Informazioni generali

Pilz GmbH & Co. KG
Felix-Wankel-Strasse 2
73760 Ostfildern
Deutschland/Germania
www.pilz.com

16 maggio 2024

Protezione per aziende, macchine e prodotti

Safety e Industrial Security – Tutto da un unico fornitore

Ostfildern, 16 maggio 2024 - **Oggetto degli incidenti di security non sono più solo i sistemi informatici (IT) ma sempre più spesso anche l'ambiente di produzione (OT). In ambito Industrial Security gli incidenti non sono solo gli attacchi mirati ma anche manomissioni e manipolazioni involontarie. Il compito dell'Industrial Security nella produzione è garantire la disponibilità di macchine e impianti, così come l'integrità e la riservatezza di dati e processi meccanici. In definitiva, se un'azienda non è 'padrona' dei propri dati, sono in gioco l'azienda e la sicurezza del suo personale: non c'è safety senza security e senza safety non c'è protezione per l'essere umano.**

Nell'Unione Europea, il legislatore ha risposto alla costante crescita delle minacce informatiche: a livello aziendale, la **Direttiva per la sicurezza delle reti e delle informazioni NIS 2** richiede l'implementazione, per l'intera Unione, di un sistema di gestione della cibersicurezza.

Il **nuovo Regolamento macchine 2023/1230** prevede ora, per macchine e impianti, la protezione contro l'alterazione e obbliga a misure di security per le parti della macchina che hanno effetto sulla sicurezza funzionale.

Il **Cyber Resilience Act (CRA)** prevede misure di security per i prodotti con elementi digitali. Tra questi rientrano anche i sistemi di controllo, i sistemi IO e altri componenti installati nelle macchine.

Aziende, macchine e prodotti – A ogni livello, i fabbricanti e gli operatori di macchine devono affrontare sfide diverse e attenersi a quadri giuridici differenti.

Indipendentemente dall'obbligo imposto dal legislatore in materia di Industrial Security, c'è tutta una serie di buoni motivi per occuparsi tempestivamente di questo tema e richiedere una consulenza. Numerosi processi e condizioni legate al funzionamento delle macchine favoriscono infatti manipolazioni e manomissioni e dovrebbero essere affrontati con urgenza e opportunamente modificati. Una vita utile lunga delle macchine, ad esempio, si ripercuote sui relativi sistemi che spesso cominciano a mostrare i segni del tempo e, prima o poi, a non soddisfare più gli standard di security attuali. Questi sistemi presentano gap nella sicurezza che non possono più essere colmati in quanto il loro provider non fornisce più gli aggiornamenti per la security. Analogamente, spesso risulta impossibile implementare sui dispositivi finali anche la protezione da malware: talvolta sono obsoleti con ripercussioni sulle prestazioni che possono sfociare in perdite di produzione.

L'offerta completa di servizi e prestazioni Pilz

In definitiva, si tratta di mantenere al sicuro e protette le operazioni aziendali; tuttavia, le aziende devono superare sfide diverse che spaziano dall'identificazione delle disposizioni di legge vigenti, dall'individuazione ed eliminazione delle vulnerabilità nei sistemi, passando per la sensibilizzazione e la formazione del personale fino a includere la successiva implementazione di controlli. La security è un *Moving Target* ed è quindi necessaria una verifica periodica dello stato dell'Industrial Security delle macchine.

Pilz, azienda leader in automazione, si è adeguata a queste esigenze strutturando un'offerta di servizi, di livello internazionale, per

fabbricanti di macchine e operatori che prende in considerazione tutti gli aspetti inerenti alla protezione di uomo e macchina. Questa offerta include informazioni di base e guide e ausili per l'orientamento ma anche corsi di formazione e l'Industrial Security Consulting Service (ISCS) con cui vengono implementati progetti concreti.

