PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 27 - numero 5885 di Lunedì 07 luglio 2025

Nuove regole UE sulla sicurezza informatica per combattere le vulnerabilità

Le nuove norme UE, come il Cyber Resilience Act e il Regolamento Macchine, impongono requisiti per proteggere i sistemi di controllo da corruzioni. Gli enti di normazione dovranno garantire tecnologie sicure e affidabili nel mercato europeo.

Le vulnerabilità nei software dei prodotti spesso passano inosservate. Le nuove normative europee puntano a cambiare questa situazione. Il Cyber Resilience Act e il Regolamento Macchine stabiliscono requisiti chiari per la protezione dei sistemi di controllo contro corruzioni accidentali o intenzionali. Gli organismi di normazione sono ora chiamati a creare una base per tecnologie sicure e affidabili nel mercato europeo, tenendo conto anche del documento guida previsto per il Regolamento Macchine.

Ogni anno, i ricercatori in ambito sicurezza segnalano migliaia di vulnerabilità IT nei prodotti, che vanno da *backdoor* nei sistemi di controllo industriale a comandi radio che si fidano ciecamente di qualsiasi segnale ricevuto. Molti utenti non sono nemmeno a conoscenza di queste falle, e finora i produttori hanno avuto pochi incentivi a investire risorse per risolverle. A fronte di questo fallimento del mercato, la Commissione Europea ha risposto con un pacchetto normativo completo:

- Il **Cybersecurity Act** stabilisce il mandato per l'**Agenzia dell'Unione Europea per la cybersicurezza (ENISA)**. ENISA mira a migliorare la comunicazione delle vulnerabilità tra segnalatori, produttori, operatori e autorità pubbliche in Europa, e ha creato a tal fine una banca dati europea.
- La **Direttiva NIS-2** impone obblighi a entità essenziali e importanti (organizzazioni e aziende) per garantire la sicurezza delle reti e dei sistemi informativi, insieme a requisiti vincolanti per la segnalazione degli incidenti di sicurezza. Attualmente, diversi Stati membri sono in ritardo con il recepimento della direttiva nel diritto nazionale.
- Il **Cyber Resilience Act (CRA)** definisce gli obblighi dei produttori per prevenire e gestire le vulnerabilità. Ad esempio, devono garantire la disponibilità di un canale di contatto per le emergenze. Sono già disponibili diverse specifiche gratuite per questo canale, che definiscono, tra l'altro, modalità standardizzate per descrivere la criticità delle vulnerabilità e i formati dei dati:
    - La **RFC 9116** dell'**Internet Engineering Task Force (IETF)** descrive come le aziende possano utilizzare un semplice file di testo per rendere disponibile a livello globale l'informazione su chi contattare in caso di vulnerabilità.
    - Il CRA non impone un formato specifico per l'elenco dei software inclusi nel prodotto (**Software Bill of Materials ? SBOM**), che deve essere generato dal produttore. I formati **CycloneDX** e lo standard **ISO/IEC 5692** (System Package Data Exchange) stanno trovando ampio consenso. L'SBOM può essere utilizzato per la segnalazione automatica dei prodotti contenenti software vulnerabile.
    - Il framework **ISO/IEC 20153 CSAF (Common Security Advisory Framework)** è stato stabilito per le raccomandazioni leggibili da macchina richieste dal CRA.

L'importanza del CRA si riflette anche nel numero di nuovi lavori normativi: solo nel 2025, circa 40 proposte di nuovi standard saranno sottoposte a voto per l'armonizzazione con il CRA.

Pubblicità

Documento guida UE a supporto dei requisiti di sicurezza del Regolamento Macchine

Il **Regolamento Macchine**, rivolto ai produttori, richiede nell'**Allegato III**, sezioni 1.1.9 e 1.2.1, che la protezione contro la corruzione accidentale o intenzionale sia garantita fin dalla fase di progettazione. Inoltre, devono essere raccolte prove di eventuali interventi legittimi o illegittimi.

