GIORNATA MONDIALE DELLA SICUREZZA 2025

SICUREZZA 365:
OGNI GIORNO CONTA

COMMISSIONI Sicurezza Industriale e ICT

29 aprile 2025
dalle 12:00
alle 13:00

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI TORINO

Cybersecurity nell'automazione industriale: minacce, impatti e scenari futuri

Simone Bizzarri

CONTENUTI

1. **Introduzione**: Perché la cybersecurity è fondamentale nell'industria
2. **Definizione di Cybersecurity**
3. **Perché parlare di cybersecurity industriale**
4. **Tipologie di attacchi informatici principali**: Virus e malware, Phishing, Attacchi DDoS, Hacking, Ransomware, Ingegneria sociale, spoofing, sniffing, insider
5. **Focus su Virus e Malware**: contromisure pratiche
6. **Attacchi Hacking specifici e difese**
7. **Aspetti di cybersecurity specifici per Industria 4.0**: Protezione dati, Sicurezza reti industriali, Vulnerabilità, Formazione utenti, Collaborazione settoriale
8. **Use Case: Attacco a un sistema CNC**: Architettura sistema CNC – IIoT, Punti deboli del sistema, Possibili difese pratiche
9. **Il nuovo Regolamento Macchine (UE 2023/1230):** Introduzione dei rischi di cybersecurity, Requisiti di protezione hardware/software, Nuovi obblighi per produttori e operatori
10. **Conclusioni**

CYBERSECURITY: DEFINIZIONE E ATTIVITÀ PRINCIPALI

La cybersecurity, anche nota come sicurezza informatica, è un campo che si occupa di proteggere i sistemi informatici, le reti e i dati da accessi non autorizzati, danni o intrusioni.

Essa comprende una serie di pratiche, strumenti e misure di sicurezza volte a prevenire, rilevare e rispondere alle minacce informatiche.
La cybersecurity si occupa di proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e dei sistemi digitali. Ciò include la protezione dei dati personali e sensibili, la prevenzione degli attacchi informatici, la gestione delle vulnerabilità e la risposta agli incidenti di sicurezza.
Le attività di cybersecurity possono comprendere:
l'implementazione di ***firewall***, ***sistemi di rilevamento*** *delle intrusioni,* ***crittografia*** *dei dati,* ***autenticazione*** *multi-fattore,* ***monitoraggio dei log*** *di sistema,* ***test di penetrazione*** *e* ***formazione degli utenti*** *per promuovere la consapevolezza sulla sicurezza.*

L'obiettivo principale della cybersecurity è garantire la protezione dei sistemi e dei dati da minacce interne ed esterne, come malware, phishing, attacchi DDoS, violazioni dei dati e altre forme di attività malevole.

PERCHÉ PARLARE DI CYBERSECURITY INDUSTRIALE?

I cyber attacchi rappresentano una minaccia sempre più rilevante per i sistemi automatici e integrati di processo industriale. Tra le tipologie di attacchi più rilevanti si possono includere:

- **Ransomware**: Questi attacchi bloccano l'accesso ai sistemi o ai dati dell'azienda, richiedendo un pagamento per ripristinare l'accesso. Possono causare interruzioni significative nei processi produttivi e nella raccolta dei dati

- **Phishing**: Gli attacchi di phishing cercano di ottenere informazioni sensibili tramite l'inganno dei dipendenti, ad esempio attraverso e-mail fraudolente o siti web contraffatti. Una volta ottenute le credenziali, gli aggressori possono accedere ai sistemi e compromettere la sicurezza

- **Denial-of-Service (DoS):** Questi attacchi sovraccaricano i sistemi con un'elevata quantità di traffico, rendendoli inutilizzabili e causando interruzioni nei processi di produzione.

I sistemi target di questi attacchi includono le **macchine CNC**, i **sistemi di controllo automatico di processo** e i **sistemi informatici cloud-based** per la raccolta dei dati da un sistema **IIoT**.

TIPOLOGIE DI ATTACCHI INFORMATICI (1/2)

Virus e malware	• programmi dannosi che possono infettare un sistema informatico e causare danni ai dati o al software
Phishing	• tentativi di frode online in cui gli hacker cercano di ottenere informazioni personali
Attacchi DDoS (”Distributed Denial of Service”)	• attacchi informatici che mirano a sovraccaricare un sistema o una rete con una grande quantità di traffico
Attacchi di hacking	• tentativi di accedere illegalmente a un sistema informatico o a una rete
Attacchi di ransomware	• attacchi informatici in cui gli hacker bloccano l’accesso ai dati o ai sistemi informatici

TIPOLOGIE DI ATTACCHI INFORMATICI (2/2)

Attacchi di ingegneria sociale	• coinvolgono la manipolazione psicologica delle persone per ottenere accesso non autorizzato a sistemi o informazioni riservate
Attacchi di spoofing	• implicano la falsificazione dell'identità o dell'origine di un'entità o di un sistema
Attacchi di sniffing	• coinvolgono il monitoraggio e l'intercettazione del traffico di rete al fine di ottenere informazioni sensibili come password o dati personali
Attacchi di insider	• vengono perpetrati da individui interni all'organizzazione, come dipendenti o collaboratori

