Cosa dovrebbero sapere i Manager su cyber security industriale

Tratto dal White Paper "What Executives Need to Know About Industrial Control Systems Cybersecurity" di Joseph Weiss, PE, CISM, CRISC, ex Managing Director ISA99

Presentazione

La protezione delle informazioni e dei sistemi di controllo sta assumendo sempre più importanza in tutte le Aziende, e vengono scoperte violazioni della sicurezza informatica sempre più preoccupanti e significative.

Imprenditori e Manager sono oggi tenuti a identificare, classificare e mitigare continuamente i rischi, anche quelli derivanti da incidenti informatici.

Per affrontare il tema, provate a porvi le seguenti domande sull'esposizione della vostra Azienda alle vulnerabilità della sicurezza informatica dei sistemi utilizzati in produzione:

- Quali opportunità esistono per la violazione?
- Quale esposizione al rischio ha la mia Azienda e quali sono le conseguenze di tale esposizione?
- Qual è il danno massimo che potrebbe essere causato se si verifica una di queste violazioni?
- Quali misure di sicurezza specifiche proteggono ciascuna delle nostre risorse?
- Se i nostri sistemi presentano vulnerabilità di sicurezza informatica, in che modo tali vulnerabilità influiscono sui nostri obiettivi e iniziative in materia di sicurezza?
- Chi nella nostra organizzazione è responsabile di queste misure di sicurezza?
- I team IT e OT sono coordinati e lavorano insieme per proteggere i nostri sistemi?
- Abbiamo stanziato risorse adeguate, utilizziamo gli standard ed abbiamo l'attrezzatura giusta per darci il miglior risultato possibile?

Questo white paper affronta queste e altre domande nel contesto dei seguenti obiettivi:

- Capire le caratteristiche e le vulnerabilità uniche dei sistemi di controllo industriale;
- Vedere le principali differenze tra IT e OT sulla sicurezza informatica;
- Valutare i potenziali impatti di incidenti sulle infrastrutture critiche e sui processi di produzione;
- Identificare standard, formazione e programmi di awareness per le aziende

Per creare e mantenere sistemi sicuri, è necessario:

- Prima assicurarci che i nostri processi e le comunicazioni tra i diversi reparti aziendali siano efficaci
- Che ci sia consapevolezza che i sistemi di controllo industriale siano da proteggere.
- Terzo, dobbiamo arrivare e capire se i sistemi che utilizziamo siano intrinsecamente sicuri e tenuti aggiornati riguardo a vulnerabilità note, secondo standard di settore e i piani di conformità.
- Infine, dobbiamo valutare se il nostro personale abbia adeguata esperienza riguardo alla cyber security industriale e si coordini da vicino con il nostro personale IT per proteggere sistemi ed impianti.

Introduzione

Sistema di controllo industriale (ICS) è un termine generale che comprende diversi tipi di sistemi di controllo utilizzati nella produzione industriale.

A volte altri nomi o sigle vengono usati in modo intercambiabile (come ad esempio “SCADA”):

- Sistemi di controllo distribuito (DCS) che monitorano e controllano grandi impianti come centrali elettriche e raffinerie
- Sistemi SCADA (Supervisory Control and Data Acquisition) che monitorano e controllano asset dispersi come reti elettriche, acquedotti o anche impianti industriali
- Controllori logici programmabili (PLC) che controllano i singoli processi e macchinari
- Unità terminali remote (RTU) che fungono da concentratori di dati
- Dispositivi da campo “intelligenti”, come sensori che misurano il processo (pressione, temperatura, livello, flusso, ecc.), analizzatori che monitorano i componenti chimici, azionamenti che aprono e chiudono le valvole, fanno partire e fermano motori, ecc.

In sostanza, un sistema di controllo industriale è un sistema composto da diversi sistemi, progettato per monitorare e controllare i processi fisici e garantire operazioni e produzioni sicure ed automatizzate

Differenze tra IT Cybersecurity e ICS Cybersecurity

Incidenti informatici dannosi si verificano o vengono identificati di continuo.
Spesso sono violazioni dei dati, che compromettono la riservatezza di informazioni, e le conseguenze a volte non si limitano alle violazioni dei dati e alla compromissione dei dati personali.

