NUOVE NORMATIVE EUROPEE DI CYBER SECURITY

NIS 2, RED, MR E CRA E IL PERCORSO DI ASEM

ASEM
A ROCKWELL AUTOMATION COMPANY

NUOVE NORMATIVE EUROPEE DI CYBER SECURITY

AGENDA

1 Executive Overview

2 RED Cyber

3 NIS 2

4 Machinery Regulation

5 Cyber Resilience Act

6 Cosa c'entra la IEC 62443?

7 Appendice

EXECUTIVE OVERVIEW

Un nuovo quadro normativo europeo

Dal 2025 al 2028 entreranno in vigore NIS 2, RED Cyber Security, Machinery Regulation e Cyber Resilience Act, introducendo requisiti tecnici, organizzativi e di prodotto sempre più stringenti per garantire la sicurezza IT/OT nell'industria.

Impatto sulle aziende e sui prodotti

Le norme richiedono gestione del rischio, rafforzamento della governance cybersecurity, protezioni avanzate nei prodotti digitali e connessi, oltre a dimostrare conformità tramite processi strutturati, certificazioni e aggiornamenti sicuri.

Il percorso di ASEM

ASEM sta adeguando processi e prodotti agli standard internazionali (ISO 27001, IEC 62443), rafforzando il Secure Development Lifecycle, introducendo SBOM, migliorando il vulnerability management e collaborando con partner specialistici per gap-analysis e verifiche di sicurezza.

Obiettivo

Supportare clienti e partner nella transizione normativa garantendo soluzioni sicure, affidabili e conformi, riducendo il rischio cyber su macchine e impianti e garantendo continuità operativa.

EXECUTIVE OVERVIEW

La **NIS 2** riguarda la gestione del rischio aziendale
in ambito cyber security
→ End User ←

La **Machinery Regulation (MR)** riguarda la cybersecurity
nella sicurezza fisica delle macchine
→ OEM / Integrators ←

Il **Cyber Resilience Act (CRA)** riguarda
la cybersecurity del prodotto digitale
→ Suppliers ←

RED CYBER

RED CYBER SECURITY: COS'È

La Radio Equipment Directive (RED) – Cyber Security Art. 3.3

Aggiorna le norme armonizzate per le apparecchiature radio, includendo requisiti di sicurezza informatica per le categorie e le classi di *apparecchiature radio connesse a Internet*.

Con l'entrata in vigore della RED Cyber Security (Art. 3.3), tutti i prodotti che integrano funzionalità Wi-Fi o Cellular devono essere conformi ai nuovi requisiti di sicurezza per poter mantenere la marcatura CE.

RED Cyber Security sui prodotti ASEM

ASEM ha condotto una valutazione completa dei prodotti con interfacce radio (Wi-Fi/Cellular) per stabilire il percorso di conformità alla RED Cyber Security, identificando i dispositivi da certificare e quelli da portare a fine vita in previsione delle nuove regole CE.

Scadenze

- Entrata in vigore: 1 Agosto 2025

RED CYBER SECURITY: QUALI PRODOTTI SONO COINVOLTI

PRODOTTO	STATO
RK11 / RM11 4G Global	End of Life
RK21 / RK22	Certificati RED
HMI40 / HMI50	End of Life - varianti con Wifi e/o Cellular
BM122 / BM130/ BM131	End of Life
VK3500	Certificato RED
ASEM 6300B-JB1AAD **ASEM 6300B-JB1BAD**	Certificati RED

RED CYBER SECURITY: VALIDITÀ DELLA CERTIFICAZIONE RED

I prodotti certificati RED Cyber si distinguono in due categorie:

- Le unità prodotte *prima del 1 Agosto 2025*
  Mantengono la marcatura CE senza necessità di certificazione RED Cyber Security

- Le unità prodotte *dopo il 1 Agosto 2025*
  Sono coperte dalla certificazione RED Cyber Security e la Declaration of Conformity (DoC) è stata aggiornata includendo le nuove sezioni richieste dalla norma.

  La nuova DoC e il RED Cyber Security Certificate of Compliance
  sono disponibili sul sito ASEM per ciascun prodotto certificato.

NIS 2

NIS 2: COS'È

La Network and Information Security 2 (NIS 2)

Mira a migliorare la sicurezza informatica nelle aziende,
imponendo requisiti più stringenti *per la protezione delle reti e dei dati aziendali*.