Con la qualifica "CESA – Certified Expert for Security in Automation", da un anno Pilz offre un percorso formativo (durata: 2 giorni) per esperti che eroga ai partecipanti una conoscenza compatta e allo stato dell'arte della situazione normativa in tema Security. Altri contenuti del corso sono le misure pratiche per la riduzione del rischio, come il controllo degli accessi, l'incremento della sicurezza della rete con mezzi tecnici e anche le misure organizzative per la riduzione dei rischi in materia di Security. Dopo avere superato l'esame, i partecipanti ottengono un attestato, riconosciuto a livello mondiale, da TÜV NORD che ne certifica la qualifica di "CESA-Certified Expert for Security in Automation".

Con il nuovo servizio Industrial Security Consulting Service (ISCS), Pilz amplia l'analisi sulla tecnica di sicurezza delle macchine con una osservazione olistica di safety e security. A partire da una metodologia di comprovata efficacia per servizi e prestazioni nel settore della sicurezza funzionale delle macchine e sulla base della serie di norme sulla security IEC 62443, Pilz ha sviluppato un'offerta che, una volta implementata, consente alle aziende di essere preparate al meglio in tema Industrial Security e di soddisfare le disposizioni di legge più recenti.

Quattro moduli per una Industrial Security migliorata

ISCS si compone di 4 moduli: analisi delle esigenze di protezione, valutazione del rischio di Industrial Security, concept di Industrial Security e verifica di sistema Industrial Security.

Nell’analisi delle esigenze di protezione, gli esperti Pilz determinano il fabbisogno di protezione, all’interno dell’azienda, per quanto riguarda i singoli “asset” della macchina o dell’impianto nonché i relativi obiettivi di protezione. Nella seconda fase, ossia la valutazione del rischio, vengono considerati tutti i rischi e la loro probabilità di accadimento, per ogni sottoarea per l’intero ciclo di vita del sistema. Successivamente gli esperti di Pilz discutono con i clienti le possibili soluzioni per la mitigazione dei rischi rilevati e per eventuali pericoli.

Nella terza fase, gli esperti Pilz creano il concept Industrial Security con strategie e misure mirate alla difesa e riduzione di rischi generati da attacchi, manipolazioni e usi errati. Vengono inoltre create policy, disposizioni e linee guida per l’ulteriore realizzazione o funzionamento sicuri del sistema. Nell’ultima fase, la verifica del sistema di Industrial Security, viene controllata l’efficacia delle contromisure implementate.

Garantire la disponibilità delle macchine

Industrial Security Consulting Service supporta nella mitigazione o nelle prevenzione di cyberattacchi. Si riduce anche il numero di incidenti alla sicurezza innescati involontariamente. A sua volta, ciò incrementa la disponibilità delle macchine e, in ultima istanza, consente di risparmiare in termini di costi e mantenere una redditività efficiente.

Il compito principale di ISCS è proteggere il personale addetto alla macchine con misure di security idonee: un incidente di security può infatti trasformarsi in un ostacolo alle misure di safety. Una barriera fotoelettrica, ad esempio, davanti a una macchina si occupa di evitare che l’operatore entri in una zona pericolosa. Se tuttavia un hacker riesce a introdursi nel relativo sistema di controllo e nel meccanismo,

è possibile che la funzione di protezione della barriera fotoelettrica non sia più garantita. La Security protegge la Safety!

Fabbricanti di macchine e operatori riceveranno così da Pilz un'offerta di servizi che prende in considerazione tutti gli aspetti inerenti alla protezione di uomo e macchina.

Per la concreta implementazione nella macchina è quindi altamente opportuno un approccio comune di safety e security. Questo perché non c'è safety senza security e senza safety non c'è protezione per l'essere umano.

Regolamentazione chiara e precisa: chi può fare cosa sulla macchina?

La sicurezza di una macchina e dei suoi operatori dipende dalla regolamentazione degli accessi, sia che si tratti di persone o di reti. Gli accessi devono essere protetti da interventi non autorizzati, ad esempio durante il funzionamento della macchina le persone non possono sostare all'interno della zona pericolosa. Se un operatore macchina autorizzato si trova all'interno di questa zona per ragioni di manutenzione, occorre assicurare che nessuna altra persona effettui interventi sull'impianto in quello stesso momento. Infatti, anche le migliori intenzioni in termini di funzionamento, servizio o manutenzione relativamente a un impianto, sia in loco che tramite rete, potrebbero altrimenti avere conseguenze fatali.