ATTACCHI HACKING NON COMPRESI NELLE ALTRE CATEGORIE

Attacchi di forza bruta	• cercano di indovinare la password di un account utilizzando un elenco di password comuni o tentando tutte le possibili combinazioni di caratteri fino a quando non viene trovata quella corretta
Attacchi di man-in-the-middle (MitM)	• cercano di intercettare le comunicazioni tra due parti, ad esempio tra l'utente e il sito web, per rubare informazioni sensibili come le credenziali di accesso
Attacchi di injection	• cercano di inserire codice dannoso in un'applicazione web o in un database utilizzando input utente non validati

ALCUNE MISURE DI CONTRASTO (1/2)

- **Utilizzare software antivirus**
- **Mantenere il sistema operativo e le applicazioni aggiornate**
- **Fare attenzione alle e-mail e ai download**
- **Utilizzare una connessione ad Internet sicura**
- **Eseguire scansioni periodiche del sistema**
- **Fare il backup regolare dei dati**
- **Educazione degli utenti**

ALCUNE MISURE DI CONTRASTO (2/2)

- **Essere cauti con le email**
- **Verificare l'URL dei siti web**
- **Non fornire informazioni personali**
- **Utilizzare l'autenticazione a due fattori**

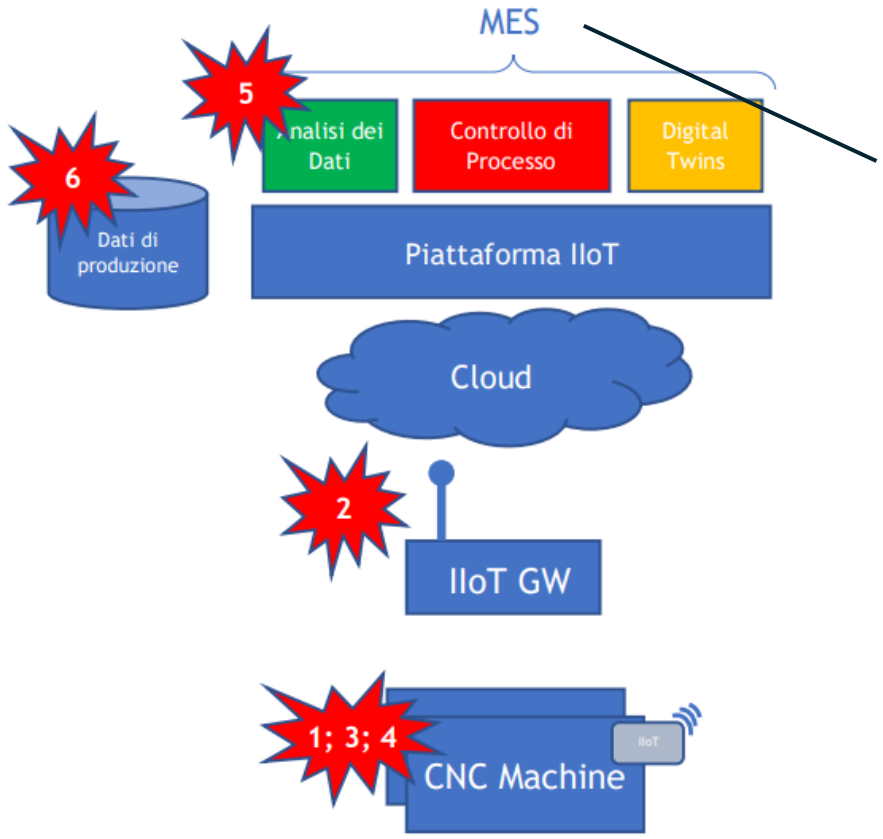
ASPETTI DI CYBER SECURITY SPECIFICI NELL'AMBITO DELL'INDUSTRIA 4.0

- **Protezione dei dati sensibili**
- **Sicurezza delle reti industriali**
- **Gestione delle vulnerabilità**
- **Formazione e consapevolezza degli utenti**
- **Collaborazione tra settori**

USE CASE - ATTACCO A UN SISTEMA CNC: ARCHITETTURA DI RIFERIMENTO

Il gateway IoT trasmette i dati raccolti dalle macchine utensili CNC a una piattaforma IIoT, che consente l'elaborazione, l'archiviazione e l'analisi dei dati

Le macchine utensili CNC sono connesse a un gateway IoT tramite protocolli di comunicazione standard (ad esempio OPC, MQTT o MTConnect) o tramite sensori e dispositivi di monitoraggio



La piattaforma IIoT può essere integrata con un sistema MES, che consente la gestione centralizzata della produzione.
Il sistema MES può utilizzare i dati delle macchine utensili CNC per la pianificazione delle attività, la gestione delle risorse e il controllo della qualità.