I sistemi di controllo industriale utilizzati nelle infrastrutture critiche, nell’industria come nelle utility, utilizzano sistemi di controllo basati su computer.

Spesso indicati come sistemi "SCADA", OT e Industrial IoT, molti sono legati a processi critici dai quali la società moderna dipende e senza i quali non può continuare a funzionare.

In genere i sistemi OT non hanno l'aspetto di quelli utilizzati nell'ambiente IT aziendale convenzionale e, anche se utilizzano componenti e dispositivi comuni, non vengono monitorati per le minacce informatiche come quelli nell'ambiente IT aziendale.

È importante riconoscere e comprendere le differenze tra cyber security IT e cyber security OT/ICS e la figura qui sotto (tratta da un Survey di SANS 2019) evidenzia come alcuni dei fattori più significativi vengono considerati diversamente in ordine di importanza dai responsabili IT e da quelli OT.

Table 5. Critical Drivers for IIoT Security and Rankings by Responsible Party

	Driver	Overall Response	IT Team Rankings	OT Team Rankings
1	Protection of data (company, customer, vendor, other)	47.2%	1	6
2T	Protection of equipment and systems	40.5%	4T	3
2T	Protection against financial loss (assets, brand, company value)	40.5%	2	4T
4T	Compliance with industry regulations	36.0%	3	4T
4T	Increases in reliability, availability, efficiency, productivity	36.0%	4T	1
4T	Safety inside the operation	33.7%	6	2
7	Integration and synergistic alignment of IT and OT practices, policies and procedures	23.6%	7T	7T
8	Reduce corporate liability/improve enterprise risk management	16.9%	7T	9T
9	Safety outside of the operation	15.7%	9T	7T
10	Mitigate supply chain risks, both upstream and downstream	9.0%	9T	9T

Concentrarsi sulla sfida

Gli incidenti informatici sono stati definiti dagli enti di standardizzazione come eventi che mettono a rischio Riservatezza, Integrità o Disponibilità (RID) di un sistema informativo.

Secondo il NIST (The National Institute of Standards and Technology USA nist.gov) un incidente non deve necessariamente essere dannoso per essere significativo e per comportare rischi per il processo e le persone coinvolte nel processo.

Tuttavia, poiché quando si parla di sicurezza informatica si pensa subito all'IT, un incidente viene spesso effettivamente classificato come un attacco malizioso via Internet contro un sistema basato su Windows, e con l'intento di rubare informazioni.
In generale, nell'IT si parla di cyber security fine a sé stessa: l'IT lavora per identificare le vulnerabilità informatiche anche senza necessità di valutarne le conseguenze.

Sfortunatamente, questo paradigma non si applica agli ICS e non affronta l'aspetto più importante degli ICS: la sicurezza intesa come "safety".

Infatti, sono proprio le conseguenze che sono di maggiore interesse quando si considera la sicurezza dei sistemi di controllo critici, e molti di questi sistemi sono installati in strutture con un'aspettativa di vita prevista tra i 10 ed i 25 anni.

Le architetture e la stretta connessione con il processo controllato comporta che spesso non possono essere aggiornati facilmente alle ultime tecnologie informatiche, e non si possono installare patch in modo rapido ed automatico.

Con una aggravante: molti che lavorano nel settore lamentano una mancanza di attenzione da parte del Management delle Aziende e successiva difficoltà a farsi ascoltare, ed ottenere fondi per affrontare la cyber security in modo sistematico.

Nondimeno una rilevante parte della Minaccia Cyber riguarda tematiche inerenti a Cyber Crime (non legato solamente ad aspetti economici), Spionaggio/Sabotaggio e Warfare, tutte componenti che rendono appetibili proprio i sistemi ICS (pensiamo ai sistemi delle infrastrutture critiche) per gli aspetti legati alla sicurezza fisica e il potenziale impatto sull'opinione pubblica.