Una parte costitutiva importante è l'implementazione di un sistema di Identity and Access Management (IAM) che disciplini in modo chiaro autorizzazioni e accessi a macchine e impianti all'interno dell'azienda. Rientrano in tale ambito misure e disposizioni di tipo organizzativo e anche funzioni di sicurezza adeguate. Un sistema di autorizzazione all'accesso come PITreader di Pilz rappresenta quindi il modulo

prodotto adatto. In questo modo, gli utenti sono in grado di far fronte alle sfide poste in materia di tutela della salute e incolumità del personale, responsabilità civile, produttività ai massimi livelli e protezione dei dati.

Con il sistema di selezione della modalità operativa e autorizzazione all'accesso PITmode fusion, Pilz offre una scelta della modalità operativa sicura e funzionale e anche una regolamentazione dell'autorizzazione all'accesso a macchine e impianti: su un transponder codificato RFID, ogni operatore ottiene le autorizzazioni a operare sulla macchina corrispondenti al proprio livello di competenza e qualifica. L'impianto può così essere comandato e controllato unicamente dalle persone autorizzate nelle modalità operative specificate. In questo modo viene definito un livello elevato di protezione contro azioni, manipolazioni e manomissioni involontarie.

Se il sistema di selezione della modalità operativa e di autorizzazione all'accesso viene integrato con i componenti di un sistema modulare per ripari mobili, si crea un concept coerente di regolazione dell'accesso alla macchina, attento ai punti di vista correlati a safety e security.

La migliore messa in sicurezza dei ripari mobili non serve a nulla se i dati, il know-how e i flussi operativi non sono sufficientemente protetti da accessi non autorizzati e da manipolazioni/manomissioni e da possibili attacchi al sistema di controllo da parte di hacker.

Protezione da attacchi esterni grazie all'Industrial Firewall

L'Industrial Firewall SecurityBridge di Pilz protegge le reti di automazione dagli interventi provenienti dall'esterno. Il firewall supervisiona il traffico dei dati tra PC e sistema di controllo e riduce

così l’area esposta agli attacchi hacker e a manipolazioni/manomissioni. SecurityBridge protegge da manipolazioni e manomissioni non solo i sistemi di controllo Pilz ma anche i sistemi di controllo di terzi.

La convinzione di Pilz si fonda sulla certezza che solo un approccio olistico a safety e security possa garantire una protezione completa per l’uomo e per la macchina. Se occuparsi di security e a quale livello occuparsene non è più qualcosa lasciato alla discrezionalità di un’azienda. Nel frattempo questo aspetto è diventato disposizione di legge. Nella costruzione delle macchine, la security intesa come Industrial Security, non è demandata unicamente all’IT ma anche parte integrante del concept e della costruzione. L’implementazione a posteriori della security è onerosa in termini di tempi e costi e implica spesso sacrificare semplicità d’uso per l’utente, funzionalità e produttività.

((Caratteri: 10.173))

((Box:))

La legislazione UE sul tema Industrial Security: una panoramica

In Europa in particolare, il legislatore risponde al panorama delle minacce con una serie di leggi. È per questa ragione che l’Europa vanta le disposizioni più severe in materia al mondo. Sono comunque in corso armonizzazioni con altri Paesi e anche lì arriveranno leggi simili. Si può quindi prospettare un’armonizzazione di portata mondiale per quanto concerne l’Industrial Security.

NIS 2: più obblighi per le aziende

La NIS (Network and Information Security) è una direttiva dell'Unione Europea tesa a rafforzare la sicurezza informatica. Si tratta di una direttiva già in vigore dal 2016 che interessava, finora, i player attivi in infrastrutture critiche, tra cui i settori energia, trasporti, banche e finanza, sanitario, approvvigionamento e distribuzione di acqua potabile e anche infrastrutture digitali. I fornitori di questi settori erano tenuti, con particolare riferimento alla security, ad adottare "idonee disposizioni e misure di sicurezza" e a notificare incidenti ed eventi gravi in materia di sicurezza informatica. La nuova Direttiva relativa a misure per un livello comune elevato di cibersicurezza 2 EU 2022/2555 (NIS 2) obbligherà in futuro un numero considerevolmente maggiore di aziende ad adottare misure di Risk Management per la cibersicurezza. NIS 2 estende, ad esempio, i settori coinvolti aggiungendo l'industria manifatturiera/produttiva, tra cui anche l'automotive e i produttori di apparecchiature elettriche.