PUNTI DEBOLI DI UN SISTEMA CNC

Macchine utensili CNC: Le macchine utensili possono essere vulnerabili ad attacchi che cercano di compromettere il loro funzionamento o di alterare i parametri di produzione. Gli attaccanti potrebbero cercare di infiltrarsi nelle macchine tramite accessi non autorizzati o sfruttando vulnerabilità nel firmware o nel software.

Gateway IoT: I gateway IoT che fungono da interfaccia tra le macchine utensili e il sistema centrale possono essere soggetti ad attacchi mirati per ottenere accesso alle macchine o per interrompere la comunicazione tra le macchine e il sistema centrale. Gli attaccanti potrebbero cercare di sfruttare vulnerabilità nel software o nelle configurazioni dei gateway.

Rete di comunicazione: La rete utilizzata per la comunicazione tra le macchine utensili, i gateway e il sistema centrale può essere un punto di attacco potenziale. Gli attaccanti potrebbero cercare di intercettare, manipolare o interrompere la comunicazione tra i dispositivi.

Sistema di controllo e monitoraggio centrale: Il sistema centrale che gestisce e monitora le macchine utensili può essere un obiettivo per attacchi mirati. Gli attaccanti potrebbero cercare di ottenere accesso non autorizzato al sistema, manipolare i dati di monitoraggio o interrompere il funzionamento del sistema.

POSSIBILI AZIONI DI DIFESA DI UN SISTEMA CNC

- **Segmentazione della rete**
- **Implementare una rete di comunicazione dedicata**
- **Utilizzare un gateway di sicurezza**
- **Applicare segmentazione di rete**
- **Implementare controlli di accesso**
- **Monitoraggio costante**
- **Implementazione di autenticazione e autorizzazione robuste**
- **Monitoraggio del traffico di rete**
- **Aggiornamenti regolari del firmware e del software**
- **Crittografia dei dati**
- **Monitoraggio dei log e delle registrazioni**
- **Consapevolezza della sicurezza**

IL NUOVO REGOLAMENTO MACCHINE (UE 2023/1230) (REF. QUADRA)

Il 29 giugno 2023 è stato pubblicato il nuovo regolamento (UE) 2023/1230 relativo alle macchine, che andrà a sostituire la direttiva macchine 2006/42/CE.

Il Regolamento 2023/1230 introduce nuovi componenti di sicurezza
I componenti di sicurezza rientrano nel campo di applicazione della direttiva macchine e, come tali, devono essere marcati CE.
Nella definizione di "componente di sicurezza" del nuovo regolamento macchine sono stati introdotti anche i componenti digitali, compreso il software;
Il software che svolge funzioni di sicurezza immesso sul mercato separatamente dovrà quindi essere marcato CE ai sensi del regolamento macchine ed essere accompagnato da una dichiarazione di conformità UE e, per quanto necessario, da istruzioni per l'uso.

Intelligenza artificiale
Il nuovo regolamento macchine si applica ai sistemi che utilizzano tecnologie di intelligenza artificiale per gli aspetti che riguardano le possibili influenze sulla sicurezza delle macchine.
In particolare, la valutazione dei rischi dovrà tenere conto dell'evoluzione del comportamento delle macchine progettate per funzionare con diversi livelli di autonomia.

Il nuovo Regolamento macchine (UE) 2023/1230 richiede che vengano tenuti in considerazione anche i rischi provocati da **attacchi informatici**, requisito non previsto dall'attuale direttiva macchine 2006/42/CE.

IL NUOVO REGOLAMENTO MACCHINE (UE 2023/1230) (REF. QUADRA)

Il nuovo Regolamento macchine (UE) 2023/1230 richiede che vengano tenuti in considerazione anche i rischi provocati da **attacchi informatici**, requisito non previsto dall'attuale direttiva macchine 2006/42/CE.

Cosa prevede il Regolamento macchine per la cybersecurity?
Per affrontare i rischi provocati da attacchi informatici, nel nuovo Regolamento macchine è stato aggiunto un requisito essenziale di sicurezza e di tutela della salute, il requisito 1.1.9, che chiede che i sistemi informatici delle macchine siano protetti dall'alterazione; in particolare, tale requisito prevede che:

1. il collegamento alla macchina di un altro dispositivo non determini una situazione pericolosa;
2. i componenti hardware che permettono l'accesso al software legato alla sicurezza siano protetti da alterazioni accidentali o intenzionali;
3. la macchina raccolga prove in merito a interventi legittimi o illegittimi su tali componenti;
4. software e dati critici per la sicurezza siano individuati come tali e protetti da alterazioni accidentali o intenzionali;
5. informazioni su questi software siano facilmente disponibili in qualsiasi momento, ad esempio sul pannello di controllo della macchina;
6. la macchina raccolga prove in merito a interventi legittimi o illegittimi su tali software.

CONCLUSIONI

La cybersecurity industriale è oggi un pilastro fondamentale per garantire la continuità operativa e la sicurezza dei sistemi.
Il nuovo Regolamento Macchine (UE 2023/1230) rafforza l'integrazione tra sicurezza fisica e informatica.
Proteggere ogni giorno significa investire nel futuro.

Grazie per l'attenzione