„La cybersecurity diventa parte integrante dell'omologazione dei prodotti“

Cyber Resilience Act e Regolamento Macchine UE: cosa devono sapere ora i costruttori di macchine – Intervista a Jürgen Leng

Dürmentingen - Il Regolamento Macchine UE 2023/1230 e il Cyber Resilience Act (CRA) definiscono nuovi standard per la sicurezza delle macchine. In futuro, i produttori dovranno considerare e documentare sistematicamente non solo la sicurezza funzionale, ma anche la protezione dai rischi informatici. In questa intervista, l'esperto normativo Jürgen Leng (Business Development Manager presso SCHLEGEL) spiega a cosa devono prestare attenzione le aziende e come Schlegel, con 2BSecure, offre una protezione pratica ed efficace.

Signor Leng, CRA e Regolamento Macchine: a cosa devono prepararsi le aziende in tema di sicurezza delle macchine?
Jürgen Leng: Con il nuovo Regolamento Macchine UE (UE) 2023/1230 e il Cyber Resilience Act (CRA), la cybersecurity diventa per la prima volta una componente obbligatoria della sicurezza delle macchine. Oltre alla sicurezza funzionale, i produttori dovranno in futuro considerare e documentare in modo sistematico anche la protezione dai rischi informatici.
Un'importante novità è rappresentata dalla protezione contro la cosiddetta "corruzione" richiesta nell'Allegato III, sezione 1.1.9 del Regolamento Macchine. Si tratta di un termine della normativa che indica la manipolazione o la modifica non autorizzata di macchine, software o parametri che può compromettere le funzioni rilevanti per la sicurezza.

Cosa si intende concretamente?
La norma prEN 50742 "Protezione delle macchine contro la corruzione" fornisce ai costruttori linee guida pratiche. Definisce come progettare e gestire le macchine in modo da prevenire sia le manipolazioni involontarie sia quelle intenzionali.
L'attenzione è rivolta in particolare a:

- Protezione degli accessi alle macchine e ai sistemi di controllo
- Messa in sicurezza delle interfacce esterne
- Protezione contro versioni software manipolate
- Garanzia dell'integrità delle funzioni rilevanti per la sicurezza

Parallelamente, il CRA richiede prove chiare della cybersecurity delle macchine connesse in rete, una novità assoluta a livello UE.

Quali requisiti concreti introduce il Cyber Resilience Act per i costruttori di macchine?
Il CRA impone ai produttori di garantire la cybersecurity per l'intero ciclo di vita del prodotto, dallo sviluppo fino alla fine del suo utilizzo.
Tra i requisiti più importanti figurano:

- Security by Design & Default: la cybersecurity deve essere considerata già in fase di sviluppo. I prodotti non devono utilizzare password standard e le interfacce inutilizzate devono essere disattivate.
- Valutazione del rischio e gestione delle vulnerabilità: prima dell'immissione sul mercato, il produttore è tenuto a effettuare una valutazione sistematica dei rischi informatici. Le vulnerabilità individuate devono essere documentate e corrette rapidamente.
- Aggiornamenti di sicurezza obbligatori: gli aggiornamenti di sicurezza devono essere forniti per almeno cinque anni oppure per tutta la vita utile prevista del prodotto.
- divulgazione di tutti i componenti software (compreso l'open source) per garantire trasparenza lungo la catena di fornitura (Software Bill of Materials – SBOM).

Pillhof 51 · I-39057 Appiano
+39 0471 633348 | info@interel-trading.eu
www.interel-trading.eu

INTEREL TRADING

- Obblighi di notifica: gli incidenti di sicurezza gravi devono essere segnalati alle autorità competenti.
- Valutazione della conformità e marcatura CE: a seconda della classe di rischio, sono richieste auto-valutazioni o verifiche da parte di organismi esterni. Inoltre, i requisiti del CRA entreranno a far parte della valutazione di conformità CE.
- Per i costruttori di macchine ciò significa che la cybersecurity diventerà in futuro una componente fissa dell'omologazione del prodotto.