Nel portale dell'agenzia per la cybersicurezza nazionale dedicato al NIS [LINK]
si trova la documentazione ufficiale:

- una presentazione powerpoint [LINK]
  che fa una panoramica della normativa, con le relative tempistiche
- un prospetto generale [LINK] e uno prospetto dettagliato [LINK]
  che illustrano quali tipologie di aziende
  sono tenute ad essere a norma come *soggetto importante* o *soggetto essenziale*.

Scadenze

- Entrata in vigore: 1 Gennaio 2025
- Deadline per l'implementazione delle misure di sicurezza: 31 Ottobre 2026

NIS 2: CHI È COINVOLTO

Chi è soggetto NIS 2

Un soggetto NIS 2, Essenziale o Importante, dovrà adottare un approccio strutturato alla sicurezza informatica. La NIS 2 infatti non è una certificazione di prodotto, ma un approccio basato sulla gestione del rischio. Le misure di sicurezza devono essere proporzionate al contesto, alla criticità dei servizi e all'impatto potenziale degli incidenti.

Chi non è soggetto NIS 2

La NIS 2 estende la responsabilità della sicurezza informatica anche alla supply chain.
I soggetti essenziali e importanti devono valutare e gestire i rischi cyber
derivanti da software e componenti utilizzati nei propri sistemi e impianti da parte di OEM e integratori.

NIS 2: COSA VIENE CHIESTO

Quando l'end-user chiede all'OEM/integratore:

Siete NIS 2 compliant?

Non sta chiedendo una certificazione o una checklist ISO. Sta chiedendo invece:

Se succede un incidente,
potete dimostrarmi di aver gestito correttamente
il rischio cyber della soluzione che mi avete fornito?

NIS 2: COME SI DIMOSTRA IL CONTROLLO DEL RISCHIO

All'end-user va data garanzia di aver coperto tutte e quattro le aree:

1. Sicurezza della Supply Chain e Sviluppo Software
2. Gestione dei Rischi e Misure Tecniche (Accessi e Cifratura)
3. Gestione degli Incidenti e delle Vulnerabilità
4. Audit, Monitoraggio e Continuità Operativa

ASEM mette a disposizione uno strumento dedicato ad OEM e Integratori per generare il report di mitigazione su questi quattro punti

MACHINERY REGULATION

MACHINERY REGULATION: COS'È

Il nuovo Regolamento Macchine (UE) 2023/1230, denominato anche Machinery Regulation (MR), sostituisce la precedente Direttiva Macchine

Introduce requisiti espliciti di cybersecurity per macchine connesse

Motivo: un attacco cyber può generare un rischio fisico

NOTA: È una normativa che incide direttamente sulla sicurezza delle macchine e sul processo di marcatura CE

Scadenza

- Entrata in vigore: 20 gennaio 2027

MACHINERY REGULATION: PERCHÈ LA CYBERSECURITY CONTA

Anche se il software non è un componente di sicurezza,
può diventare un vettore di rischio, ad esempio:

- accesso remoto che consente modifiche pericolose
- comunicazione con PLC o safety controller
- protocolli non autenticati o non cifrati

Per questo il software rientra nei requisiti dell'Annex III

MACHINERY REGULATION: COSA CHIEDE L'ANNEX III

Il regolamento nell'Annex III include clausole come l'Art. 1.1.9 (Protezione dall'alterazione) e l'Art. 1.2.1 (Sicurezza ed affidabilità dei sistemi di comando) che richiedono:

- che collegamenti remoti o dispositivi connessi non creino situazioni pericolose
- che HW e SW siano protetti da manomissioni accidentali o intenzionali
- che siano rilevabili e tracciabili modifiche legittime o illegittime
- che software e dati critici siano identificati e protetti

non si parla di security IT, ma di protezione della macchina

MACHINERY REGULATION: RUOLI E RESPONSABILITÀ

Gli OEM e Costruttori di Macchine

- Restano responsabili della conformità CE della macchina

Gli integratori

- Devono dimostrare che i componenti digitali non introducono rischi

Cosa fa ASEM ?

- Progetta prodotti secondo principi *secure-by-design* e *secure-by-default*
- Assicura: autenticazione forte, comunicazioni cifrate, gestione accessi e logging
- Allinea i seguenti prodotti ai requisiti della Machinery Regulation
  - UBIQUITY, RK2x Router, FactoryTalk Remote Access, Stratix 4300
  - FactoryTalk Optix, OptixPanel, OptixEdge

La cybersecurity diventa parte del fascicolo tecnico.
ASEM fornisce componenti progettati per supportare il percorso di marcatura CE della macchina.