OT Cyber Security: casistica e incidenti

Uno dei motivi principali addotti per questa mancanza di attenzione è che c'è poca storia e casistica ed in passato sono stati segnalati pochi incidenti informatici ai sistemi di controllo ed automazione che abbiano causato danni

Un'eccezione è stato il "famoso Stuxnet" in Iran nel 2010: sfortunatamente, spesso ci si sente rispondere "Stuxnet non ci riguarda, non abbiamo centrifughe per arricchire uranio".

Niente potrebbe essere più lontano dalla verità: se un malware può mandare in tilt un PLC come successo nell'incidente di Stuxnet, lo stesso può essere utilizzato per attaccare un PLC che gestisce un impianto industriale (come è poi successo), un gasdotto, una centrale elettrica, una rete idrica o impianto di trattamento delle acque reflue, sistema di sicurezza di un edificio e altro ancora.

Gli aspetti più importanti nei sistemi di controllo industriale sono Affidabilità e Safety.

Di conseguenza, il personale di ICS ha preoccupazioni diverse; sono focalizzati sulle minacce informatiche (dannose o non intenzionali) solo se influenzano l'affidabilità (continuità operativa) e la safety.

Ciò significa che i problemi legati alla cyber security riguardano:

- Perdita di visibilità sul processo/impianto: se guido un'auto, gli strumenti sul cruscotto funzionano e posso fidarmi delle informazioni che trasmettono?
- Perdita di controllo: mentre guido, continuo ad avere il controllo diretto sul pedale dell'acceleratore, del pedale del freno e del volante?

Entrambi questi problemi sono stati fattori chiave di quanto accaduto con Stuxnet: le centrifughe giravano senza controllo e il display indicava all'operatore che non c'erano problemi.

Le vulnerabilità dei sistemi di controllo sono importanti?

Chi ha interesse ad attaccare impianti nell'industria e nelle utility, è alla ricerca di exploit con cui è possibile danneggiare i processi fisici: già si immagina la devastazione e il conseguente terrore che sarebbero causati dal danno ad una centrale elettrica, ad una acciaieria o all'interruzione di erogazione di un servizio essenziale, come ad esempio la compromissione della rete elettrica o l'approvvigionamento idrico.

I dispositivi che possono causare danni catastrofici attraverso il funzionamento remoto dei componenti informatici sono un obiettivo ideale per i compromessi: pensiamo anche all' IIoT (Industrial IoT).

Ne consegue che dovremmo proteggere questi dispositivi un "bersaglio" per evitare che:
a) possano essere oggetto di incidenti e attacchi dannosi
b) garantire che le azioni non dolose di un insider (personale nella stessa Azienda o manutentori esterni) non causino incidenti informatici involontari.

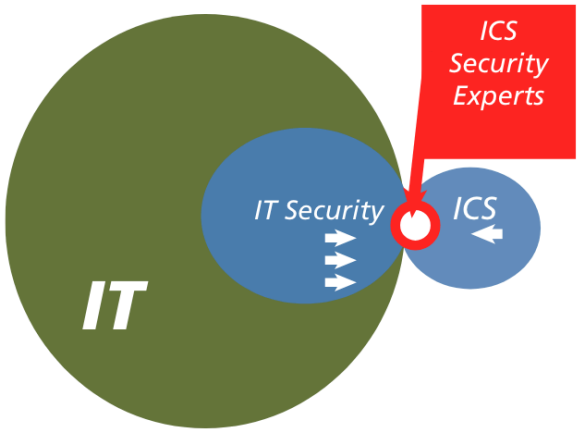
Dal punto di vista metodologico, un esperto di cyber security dei sistemi di controllo industriale esamina architettura ed i sistemi connessi in modo olistico, identificando le vulnerabilità fisiche dei dispositivi di automazione e del processo e cercando i modi per sfruttare le vulnerabilità mediante manipolazioni informatiche.

Sono poche le persone con l'esperienza necessaria per comprendere sia il processo fisico controllato che il dominio del sistema di controllo con le sue caratteristiche di architettura e conosca come affrontare le vulnerabilità IT/OT.

Questa potrebbe essere la descrizione di esperti di ICS Cybersecurity: ovvero persone che colmano i divari tra queste aree di competenza tradizionali.

