PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 28 - numero 6072 di Lunedì 04 maggio 2026

Cyber Resilience Act: come l'UE sta rafforzando la sicurezza dei prodotti digitali

Il Regolamento per garantire che tutti i prodotti digitali presenti sul mercato siano al sicuro dalle minacce informatiche: obblighi di sicurezza, gestione vulnerabilità e aggiornamenti obbligatori fino al 2027 per software e dispositivi connessi.

Il Cyber Resilience Act (CRA) è una normativa dell'Unione Europea che introduce un cambiamento significativo nel modo in cui vengono progettati, venduti e mantenuti i prodotti digitali. L'obiettivo è semplice ma ambizioso: rendere obbligatoria la sicurezza informatica per tutti i prodotti con elementi digitali immessi sul mercato europeo, dai software ai dispositivi connessi.

A differenza delle norme precedenti, che si concentravano soprattutto sui servizi o sulla gestione dei dati, il CRA agisce direttamente "alla radice" del problema, imponendo che la sicurezza sia integrata fin dalla progettazione del prodotto e mantenuta per tutto il suo ciclo di vita. In altre parole, non si tratta più di aggiungere protezioni in un secondo momento, ma di costruire prodotti sicuri fin dall'inizio.

Un nuovo standard di sicurezza per prodotti digitali

Il CRA stabilisce che i prodotti digitali immessi sul mercato europeo devono essere progettati e mantenuti secondo principi di **"cybersecurity by design"** e **"by default"**.

In particolare, i produttori devono garantire che:

- i prodotti siano sicuri già dalla fase di progettazione
- le vulnerabilità vengano gestite in modo continuo
- siano disponibili aggiornamenti di sicurezza per tutto il ciclo di vita del prodotto
- gli utenti ricevano informazioni chiare sulla sicurezza dei prodotti

Questi requisiti si applicano a una vasta gamma di prodotti, dai dispositivi IoT alle applicazioni software.

Perché l'Unione Europea ha introdotto il CRA

La nascita del Cyber Resilience Act risponde a un problema sempre più evidente nel mercato digitale europeo: molti prodotti connessi vengono immessi sul mercato con livelli di sicurezza insufficienti o con aggiornamenti irregolari, esponendo utenti e imprese a rischi informatici.

L'UE ha quindi deciso di intervenire per aumentare il livello minimo di sicurezza dei prodotti digitali, ridurre le vulnerabilità sfruttabili dagli attaccanti e rafforzare la fiducia nel mercato unico digitale. L'idea di fondo è che un ecosistema digitale più sicuro sia anche più competitivo e affidabile.

Come verrà applicato il regolamento

L'attuazione del CRA coinvolge direttamente i produttori, che dovranno adeguare i propri processi di sviluppo e manutenzione. Sarà necessario dimostrare che i prodotti rispettano i requisiti di sicurezza previsti e che esiste un sistema efficace per la gestione delle vulnerabilità.

Anche gli Stati membri avranno un ruolo importante, attraverso attività di sorveglianza del mercato e controllo della conformità dei prodotti. In alcuni casi, sarà richiesto il coinvolgimento di organismi di valutazione indipendenti prima dell'immissione sul mercato.

Un'entrata in vigore graduale

Il regolamento è entrato in vigore nel 2024 (venti giorni dopo la pubblicazione nella Gazzetta Ufficiale dell'UE). Da questo momento la norma esiste formalmente, ma la maggior parte degli obblighi non si applica ancora subito.

Dal **10 settembre 2026** i produttori dovranno segnalare vulnerabilità attivamente sfruttate, comunicare incidenti di sicurezza significativi ed entra a pieno regime il sistema di reporting verso le autorità europee

Dal **10 dicembre 2026** diventano operative pienamente le procedure di valutazione della conformità per categorie di prodotti che richiedono controlli esterni e gli organismi notificati iniziano a operare su larga scala per certificazioni e verifiche.

Dal **10 dicembre 2027** tutti i prodotti con elementi digitali immessi sul mercato UE dovranno essere pienamente conformi al CRA, la cybersecurity by design e by default diventa obbligo effettivo per tutti i produttori, si applicano integralmente requisiti su aggiornamenti, gestione del ciclo di vita e documentazione di sicurezza

Cosa cambia concretamente

Per le aziende, il CRA comporta un cambiamento rilevante: la sicurezza non sarà più un aspetto opzionale o secondario, ma un requisito fondamentale per poter vendere prodotti nel mercato europeo. Sarà necessario strutturare processi più rigorosi per la gestione delle vulnerabilità e garantire aggiornamenti continui.

Per gli utenti finali, invece, il risultato atteso è un miglioramento significativo della sicurezza dei prodotti digitali. I dispositivi e i software dovrebbero diventare più affidabili, meglio aggiornati e più trasparenti nella gestione dei rischi.

Un tassello della strategia europea

Il Cyber Resilience Act si inserisce nella più ampia strategia europea per la cybersicurezza e si affianca ad altre normative come la direttiva NIS2. Insieme, queste misure mirano a rafforzare la resilienza digitale dell'Unione Europea, intervenendo sia sulle infrastrutture critiche sia sui prodotti tecnologici utilizzati ogni giorno.

Il CRA segna un cambio di paradigma importante: la sicurezza informatica non viene più trattata come un'aggiunta successiva, ma come un requisito fondamentale e obbligatorio nella progettazione di qualsiasi prodotto digitale destinato al mercato europeo.

Federica Gozzini

www.puntosicuro.it