CYBER RESILIENCY ACT

CYBER RESILIENCE ACT: COS'È

- Il Cyber Resilience Act (CRA) è una normativa europea che:
  - introduce requisiti obbligatori di cybersecurity
  - si applica a hardware e software con elementi digitali
  - è condizione necessaria per ottenere e mantenere la marcatura CE

È una normativa di prodotto, non organizzativa

Scadenza

- Obbligo segnalazione di vulnerabilità sfruttata e/o incidenti: 11 Settembre 2026
- Entrata in vigore: 11 Dicembre 2027

CYBER RESILIENCE ACT: A CHI SI APPLICA

- Il Cyber Resilience Act si applica a:
  - produttori di hardware
  - produttori di software
  - fornitori di prodotti digitali integrabili in macchine o sistemi

- Il Cyber Resilience Act inoltre:
  - Non dipende dal settore industriale
  - Vale per tutti i prodotti connessi

CYBER RESILIENCE ACT: COSA RICHIEDE

- Il CRA richiede che il produttore:
  - sviluppi secondo un Secure Development Lifecycle
  - gestisca aggiornamenti di sicurezza per almeno 5 anni dalla vendita
  - garantisca integrità del software
  - garantisca aggiornamenti sicuri
  - garantisca protezione da accessi non autorizzati
  - fornisca informazioni di sicurezza (es. SBOM)

CRA è quindi una normativa sia **di prodotto** sia **di processo**

La sicurezza diventa un obbligo continuo, non una verifica una-tantum

CYBER RESILIENCE ACT: STANDARD DI RIFERIMENTO

Non esistono ancora standard armonizzati CRA
ma i riferimenti principali sono:

- IEC 62443-4-1 per il processo di sviluppo
- IEC 62443-4-2 per i requisiti di prodotto
- ISO/IEC 27001 per la governance

Il CRA non inventa nuovi concetti,
ma li rende obbligatori per legge

CYBER RESILIENCE ACT: RUOLI E RESPONSABILITÀ

- Gli OEM devono:
  - utilizzare componenti conformi CRA ed evitare prodotti non aggiornabili o non supportati
- Gli integratori devono:
  - integrare i prodotti senza indebolirne la sicurezza e non introdurre configurazioni che annullino le protezioni
- Cosa fa ASEM ?
  - Progetta hardware e software secondo principi secure-by-design
  - Applica il Secure Development Lifecycle Rockwell (IEC 62443-4-1) ai prodotti ASEM rilevanti per il CRA
  - Integra: meccanismi di aggiornamento sicuro, protezione dell'integrità del software, gestione delle vulnerabilità e SBOM

ASEM fornisce prodotti progettati per supportare la conformità CRA dei clienti
La cybersecurity diventa un requisito di prodotto e ASEM fornisce i mattoni giusti per affrontarlo

COSA C'ENTRA LA IEC 62443?

COSA C'ENTRA LA IEC 62443?

- La IEC 62443 è la famiglia di standard internazionali per la cybersecurity dei sistemi di automazione industriale (IACS), riconosciuta a livello globale e vendor-neutral

- Per la Machinery Regulation (UE) 2023/1230, non esiste ancora uno standard armonizzato dedicato alla cybersecurity delle macchine, ma la IEC 62443 è indicata come il riferimento principale per implementare i controlli di sicurezza richiesti dall'Annex III (Art. 1.1.9 e 1.2.1)

- Per il Cyber Resilience Act, i riferimenti principali sono:
  - IEC 62443-4-1 → processo di sviluppo sicuro (Secure Development Lifecycle)
  - IEC 62443-4-2 → requisiti tecnici di sicurezza del prodotto (component-level)

La IEC 62443 sarà, molto probabilmente,
la base degli standard armonizzati sia per il CRA sia per la MR

CERTIFICAZIONE 62443-4-2 ≠ CONFORMITÀ MACHINERY REGULATION

⚠️ *Inserire un componente certificato IEC 62443-4-2 in una macchina non rende automaticamente la macchina conforme alla Machinery Regulation* ⚠️

- La Machinery Regulation richiede che la cybersecurity sia parte della valutazione del rischio complessiva della macchina (Art. 1.1.9, 1.2.1) non che vengano impiegati componenti certificati IEC 62443-4-2
  - Un prodotto con autenticazione forte non serve a nulla se l'OEM lascia le credenziali di default.
  - Un prodotto con comunicazioni cifrate non protegge se l'integratore non abilita TLS/SSL
  - Un prodotto con logging non è utile se nessuno raccoglie e monitora i log.