Il personale IT in genere formazione in informatica con poco background ingegneristico, mentre il personale operativo ha background ingegneristico con poca formazione sulla sicurezza.

Esiste un divario tra le organizzazioni IT e OT, ed è responsabilità del management e abbattere queste divisioni organizzative ad esempio mediante la creazione di nuove figure professionali “ibride” o migliorando, in maniera incrociata, le skill delle due aree professionali.



ICS Cybersecurity Experts bridge the gap between IT Security expertise and Industrial Control Systems expertise—a rare combination of skills in high demand today.

L’importanza delle skill in IT e OT Cyber Security

Gli esperti di sicurezza IT sanno tutto su server, client, Windows e protocolli IP e dispongono di numerosi tipi di tecnologie per cercare minacce informatiche a livello di Windows e IP, ma poca comprensione e pochissimi strumenti "al di sotto del livello IP".

Il personale dei sistemi di controllo è in genere concentrato sull'affidabilità operativa e sulla safety, non sulla sicurezza informatica.

Ne consegue che sono rari gli specialisti di computer forensics che abbiano una formazione minima per identificare gli incidenti informatici ICS.

Certo ci sono i CERT (Computer Emergency Response Teams CERT) che dispongono di database con centinaia di migliaia di cyber probe e attacchi, ma pochi, incidenti ICS/OT censiti.

Inoltre, sono poche o nessuna le normative per garantire che gli incidenti informatici ICS siano esaminati in modo forense per identificare vere cause ed effetti.
La mancanza di un'analisi forense adeguata può mettere in discussione i risultati ufficiali sulla verifica e l'attribuzione: questi fattori sono dettagli importanti per scopi assicurativi e di compliance, nonché informazioni preziose in vista di tecnologie informatiche in evoluzione per fronteggiare anche questi incidenti cyber.

Nell'ambiente IT, sono da tempo disponibili tecnologie per monitorare e identificare gli attacchi informatici (sebbene siano stati molti i casi in cui sistemi compromessi siano stati scoperti con il ritardo di mesi…).

Nel mondo OT questi tool hanno iniziato ad affacciarsi sul mercato solo negli ultimi anni e sono ancora in fase di sviluppo/affinamento e di accettazione da parte di molti.

Infatti, per i sistemi di controllo la casistica è differente. Vediamo un esempio.
Quando si verifica un evento o un disservizio come un blackout elettrico o la rottura di un tubo, i risultati sono immediati e l'impatto non può essere nascosto.
Senza la prospettiva di un esperto di cyber security industriale, può essere difficile determinare se la causa sia un incidente cyber, una violazione informatica o un “semplice” guasto.

Gli esperti di cyber security industriale infatti:
- Capiscono il processo fisico controllato
- Comprendono architettura del sistema di controllo con le sue caratteristiche
- Comprendono i rischi e le mitigazioni delle vulnerabilità IT/OT sfruttabili
- Hanno una buona conoscenza degli standard di settore e comprendono come si applicano a persone, processi e prodotti
- Possono colmare il divario di conoscenze tra l'organizzazione IT e OT

Il divario culturale che l’IT e l’OT può rendere più complesso proteggere i sistemi di controllo industriale, aggravando quindi l’esposizione al rischio.

Standard di settore e compliance: su cosa ci possiamo basare?

La sicurezza informatica di ICS è un problema globale e la sfida si estende a processi, persone e apparecchiature.

Al fine di disegnare, installare e mantenere sistemi di controllo sicuri:

- dobbiamo garantire che i nostri processi e la comunicazione tra loro siano protetti;
- dobbiamo assicurarci che il nostro personale sia formato e abbia esperienza nella cyber security industriale;
- dobbiamo assicurarci che i componenti dei sistemi siano intrinsecamente sicuri e aggiornati nei confronti di vulnerabilità note.

ISA (www.isa.org) è associazione leader per chi si occupa di sistemi di automazione, strumentazione e controllo industriale ed ha lavorato a lungo (dal 1999) sull'unico standard di sicurezza informatica industriale adottato in tutto il mondo.