Quali prodotti sono interessati dal CRA?
Il CRA si applica a tutti i prodotti con elementi digitali fabbricati, importati o distribuiti nell'Unione Europea. Il campo di applicazione è quindi molto ampio, poiché comprende tutti i prodotti che possono essere collegati a reti o dispositivi.

I prodotti vengono classificati in diverse classi di rischio. Nella classificazione, un ruolo determinante è svolto dal potenziale danno che possono causare. I prodotti utilizzati, ad esempio, nelle infrastrutture critiche, nella produzione industriale o nel settore energetico rientrano in categorie di rischio più elevate. Per i produttori ciò comporta procedure di valutazione della conformità più estese e rigorose.

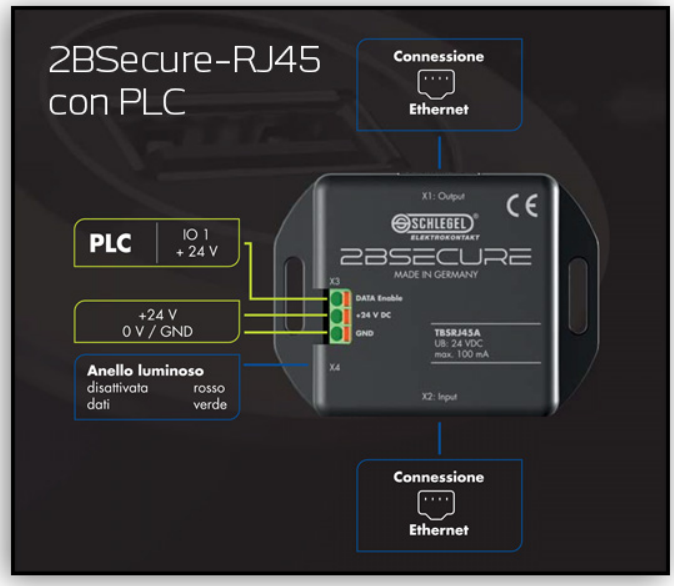
Chi desidera verificare se uno dei propri prodotti rientra nell'ambito del CRA può utilizzare il test disponibile sul sito web del TÜV Süd. Attraverso poche domande verrà determinato se il Cyber Resilience Act è rilevante per i propri prodotti: (www.tuvsud.com/de-de/dienstleistungen/produktpruefung-und-produktzertifizierung/cyber-resilience-act/cra-grafik)

Quanto è elevato attualmente il potenziale di rischio derivante dagli attacchi informatici?
Il rischio è già oggi elevato e le imprese ne sono pienamente consapevoli. Secondo l'associazione di categoria Bitkom (Rapporto economico 2025), il 72% degli intervistati considera elevata la minaccia informatica; inoltre, negli ultimi dodici mesi circa il 66% delle aziende tedesche è stato vittima di furti di dati. Circa il 70% degli attacchi è attribuito alla criminalità organizzata. I danni derivanti da interruzioni operative, furto o compromissione di sistemi informativi, sistemi produttivi o processi aziendali sono aumentati da 2024 a 2025 di quasi 20 miliardi di euro, raggiungendo 73,3 miliardi di euro.

Il tema è quindi di grande attualità. Lo stesso vale per il calendario di attuazione del CRA: l'obbligo di notifica delle vulnerabilità e degli incidenti di sicurezza previsto dal CRA entrerà in vigore l'11 settembre 2026. Dall'11 dicembre 2027 tutti i nuovi prodotti dovranno essere pienamente conformi al CRA.

La protezione delle interfacce esterne fa parte della norma sulla protezione contro la corruzione. Perché queste interfacce vengono spesso trascurate?
Il rischio derivante dalle interfacce fisiche delle macchine viene effettivamente spesso sottovalutato. Con la crescente interconnessione delle macchine nell'ambito dell'Industria 4.0 aumenta anche il rischio di attacchi informatici tramite porte USB o Ethernet. In molti casi queste rappresentano accessi di servizio necessari, ma allo stesso tempo costituiscono potenziali punti di ingresso.