Il valore non è nel certificato, ma nella capacità di mettere il costruttore della macchina nelle condizioni di applicare le capability di cybersecurity del prodotto.

CERTIFICAZIONE 62443-4-2 ≠ CONFORMITÀ MACHINERY REGULATION

- Quello che conta davvero è che il fornitore metta a disposizione:
  - 📄 Documentazione tecnica di sicurezza chiara e operativa (hardening guide, security manual)
  - 🔧 Istruzioni per configurare e attivare le capability: autenticazione, cifratura, controllo accessi, logging
  - 📋 Linee guida per l'integrazione sicura del prodotto nella macchina o nell'impianto
  - 🛡️ Informazioni per la valutazione del rischio: quali minacce il prodotto mitiga, a quale livello di sicurezza, e quali responsabilità restano in capo all'integratore
  - 🔄 Processi di vulnerability management e aggiornamento accessibili e documentati

- Un buon fornitore non consegna solo un certificato: consegna gli strumenti per costruire una macchina sicura.
- La responsabilità della conformità CE della macchina resta dell'OEM/costruttore, ma il fornitore di componenti ha il dovere di rendere praticabile l'applicazione delle capability di sicurezza, non solo di dichiararle su carta.

CERTIFICAZIONE 62443-4-2 ≠ CONFORMITÀ CRA

⚠️ Un prodotto certificato IEC 62443-4-2
non è automaticamente conforme al CRA ⚠️

- La IEC 62443 è uno standard tecnico volontario, il CRA è una normativa europea obbligatoria. Il CRA richiede elementi aggiuntivi che la certificazione 62443 da sola non copre

Aspetto	IEC 62443-4-2	CRA
Natura	Standard volontario	Regolamento UE obbligatorio
Requisiti tecnici prodotto	✅ Coperti	✅ Coperti (parzialmente allineati)
Vulnerability handling e reporting (24h/72h/14gg)	❌ Non previsto	✅ Obbligatorio (Art. 14)
Monitoraggio post-market	❌ Non previsto	✅ Obbligatorio
SBOM (Software Bill of Materials)	❌ Non previsto	✅ Obbligatorio
Documentazione tecnica e conformità UE	❌ Non previsto	✅ Obbligatoria (Allegato VII)
Dichiarazione UE di conformità + CE	❌ Non previsto	✅ Obbligatoria
Minimum support period of 5 years	❌ Non previsto	✅ Obbligatorio (Art. 13(8))

APPENDICE

NIS 2 - ARTICOLI

Sicurezza della Supply Chain e dello Sviluppo Software
La direttiva, agli *Art. 21.2.d* e *21.2.e* impone di garantire la sicurezza lungo l'intera catena di approvvigionamento, richiedendo di valutare rigorosamente sia l'affidabilità dei fornitori sia la qualità dei processi di sviluppo e acquisizione dei prodotti ICT.

Hardening di Sistema, Controllo degli Accessi e Cifratura dei Dati
La direttiva, agli *Art. 21.2.g*, *21.2.h*, *21.2.i* e *21.2.j* richiede di mettere in sicurezza le reti industriali imponendo rigorose politiche di controllo degli accessi logici e fisici agli asset. Questo include l'uso di soluzioni di autenticazione a più fattori (MFA), solide pratiche di igiene informatica e l'impiego della crittografia per garantire l'integrità dei dati.

Gestione Vulnerabilità e Risposta agli Incidenti
La direttiva all'*Art. 23* e agli *Art. 21.2.b* e *21.2.e* richiede la predisposizione di procedure chiare per la prevenzione, il rilevamento e la gestione degli incidenti, includendo la segnalazione tempestiva delle vulnerabilità significative.

Monitoraggio, Audit e Continuità Operativa
La direttiva agli *Art. 21.2.a*, *21.2.c* e *21.2.f*, impone di garantire la resilienza delle attività aziendali attraverso l'analisi dei rischi, il monitoraggio continuo dei sistemi, l'implementazione di piani di ripristino in caso di disastro e procedure per valutare regolarmente l'efficacia delle misure di sicurezza adottate.