Le analisi dei rischi e i concept di sicurezza sono richiesti per i sistemi informatici, la protezione della supply chain e la sicurezza del personale. A tutto questo si aggiungono approcci mirati al controllo degli interventi e alla gestione degli impianti come pure corsi di formazione obbligatori per il management.

La direttiva è stata approvata dal Parlamento e dal Consiglio dell'Unione a fine 2022. Come tutte le direttive UE, anche NIS 2 non entra in vigore subito e in modo vincolante nei singoli Stati membri UE ma deve essere prima recepita come legge nazionale. Entro il 18 ottobre 2024, gli Stati membri hanno l'obbligo di convertire la direttiva in legge nazionale. Le aziende sono invitate a prendere quanto prima in considerazione NIS 2 e a svolgere un'analisi esaustiva della propria security. In questa analisi rientra, ad esempio, la realizzazione di un sistema di gestione della sicurezza delle informazioni (ISMS -

Information Security Management System). Al riguardo può rivelarsi utile una certificazione secondo la norma ISO 27001 sulla sicurezza delle informazioni.

NIS 2 applicata agli impianti eolici: con l'avvento di NIS 2, anche i costruttori di macchine, come del resto chi si occupi di realizzare impianti per la produzione di energia elettrica (ad es. impianti eolici), dovranno soddisfare i requisiti della nuova normativa. Il fabbricante di impianti eolici necessita a sua volta di soluzioni di automazione, sistemi di controllo o sensori. A partire da una determinata dimensione, anche i fabbricanti di componenti elettrici sono soggetti alla NIS 2. NIS 2, inoltre, prescrive la massima attenzione verso i fornitori e quindi un'azienda come Pilz deve occuparsi anche dell'implementazione di una supply chain sicura e stabilire requisiti specifici per i propri fornitori. NIS 2 copre tutti gli aspetti della supply chain.

Il nuovo Regolamento macchine: niente marcatura CE senza security

Nel quadro della sicurezza funzionale delle macchine, la Direttiva Macchine 2006/42/CE riveste un'importanza fondamentale:

per potere introdurre macchine sul mercato europeo, i costruttori di macchine sono da sempre tenuti a eseguire una corrispondente procedura di valutazione della conformità al termine della quale si ottiene la Marcatura CE.

Nel giugno 2023, con la nuova denominazione di Regolamento Macchine, è stato pubblicato il documento con le disposizioni allo stato dell'arte della tecnica e tecnologia. Trattandosi di un regolamento non è necessaria la conversione preliminare in legge

nazionale. I costruttori di macchine avranno tempo fino al 20 gennaio 2027 per adeguarsi ai nuovi requisiti e recepirli entro la scadenza.

Il Regolamento Macchine sostituisce la Direttiva Macchine in vigore, rendendo obbligatoria la cyber security a differenza di quanto stabiliva la normativa precedente. Se la Direttiva Macchine era una semplice riflessione sulla safety, nel Regolamento l'obiettivo di protezione Security è stato recepito alla voce "Protection against corruption" all'interno della sezione "Essential health and safety requirements EHSR": le funzioni di sicurezza della macchina non devono essere pregiudicate da un'alterazione involontaria o intenzionale.

Questo nuovo percorso verso la marcatura CE solleva tutta una serie di nuovi quesiti e domande per costruttori e operatori di macchine: dovranno infatti rivedere e rielaborare i concept di sicurezza finora in uso per safety e security.