La Commissione Europea prevede di pubblicare entro gennaio 2027 una guida che spiegherà in modo pratico i concetti e chiarirà gli obblighi. Uno dei cinque gruppi di lavoro incaricati della redazione della guida si occuperà delle sezioni sulla protezione contro la corruzione. La guida costituirà l'interpretazione del Regolamento e fornirà quindi un importante supporto anche all'attività di normazione.

Primi componenti per la protezione dalla corruzione già in fase di sviluppo

Il lavoro di normazione sulla proposta di norma **prEN 50742** è stato avviato presso **CENELEC**. Questa norma è volta a supportare i requisiti del Regolamento Macchine relativi alla protezione dalla corruzione. Dovrà essere il più possibile compatibile con altri standard di sicurezza come:

- **ISO/IEC 15408** (*Common Criteria*)
- **EN 17640** (metodologia di valutazione della cybersicurezza con tempistiche fisse per prodotti ICT)
- **IEC 62443** (sicurezza per l'automazione e i sistemi di controllo industriali)

La norma dovrà essere applicabile a una gamma molto ampia di prodotti, da avvitatori a batteria a utensili da officina, piattaforme di sollevamento e componenti di sicurezza. Una **bozza del comitato (CD)** della prEN 50742 è attesa nell'estate 2025. L'obiettivo è che la norma venga completata in tempo utile per l'armonizzazione prima dell'entrata in vigore del Regolamento Macchine, prevista per il **20 gennaio 2027**.

Sicurezza e protezione da manipolazioni: un approccio integrato

La tendenza a considerare anche gli aspetti di sicurezza IT oltre a quelli di sicurezza funzionale emerge anche dalla revisione della norma **ISO 12100** sulla sicurezza delle macchine. Si sta affermando un approccio secondo cui:

1. Tutti i pericoli potenziali devono essere prima identificati con una **analisi convenzionale dei rischi**, valutando i pericoli senza misure protettive.
2. Le misure protettive vengono poi implementate, e queste stesse misure devono essere **protette contro manipolazioni**, per garantirne il funzionamento affidabile.

Il principio guida è che la corruzione accidentale o intenzionale non deve generare nuovi pericoli. Deve essere garantita, ad esempio, l'attendibilità della valutazione dei segnali, come una richiesta di arresto di emergenza. L'**IFA (Istituto per la Sicurezza e la Salute sul Lavoro della DGUV)** ha analizzato vari sistemi di controllo macchina e ha riscontrato che in molti casi la funzione di arresto di emergenza può essere compromessa a distanza con sorprendente facilità.

Anche la corruzione simultanea di più macchine è un rischio da normare

La normazione deve anche tenere conto del rischio di **corruzione simultanea** di un gran numero di macchine. Per esempio, il guasto di un singolo ascensore o distributore di carburante può essere gestibile, ma un attacco su vasta scala a tutti i sistemi con lo stesso controllo potrebbe avere **conseguenze catastrofiche**. A differenza dei guasti simultanei per usura (molto improbabili), la corruzione coordinata di tutti i sistemi di un certo tipo è uno scenario di sicurezza molto serio.

Cosa fare ora: primi passi per le aziende

Alle aziende si consiglia di **implementare immediatamente il canale di contatto di emergenza** descritto nella **RFC 9116**. La ricerca ha già documentato per decenni gli elementi chiave dei futuri standard di sicurezza IT. La sfida attuale è trovare un **consenso sul livello di rischio socialmente accettabile** e sviluppare **specifiche di prova pratiche**.

Questo articolo è ripreso dal sito KAN. La traduzione in italiano è effettuata con l'assistenza dell'Intelligenza artificiale. Per un uso professionale e/o di studio si raccomanda di fare riferimento all'articolo all'origine.

Licenza Creative Commons

www.puntosicuro.it