MACHINERY REGULATION – ANNEX III

Art 1.1.9 – Protezione dall'alterazione

La macchina o il prodotto correlato devono essere progettati e costruiti in modo tale da fare sì che il collegamento ad essi di un altro dispositivo, tramite qualsiasi caratteristica del dispositivo connesso stesso o tramite qualsiasi dispositivo remoto che comunica con la macchina o il prodotto correlato, non determini una situazione pericolosa.

I componenti hardware che trasmettono segnali o dati, importanti per il collegamento o l'accesso a software che sono fondamentali affinché la macchina o il prodotto correlato rispettino i pertinenti requisiti essenziali di sicurezza e di tutela della salute, devono essere progettati in modo tale da essere adeguatamente protetti da un'alterazione accidentale o intenzionale.

La macchina o il prodotto correlato devono raccogliere prove in merito a un intervento legittimo o illegittimo su tali componenti hardware, se importante per il collegamento o l'accesso al software critico per la conformità della macchina o del prodotto correlato.

Software e dati critici per il rispetto da parte della macchina o del prodotto correlato dei pertinenti requisiti essenziali di sicurezza e di tutela della salute devono essere individuati come tali e devono essere adeguatamente protetti da un'alterazione accidentale o intenzionale.

La macchina o il prodotto correlato devono individuare il software installato sullo stesso, necessario per il suo funzionamento in condizioni di sicurezza, e devono essere in grado di fornire tali informazioni in qualsiasi momento in un formato facilmente accessibile.

La macchina o il prodotto correlato devono raccogliere prove di un intervento legittimo o illegittimo sul software o di una modifica del software installato sulla macchina o sul prodotto correlato o della sua configurazione.

MACHINERY REGULATION – ANNEX III

Art 1.2.1 – Sicurezza ed affidabilità dei sistemi di comando

I sistemi di comando devono essere progettati e costruiti in modo da evitare l'insorgere di situazioni pericolose.I sistemi di comando devono essere progettati e costruiti in modo tale che:a) riescano a resistere, se del caso, a circostanze e rischi, a previste sollecitazioni di servizio e ad influssi esterni intenzionali o meno, compresi tentativi deliberati ragionevolmente prevedibili da parte di terzi che conducono a una situazione pericolosa;b) un'avaria nell'hardware o nella logica del sistema di comando non crei situazioni pericolose;c) errori della logica del sistema di comando non creino situazioni pericolose;d) i limiti delle funzioni di sicurezza siano stabiliti come parte della valutazione del rischio effettuata dal fabbricante e non siano consentite modifiche alle impostazioni o alle norme generate dalla macchina o dal prodotto correlato o dagli operatori, neanche durante la fase di apprendimento della macchina o del prodotto correlato, qualora tali modifiche possano determinare situazioni pericolose;e) errori umani ragionevolmente prevedibili nelle manovre non creino situazioni pericolose;f) la registrazione di tracciamento dei dati generati in relazione a un intervento e delle versioni del software di sicurezza caricato dopo l'immissione sul mercato o la messa in servizio della macchina o del prodotto correlato sia consentita per cinque anni dopo tale caricamento, esclusivamente al fine di dimostrare la conformità della macchina o del prodotto correlato rispetto al presente allegato a fronte di una richiesta motivata da parte di un'autorità nazionale competente.I sistemi di controllo delle macchine o dei prodotti correlati dotati di un comportamento o una logica integralmente o parzialmente auto-evolutivi e che sono progettati per funzionare con livelli variabili di autonomia devono essere progettati e costruiti in maniera tale da:a) non essere la causa di azioni, da parte della macchina o del prodotto correlato, che vanno oltre il suo compito e il suo spazio di movimento definiti;b) consentire che siano registrati i dati relativi al processo decisionale in materia di sicurezza per i sistemi di sicurezza basati su software che garantiscono la funzione di sicurezza, compresi i componenti di sicurezza, dopo che la macchina o il prodotto correlato sono stati immessi sul mercato o messi in servizio, e che tali dati siano conservati per un anno dopo la loro raccolta, esclusivamente per dimostrare la conformità della macchina o del prodotto correlato al presente allegato a seguito di una richiesta motivata da parte di un'autorità nazionale competente;c) consentire in qualsiasi momento la correzione della macchina o del prodotto correlato al fine di preservarne la sicurezza intrinseca.