Cyber Resilience Act: security per l'intero ciclo di vita del prodotto

Oltre a considerare l'approccio dell'azienda e delle macchine, è imprescindibile implementare anche le misure di security direttamente nei dispositivi (come ad esempio nei sistemi di controllo). Nel settembre 2022, la Commissione Europea ha presentato la bozza di un regolamento il cui obiettivo è l'innalzamento del livello di sicurezza informatica dei prodotti. Il Cyber Resilience Act (CRA) si rivolge ai fabbricanti di prodotti con elementi digitali (hardware e software) che sono in grado di comunicare con altri prodotti. Coinvolti sono 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 o la macchina stessa.

Quale sarà di fatto l’entità degli effetti del CRA dipende dai criteri che saranno in ultima istanza stabiliti per la classificazione dei prodotti. Secondo il CRA dovranno essere commercializzati solo i prodotti in grado di assicurare un livello di sicurezza informatica adeguato, più precisamente per l’intero ciclo di vita del prodotto. La security inizia dunque con lo sviluppo del prodotto. Da qualche anno Pilz conforma quindi i propri processi di sviluppo anche alla norma IEC 62443-4-1 “Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements“ e ha sviluppato ad esempio SecurityBridge comprovatamente “secure”.

((Caratteri: 5.826))

Immagini

Fig. 1

Grafik_aus_Prospekt_Schulungen_mit_Pilz_3c_ppt

Safety e Security da un unico fornitore: Pilz propone un'offerta completa di soluzioni con servizi e prodotti per l'Industrial Security della macchina.

Copyright: Pilz GmbH & Co. KG

Fig. 2:

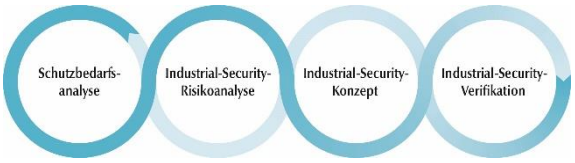
F_Services_ISCS_two_men_tablet_in_discussion_get1150297892_cold1_v0

Industrial Security Consulting Service, il nuovo servizio offerto da Pilz, aiuta le aziende a rendere sicure le proprie macchine e i propri impianti.

Copyright: © Westend61/[westend61] via Getty Images),© Pilz GmbH & Co. KG

Fig. 3:

G_Cycle_Industrial_Security_de_v0



L’offerta di servizi e prestazioni Industrial Security Consulting Service di Pilz è composta da 4 moduli: analisi delle esigenze di protezione, valutazione del rischio di Industrial Security, concept di Industrial Security e verifica di sistema Industrial Security.

Copyright: Pilz GmbH & Co. KG

Fig. 4:

F_Press_IAM_Man_using_PITreader_Key_Get1169337234_Get1169337153_cold1_v2

Un sistema completo di Identity and Access Management regolamenta l’accesso all’applicazione e garantisce quindi l’integrità delle funzioni e delle misure di sicurezza, Safety e Industrial Security incluse.

Copyright: © Westend61/[Westend61] via Getty Images, © Pilz GmbH & Co. KG

Fig. 5:

F_security_robot_man_virtual_world_Fot208731449_cold1_2019_06_v2

Con Industrial Security si intende la protezione di impianti industriali e produttivi da errori volontari e casuali. Il suo obiettivo è garantire la disponibilità di macchine e impianti, così come l'integrità e la riservatezza di dati e processi meccanici.

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 2.500 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.

www.pilz.com

Pilz sui social network:

Sui canali social media Pilz sono disponibili informazioni di carattere generale sull'azienda e le persone; forniscono inoltre informazioni aggiornate su tecnica e tecnologia dell'automazione.

www.pilz.com/facebook
www.pilz.com/X
www.pilz.com/xing
www.pilz.com/youtube
www.pilz.com/linkedin

Contatti per la stampa:

Martin Kurth
Stampa specializzata e aziendale
Tel: +49 711 3409-158
m.kurth@pilz.de

Sabine Karrer
Stampa specializzata e aziendale
Tel: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Eva Rössle
Stampa specializzata
Tel: +49 711 3409-7147
e.roessle@pilz.de

Hansjörg Sperling-Wohlgemuth
Gestione Congressi e Conferenze
Tel: +49 711 3409-239
h.sperling@pilz.de