

20.11.2024

Premi Messaggio

Pilz GmbH & Co. KG  
Felix-Wankel-Straße 2  
73760 Ostfildern  
Germania  
<https://www.pilz.com>

## **Informazioni, consigli e raccomandazioni Pilz su come recepire la normativa - Legalmente vincolante: come le aziende si preparano al Cyber Resilience Act**

Ostfildern , 20.11.2024 - **Il Cyber Resilience Act (CRA) è stato recentemente pubblicato sulla Gazzetta Ufficiale dell'Unione Europea. Il regolamento contiene disposizioni in materia di cibersecurity relativamente a prodotti con elementi digitali. 36 è il numero di mesi che le aziende interessate da questo provvedimento hanno a disposizione per ottemperare ai requisiti contenuti nel CRA. Occorre rispettare determinati obblighi di segnalazione già nei prossimi 21 mesi. Chi è di fatto soggetto a tale obbligo? E cosa richiede il CRA?**

Atto giuridico dell'UE sulla cyber resilience o resilienza informatica: il CRA (Cyber Resilience Act o Legge sulla ciberresilienza) si prefigge l'obiettivo di proteggere utilizzatori e aziende dagli attacchi informatici. Il CRA include un numero elevato di disposizioni per fabbricanti, importatori e distributori di prodotti con elementi digitali che sono in grado di comunicare con altri prodotti. Sono compresi anche i prodotti hardware e software. Coinvolti sono inoltre i prodotti dell'area B2C, come gli smartphone e i robot aspirapolvere, ma anche dell'area B2B, come i sistemi di controllo e i sensori, oltre ai prodotti software come i sistemi operativi. Il CRA è stato pubblicato il 20.11.2024 sulla Gazzetta Ufficiale dell'Unione Europea. In quanto regolamento, questa legge ha trovato applicazione immediata negli Stati membri UE.

### **I requisiti principali per i fabbricanti di macchine**

- Valutazione del rischio e relativa garanzia: i fabbricanti sono tenuti a progettare e sviluppare prodotti in modo tale che sia garantita un adeguato livello di cibersecurity durante l'intero ciclo di vita del prodotto.
- Gestione delle vulnerabilità: il fabbricante è tenuto a eliminare le vulnerabilità note attraverso aggiornamenti gratuiti della sicurezza nella misura in cui tra il fabbricante e l'utente commerciale non sia

stato concordato diversamente.

- Documentazione: i costruttori sono tenuti a identificare e documentare le vulnerabilità e i componenti dei loro prodotti.
- Obblighi di segnalazione: entro le 24 ore successive alla presa di conoscenza, il fabbricante è tenuto a segnalare un'eventuale intervenuta vulnerabilità tramite l'apposita piattaforma dell'ENISA (European Union Agency for Cybersecurity).

### **Cosa possono fare fin da subito i fabbricanti di macchine**

In qualità di azienda esperta in automazione sicura, Pilz raccomanda a tutti i fabbricanti di macchine di occuparsi con tempestività dei requisiti previsti dal CRA e di sviluppare concept di cooperazione con fabbricanti di componenti e operatori. In quale zona della rete deve essere utilizzata una macchina? Come devono essere gestiti gli aggiornamenti software? Una volta chiariti in anticipo questi quesiti, ciascun soggetto economico è in grado di adempiere ai propri obblighi organizzativi e tecnici. Pilz supporta da decenni fabbricanti di macchine e utilizzatori per quanto attiene alla sicurezza di macchine e impianti, anche per le nuove disposizioni in materia di Industrial Security. Perché senza security, una macchina con tutte le misure di safety implementate resta vulnerabile e non protetta. A tale proposito occorre applicare misure precauzionali.

### **2 consigli pratici per l'implementazione delle disposizioni CRA**

1. Sempre allo stato dell'arte: abbonarsi alle newsletter e ai feed RSS di [eur-lex.europa.eu](http://eur-lex.europa.eu) consente di mantenersi informati sulle modifiche di leggi e normative a livello UE.
  2. Il Common Security Advisory Framework (CSAF) è un framework standard e open-source per la comunicazione e la distribuzione automatizzata di informazioni sulle vulnerabilità e relativa mitigazione che possono essere gestite dalle macchine, le cosiddette Security Advisories.
- [Ulteriori informazioni sul tema Industrial Security sono disponibili qui](#)



**Didascalia:**

Testi e immagini per il download sono disponibili in:

<https://www.pilz.com/it-INT/company/press/messages/articles/243224>

### **Pilz - The spirit of safety**

Pilz è fornitore globale di prodotti, sistemi e servizi per la tecnologia di automazione. Azienda "pionieristica" nel settore dell'automazione sicura, Pilz crea sicurezza per l'uomo, le macchine e l'ambiente. Fondata nel 1948 e con sede principale a Ostfildern, vicino a Stoccarda in Germania, Pilz è oggi una realtà diffusa in modo capillare in tutto il mondo grazie a 42 filiali e rappresentanze commerciali ed oltre 2500 dipendenti.

È leader in ambito tecnologico con soluzioni di automazione olistiche che garantiscono safety e industrial security sulle macchine e che comprendono sensori, sistemi di controllo e azionamento, oltre a sistemi per la comunicazione industriale, la diagnostica e la visualizzazione. L'offerta è integrata da un portafoglio di servizi di livello internazionale che include consulenza, engineering e corsi di formazione. Le soluzioni Pilz trovano applicazione non solo nella costruzione di macchine e impianti ma in numerosi altri settori, come quello dell'intralogistica, dell'imballaggio e packaging e della tecnologia ferroviaria o della robotica.

## **Pilz sui social network**

Sui canali dei social media forniamo informazioni generali sull'azienda, sui collaboratori Pilz e sui continui sviluppi nelle tecnologie di automazione.



<https://www.facebook.com/pilzINT>



[https://twitter.com/Pilz\\_INT](https://twitter.com/Pilz_INT)



<https://www.youtube.com/user/PilzINT>



<https://www.xing.com/companies/pilzgmbh%26co.kg>



<https://www.linkedin.com/company/pilz>

## **Contatto per la stampa**

Martin Kurth

Stampa settoriale e specializzata

+49 711 3409 - 0

[publicrelations@pilz.com](mailto:publicrelations@pilz.com)

Sabine Skaletz-Karrer

Stampa specializzata

+49 711 3409 - 7009

[s.skaletz-karrer@pilz.de](mailto:s.skaletz-karrer@pilz.de)