CYBER RESILIENCE ACT - ARTICOLI

Ambito di obbligo	Descrizione dell'obbligo per il fornitore di software	Riferimenti normativi
Progettazione sicura del prodotto (Secure by design)	Garantire che il software sia progettato e sviluppato tenendo conto dei principi di cyber security fin dall'inizio, per minimizzare i rischi di attacchi e malfunzionamenti fin dall'immissione sul mercato. Il prodotto non deve contenere vulnerabilità note al momento della consegna. Implementare configurazioni di default sicure (*secure by default*).	Art. 13(1); Allegato I, parte I (punto 1 e 2)
Valutazione e documentazione dei rischi	Condurre e documentare una valutazione dei rischi di cyber security del prodotto, considerando l'uso previsto e ragionevolmente prevedibile, l'ambiente operativo e i beni da proteggere. Utilizzare i risultati della valutazione per determinare quali requisiti essenziali di sicurezza applicare e come implementarli. Mantenere aggiornata tale valutazione nel tempo (ad es. quando emergono nuove minacce o cambia l'uso del prodotto).	Art. 13(2)-(4)
Due Diligence su componenti terzi	Verificare e garantire che i componenti di terze parti inclusi (librerie software, moduli open source, etc.) non compromettano la sicurezza complessiva. Integrazione responsabile dell'*open source*: se si usano componenti FOSS (Free/Open-Source Software) non commerciali, occorre valutarne la sicurezza e magari partecipare alla loro comunità per gestire le vulnerabilità.	Art. 13(5)

CYBER RESILIENCE ACT - ARTICOLI

Ambito di obbligo	Descrizione dell'obbligo per il fornitore di software	Riferimenti normativi
Gestione delle vulnerabilità nel ciclo di vita	• Predisporre processi interni per la scoperta, segnalazione e correzione tempestiva delle vulnerabilità di sicurezza nel prodotto e nei suoi componenti: Monitorare attivamente le vulnerabilità note (es. CVE) che riguardano il proprio software o i componenti inclusi, e attuare correzioni (patch, aggiornamenti) non appena disponibili. Adottare una politica di divulgazione coordinata delle vulnerabilità (*Coordinated Vulnerability Disclosure*) per favorire le segnalazioni da parte di ricercatori e utenti esterni, e comunicare tale politica (es. indicare un contatto per inviare segnalazioni di sicurezza) • Mantenere registrazioni (log) di sicurezza e aggiornare all'occorrenza la valutazione dei rischi con le nuove informazioni su minacce/vulnerabilità.	Art. 13(6)-(8), (12) & (17); Allegato I, parte II (tutti i punti)

CYBER RESILIENCE ACT - ARTICOLI

Ambito di obbligo	Descrizione dell'obbligo per il fornitore di software	Riferimenti normativi
Aggiornamenti di sicurezza e supporto agli utenti	• Garantire la disponibilità di aggiornamenti di sicurezza (patch) efficaci: Stabilire e dichiarare un periodo di assistenza durante il quale le vulnerabilità saranno corrette e gli aggiornamenti di sicurezza forniti. Tale periodo deve tener conto della vita utile prevista del prodotto ed essere minimo di 5 anni a meno che la vita stimata del prodotto sia più breve. (Per software industriali longevi, è opportuno prevedere un supporto anche più esteso, dato l'uso pluriennale in impianti produttivi.) • Rendere disponibili le patch in modo tempestivo, gratuito e possibilmente automatizzato. Permettere all'utente di essere avvisato degli update e di installarli facilmente (preferibilmente per via telematica). Assicurarsi che gli aggiornamenti di sicurezza siano distinti da eventuali aggiornamenti di funzionalità, per evitare che l'utente debba acquistare upgrade funzionali solo per ottenere correzioni di sicurezza. • Mantenere le patch di sicurezza pubblicate scaricabili per almeno 10 anni dalla loro emissione (anche oltre il termine del supporto, se questo è < 10 anni). • Se si rilascia una nuova versione sostanzialmente modificata del software, garantire la sicurezza (conforme al CRA) almeno per l'ultima versione; *gli utenti delle versioni precedenti devono poter migrare all'ultima gratuitamente*, senza costi nascosti (es. non facendo pagare licenze aggiuntive per il solo fatto di dover installare la patch su una nuova release). • Considerare la possibilità di rendere disponibili le versioni precedenti del software in archivi pubblici (e avvertire gli utenti dei rischi dell'uso di versioni non più supportate)	Art. 13(8)–(11); Allegato I, parte II (punti 6–9)