Attraverso tali accessi possono essere introdotti malware, letti dati o modificati parametri macchina. In questo conte-



Pillhof 51 · I-39057 Appiano
+39 0471 633348 | info@interel-trading.eu
www.interel-trading.eu

INTEREL TRADING

sto, misure tecniche di protezione possono ottenere risultati significativi in modo semplice.

SCHLEGEL ha sviluppato 2BSecure, un sistema che protegge le interfacce aperte. Come funziona concretamente?
2BSecure è stato progettato come una soluzione hardware compatta che viene installata tra l'interfaccia e il dispositivo finale ed è compatibile con le comuni interfacce USB-A, USB-C ed Ethernet.
Il sistema segue un approccio preventivo: le interfacce sono disattivate di default e possono essere abilitate esclusivamente da persone autorizzate per esempio tramite selettore a chiave, tecnologia RFID o tramite uscite di PLC protette da password. Solo gli utenti autorizzati possono attivare le porte e trasferire dati; in questo modo l'accesso diventa controllabile e le manipolazioni possono essere efficacemente prevenute. La soluzione protegge sia il sistema di controllo della macchina sia i dati sensibili presenti sulla rete.

Per utilizzare il sistema sono necessari importanti interventi di retrofit?
No, la soluzione è stata volutamente progettata per essere facilmente integrabile. Può essere utilizzata sia su macchine nuove sia su impianti esistenti e può essere integrata nelle infrastrutture macchina e IT già presenti senza particolari interventi.
In questo modo segue il principio del „Security by Design".

In che misura i requisiti normativi hanno influenzato lo sviluppo del prodotto?
I requisiti normativi introdotti dal nuovo Regolamento Macchine e dal CRA hanno rappresentato un fattore determinante nello sviluppo della soluzione, poiché entrambe le normative richiedono misure di protezione dimostrabili contro accessi non autorizzati e manipolazioni.
Attraverso la protezione controllata delle interfacce fisiche, 2BSecure può contribuire all'implementazione tecnica di tali requisiti e alla riduzione documentabile dei rischi.

Contatto:
Georg Schlegel GmbH & Co. KG
Wolfgang Zoll
Kapellenweg 4
88525 Dürmentingen
Telefon +49 (7371) 502-0
Telefax +49 (7371) 502 49
www.schlegel.biz
vertrieb@schlegel

Contatto media:
Georg Schlegel GmbH & Co. KG
Bruno Jungwirth
Kapellenweg 4
88525 Dürmentingen
Telefon +49 (7371) 502-0
Telefax +49 (7371) 502 49
www.schlegel.biz
bruno.jungwirth@schlegel.biz

SCHLEGEL®
ELEKTROKONTAKT

A proposito di Georg Schlegel GmbH & Co.KG

Schlegel è sinonimo di innovazione, qualità e design. Fondata nel 1945, Schlegel è ad oggi un'azienda che opera a livello mondiale: con sede in Germania, uffici commerciali in Austria e Singapore, esporta verso più di 80 paesi di tutti i continenti.

Tra le principali competenze di Schlegel troviamo lo sviluppo e la produzione di unità di controllo, spie di segnalazione e morsettiere. La gamma prodotti comprende inoltre sistemi bus, contenitori, finecorsa, pannelli di controllo e moduli funzionali. Durante lo sviluppo di nuovi prodotti, Schlegel richiede standard elevati soprattutto a livello di design.

Più di 90 premi nazionali e internazionali confermano la competitività di progettazione dell'azienda; tra questi il Premio Design tedesco, l' IF Design Award e il Red Dot Design Award.

GERMAN INNOVATION AWARD '20 WINNER

DESIGN AWARD 2020

reddot design award

Pillhof 51 · I-39057 Appiano
+39 0471 633348 | info@interel-trading.eu
www.interel-trading.eu

INTEREL TRADING