua organizzazione.

Per il team IT

Confronta i tuoi standard di cybersecurity con i requisiti NIS2. La direttiva si aspetta misure basate sul rischio, non una semplice conformità "a checklist". Ma gli ambienti industriali richiedono adattamenti che gli approcci tipici dell'IT enterprise spesso trascurano. Architetture zero-trust, accesso basato sull'identità e connettività cloud sicura devono funzionare entro i vincoli operativi: niente patch durante i cicli di produzione, niente flussi di autenticazione che aggiungano latenza ai loop di controllo, niente misure di sicurezza che impediscano agli operatori di reagire alle emergenze.

Costruisci subito un ponte con l'OT. La conformità alla NIS2 richiede coordinamento tra la sicurezza IT e le operazioni OT. Serve una comprensione condivisa delle priorità di rischio, procedure di escalation concordate e capacità congiunte di risposta agli incidenti. La CRA è un elemento che spinge queste conversazioni: man mano che i fornitori passano a versioni conformi alla CRA, serve una pianificazione IT/OT congiunta per test, distribuzione e validazione.

Definisci i tuoi standard di approvvigionamento prodotti conformi al CRA ti offrono una base di sicurezza migliore, ma solo se chi si occupa degli acquisti sa cosa richiedere. Collabora con i team OT per definire i requisiti di sicurezza per l'acquisto di software industriale: aspettative sulla finestra di supporto, requisiti di divulgazione delle vulnerabilità, standard di documentazione di sicurezza, impegni di risposta agli incidenti. Questi requisiti ti aiutano a rispettare gli obblighi NIS2 sulla sicurezza della supply chain e al tempo stesso a promuovere comportamenti migliori da parte dei fornitori.

Per il Management

Allinea CRA e NIS2 come iniziative complementari, non come progetti di conformità separati. La NIS2 è un tuo obbligo di legge. Il CRA è un obbligo di legge per i tuoi fornitori. Ma il successo sulla NIS2 dipende in larga misura dalla conformità dei fornitori al CRA. Le organizzazioni che trattano questi temi come filoni di lavoro separati sprecano risorse e perdono opportunità strategiche.

Dedica un budget adeguato. La conformità a NIS2 non è solo un lavoro tecnico: richiede coordinamento tra operation, ingegneria, IT, acquisti, legale e risk management. Le transizioni dei fornitori verso la CRA aggiungono complessità. Pianificate budget per migrazioni tra fornitori, upgrade dei sistemi, sviluppo dei processi, formazione e monitoraggio continuo. L'investimento ripaga ben oltre la compliance: sistemi modernizzati, meno debito tecnico, una postura di sicurezza più solida e maggiore visibilità operativa.

Prendi decisioni esplicite sui sistemi legacy. Ogni organizzazione industriale ha processi critici che girano su software datato. Non potete aggiornare tutto subito. Date priorità in base all'ambito NIS2, alla criticità operativa, all'impegno del fornitore verso la CRA e all'esposizione al rischio. Alcuni sistemi hanno davvero bisogno di modernizzazione. Altri possono essere isolati, monitorati da vicino e accettati come rischio gestito. La differenza sta nel fare scelte consapevoli, invece di scivolare nella non conformità per inerzia.

Comprendere lo scenario dei controlli e delle sanzioni. NIS2 prevede sanzioni importanti per la non conformità. Ma, soprattutto, introduce responsabilità personali per gli organi di gestione. I membri del consiglio e i dirigenti possono essere chiamati a rispondere di una gestione inadeguata del rischio di cybersecurity. Non è teoria: le autorità stanno attivamente rafforzando le capacità di enforcement. Prendere sul serio NIS2 oggi costa molto meno che dover spiegare domani eventuali fallimenti. Comprendere lo scenario dei controlli e delle sanzioni.

Gettare le basi per ciò che verrà

Il **Cyber Resilience Act e la NIS2**, insieme, definiscono un nuovo standard di riferimento per la cybersicurezza industriale. I fornitori devono realizzare prodotti sicuri. Gli operatori devono garantire operazioni sicure. Nessuno dei due obblighi è facoltativo, e nessuno può funzionare senza l'altro. Le organizzazioni che vedono queste norme come un puro peso di compliance faranno lo stretto necessario e perderanno l'occasione più grande. Le organizzazioni che le considerano un motore di maturità aziendale le useranno per accelerare conversazioni che avrebbero dovuto avviare comunque.

Questioni chiave da affrontare

- Come gestire in modo sistematico il debito tecnico?
- Come garantire una collaborazione efficace tra IT e OT?
- Come bilanciare innovazione e stabilità operativa?
- Come costruire basi digitali che sostengano il prossimo decennio delle operation industriali?

Queste domande contano a prescindere dall'esistenza di CRA e NIS2. Le norme le rendono semplicemente urgenti e offrono una motivazione esterna per investimenti che erano già necessari. Questa urgenza può diventare un vantaggio, se la si gestisce con strategia. Si parte dalla chiarezza sulle responsabilità. I tuoi fornitori rispondono della conformità al CRA. Non puoi fare il lavoro al posto loro, e non dovi accettare prodotti che non rispettano i requisiti del CRA. Ma della conformità alla NIS2 rispondete voi. Non si può scaricare questa responsabilità sui fornitori, né si può dare per scontato che prodotti conformi al CRA soddisfino automaticamente gli obblighi NIS2.

NIS2

Definire l'ambito, fare l'inventario dei sistemi, riesaminare i processi di gestione del rischio e rafforzare il coordinamento tra IT e OT.

CRA

Confrontare con i fornitori i loro piani di conformità, chiarire le tempistiche di migrazione e prepararsi agli aggiornamenti dei sistemi.

Non si tratta di due progetti di compliance separati, ma di due facce della stessa medaglia: mettere in sicurezza le operation industriali per il prossimo decennio.

factory SOFTWARE
A Sonepar Company

AVEVA SELECT | ITALY

Qual è la tua prossima mossa?

Il lavoro comincia adesso.

www.factorysoftware.it