CYBER RESILIENCE ACT - ARTICOLI

Ambito di obbligo	Descrizione dell'obbligo per il fornitore di software	Riferimenti normativi
Documentazione tecnica e conformità	Predisporre la documentazione tecnica (vedi Allegato VII) prima di immettere il prodotto sul mercato, includendovi la valutazione del rischio e la descrizione di come il prodotto rispetta i requisiti di sicurezza. Sottoporre il prodotto a una valutazione di conformità (es. controllo interno della produzione o, se rientra tra i "prodotti critici", anche esame UE del tipo o certificazione) secondo le procedure indicate nell'art. 32. Redigere e fornire la Dichiarazione UE di Conformità e apporre la marcatura CE prima della vendita. Conservare la documentazione tecnica e la dichiarazione di conformità per almeno 10 anni dopo la vendita del prodotto (o per la durata del supporto, se superiore).	Art. 13(4), (12)-(14); Art. 13(20)
Informazioni e supporto agli utenti	• Fornire agli utenti finali informazioni chiare sulla sicurezza del prodotto e sul suo utilizzo sicuro: Accompagnare il software con istruzioni d'uso e informazioni di sicurezza (Allegato II), incluse le specifiche sul periodo di assistenza garantito (indicandone la data di fine supporto)Le istruzioni devono essere chiare e comprensibili, e rimanere disponibili per almeno 10 anni dal rilascio del prodotto. • Specificare all'atto dell'acquisto (ad es. sulla confezione, su un sito web o nella documentazione) *fino a quando* il prodotto riceverà aggiornamenti di sicurezza (es. "Supporto garantito fino a MM/AAAA"). Inoltre, se possibile, inviare notifica agli utenti quando il periodo di assistenza sta per scadere, in modo che siano consapevoli che il prodotto non riceverà più patch. • Indicare chiaramente i dati di contatto del fabbricante (nome, sede, e-mail, sito web) sul prodotto, imballo o documentazione, e istituire un punto di contatto unico (es. un indirizzo e-mail dedicato, un portale, ecc.) a cui gli utenti possano rivolgersi rapidamente, soprattutto per segnalare problemi di sicurezza (vulnerabilità).	Art. 13(15)-(19); Allegato II

CYBER RESILIENCE ACT – ARTICOLI

Ambito di obbligo	Descrizione dell'obbligo per il fornitore di software	Riferimenti normativi
Segnalazione di vulnerabilità e incidenti	• In caso di scoperta di una falla di sicurezza critica già sfruttata (*vulnerability under active exploitation*) o di un grave incidente informatico riguardante il prodotto: Entro 24 ore dalla scoperta, inviare un preavviso tramite la piattaforma ENISA/CSIRT designata, segnalando almeno di che tipo di problema si tratta (es. vulnerabilità 0-day sfruttata, o incidente da cyber-attacco). • Entro 72 ore, fornire una notifica dettagliata con informazioni più precise sulla natura della vulnerabilità/incidente, le azioni correttive intraprese e le misure di mitigazione consigliate agli utenti • Fornire una relazione finale – entro 14 giorni (per le vulnerabilità) o 1 mese (per gli incidenti) – descrivendo la vulnerabilità/incidente, la sua gravità, cause e impatti, e le misure correttive adottate (es. patch rilasciata) • Informare tempestivamente gli utenti del prodotto riguardo alla vulnerabilità o all'incidente e alle azioni che devono intraprendere (ad es. applicare un aggiornamento di sicurezza, modificare configurazioni, isolare il sistema dalla rete, ecc.) • Se il fabbricante non avvisa gli utenti in tempo utile, i CERT coordinatori possono divulgare essi stessi l'esistenza della minaccia • Collaborare con le autorità (ENISA, CSIRT, vigilanza mercato) fornendo eventuali informazioni aggiuntive o rapporti di follow-up su richiesta • N.B.: Tali obblighi di notifica entrano in vigore prima degli altri: dall'11 settembre 2026, anche per prodotti già sul mercato	Art. 14(1)-(8); Art. 14(8); Art. 13(21)

GRAZIE

ASEM

A ROCKWELL AUTOMATION COMPANY