Comunicato stampa

CYBER RESILIENCE ACT, CNI: LA SICUREZZA DEI PRODOTTI DIGITALI SI PROGETTA A MONTE

Al convegno del Consiglio Nazionale degli Ingegneri il punto su obblighi, conformità e sicurezza della catena di fornitura. Cappiello (Vicepresidente Vicario CNI): "Dietro ogni dichiarazione di conformità ci sarà un lavoro tecnico. E competenza e responsabilità hanno da sempre un nome: l'ingegnere".

Il Consiglio Nazionale degli Ingegneri, con la partecipazione dell'Agenzia per la cybersicurezza nazionale, ha fatto il punto sul **Cyber Resilience Act (CRA)**, il regolamento europeo che rende la sicurezza informatica un requisito obbligatorio per i prodotti con elementi digitali. L'occasione è stata il convegno **"Cyber Resilience Act – Obblighi, conformità e sicurezza della catena di fornitura"**, promosso dal CNI e dal C3i (Comitato Italiano dell'Ingegneria dell'Informazione) svoltosi martedì 3 novembre in doppia modalità: in presenza presso la sede del Consiglio Nazionale a Roma e online, dove i 3.000 posti disponibili sono andati esauriti in pochissimo tempo: segno di quanto il tema sia sentito dalla professione.

Con il regolamento (UE) 2024/2847 la sicurezza informatica entra nel perimetro della marcatura CE. La piena applicazione è fissata all'11 dicembre 2027, ma la fase operativa è già iniziata: dall'11 giugno 2026 si applicano le norme sulla notifica degli organismi di valutazione della conformità e dall'11 settembre i fabbricanti devono segnalare le vulnerabilità attivamente sfruttate e gli incidenti gravi. In Italia, lo schema di decreto legislativo di adeguamento, approvato in esame preliminare dal Consiglio dei Ministri il 2 ottobre, individua nell'ACN l'autorità di notifica e di vigilanza del mercato. Un tema reso ancora più attuale dagli attacchi informatici che nei giorni scorsi, in diversi Paesi europei, hanno colpito i sistemi di gestione da remoto della refrigerazione di numerosi supermercati.

"Il moderno cavallo di Troia – **ha affermato Carla Cappiello, Vicepresidente Vicario del CNI e promotrice dell'iniziativa** – ha la forma di un componente: una libreria software, un firmware, un aggiornamento, qualcosa che arriva da fuori, di cui ci fidiamo e che facciamo entrare nei prodotti, negli impianti, nelle case. Il Cyber Resilience Act nasce proprio per questo: neutralizzare il cavallo di Troia. Per la prima volta una norma europea fissa, in modo trasversale, requisiti comuni di sicurezza informatica per i prodotti con elementi digitali: dal baby monitor allo smartwatch, fino ai dispositivi che entrano negli impianti e negli edifici che progettiamo. La sicurezza non è più un accessorio da aggiungere a valle: è un requisito da progettare a monte e da mantenere nel tempo, aggiornamento dopo aggiornamento.

“Da qui l’interrogativo che chiama in causa la professione: “Chi analizzerà il rischio, verificherà i componenti, seguirà le vulnerabilità negli anni? Dietro ogni dichiarazione di conformità ci sarà un lavoro tecnico. E competenza e responsabilità hanno da sempre un nome: l’ingegnere. L’ingegnere dell’informazione che progetta il software, l’ingegnere impiantista che porta l’automazione negli edifici, l’ingegnere industriale che mette in rete una linea di produzione”.

Cappiello ha poi sottolineato il valore della partecipazione dell’Agenzia per la cybersicurezza: “Desidero ringraziare l’ACN per aver costruito con noi questo incontro, scegliendo il dialogo e venendo nella casa degli ingegneri italiani a spiegare le regole prima di doverle far rispettare. È il segno di un’istituzione che crede nella prevenzione prima che nella sanzione: la stessa cultura che il regolamento chiede alle imprese”.

Per l’ACN, **Federico Niccolò Ricotta** ha illustrato l’ambito di applicazione del CRA e gli obblighi degli operatori economici; **Sandro Mari** si è soffermato sui percorsi di valutazione della conformità e sulla notifica dei relativi organismi (CAB, Conformity Assessment Bodies); **Danilo D’Elia** ha presentato le opportunità di finanziamento a sostegno delle imprese impegnate nell’adeguamento. L’Ing. **Paola Rocco** ha infine analizzato come cambia la gestione del rischio lungo la catena di fornitura. I lavori sono stati moderati da **Lorenzo Ivaldi**, docente dell’Università di Genova e delegato C3i dell’Ordine degli Ingegneri della Provincia di Alessandria, parte attiva nella realizzazione del convegno.

Roma 10 novembre 2026

Antonio Felici

Capo Ufficio Stampa

Consiglio Nazionale degli Ingegneri

Via XX Settembre 5 - 00187 Roma

tel 06.69.76.701

cell 347-8761540

www.cni.it