Il comitato per lo sviluppo degli standard ISA99 riunisce esperti mondiali di cyber security industriale provenienti dall'industria, dai governi e dal mondo accademico per sviluppare la serie di standard ISA / IEC 62443 sull'automazione industriale e la sicurezza dei sistemi di controllo, guidati dai processi accreditati dell'ANSI (American National Standards Institute).

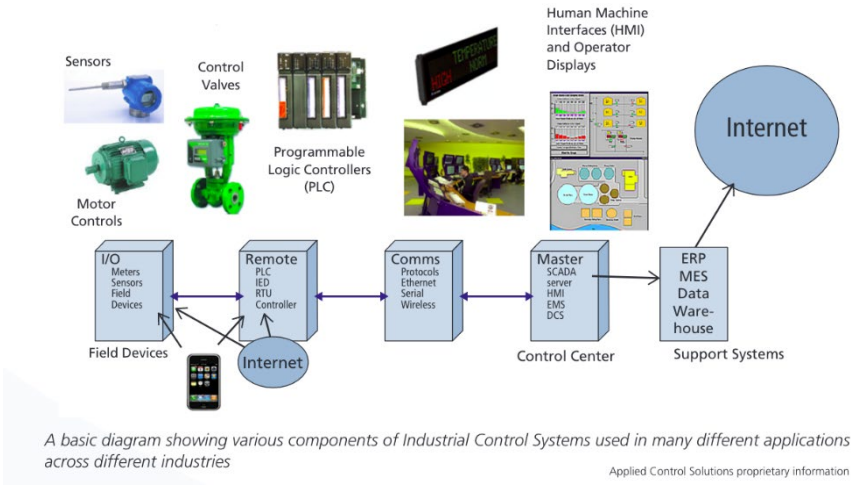
Lo standard ISA / IEC 62443 definisce i requisiti e le procedure per l'implementazione di sistemi di automazione e di controllo industriale sicuri, pratiche di sicurezza e per valutare anche la safety.

Lo standard ISA / IEC 62443 affronta la sfida della sicurezza informatica in modo olistico, colmando il divario OT e IT, e tra safety dei processi industriali e cyber security.

Data la convergenza IT-OT, dove le vulnerabilità sfruttate in un settore possono avere un impatto e danneggiare più reparti e settori, è essenziale che gli standard di sicurezza informatica siano ampiamente applicabili da chiunque.

La serie di standard ISA / IEC 62443 per la cyber security industriale è un'iniziativa applicabile a tutti i settori, nell'industria come nelle utility/infrastrutture critiche.

ISO/TR 22100-4:2018(EN) Safety of machinery — Relationship with ISO 12100 — Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects è un'interessante guida per i costruttori di machine per la valutazione del possibile impatto degli aspetti di Cyber Security con le normative di Sicurezza Fisica di un macchinario.



A basic diagram showing various components of Industrial Control Systems used in many different applications across different industries

Applied Control Solutions proprietary information

Raccomandazioni e conclusioni

La cyber security industriale è un problema con molteplici sfaccettature, che abbraccia persone, tecnologia, processi, apparecchiature e supera le tradizionali barriere geografiche, industriali e applicative.

Le vulnerabilità e gli attacchi associati, dolosi o involontari, possono portare conseguenze finanziarie, di sicurezza e di reputazione dell'Azienda e del marchio devastanti ed il Management dovrebbe considerare attentamente la propria esposizione a questi rischi.

Ci sono divari di cultura, conoscenza ed esperienza tra il personale IT e OT nella maggior parte delle Aziende e il coordinamento di queste funzioni con la presenza di esperti di cyber security industriale è fondamentale per il successo di un programma completo di sicurezza informatica.

Gli standard globali di consenso incentrati sulla cyber security industriale (come ISA/IEC 62443) possono aiutare a colmare il divario tra IT e OT e tra Safety e sicurezza informatica.

Possiamo rendere i nostri sistemi più affidabili, meno sensibili a incidenti informatici, a violazioni dolose o involontarie e proteggere la sicurezza delle nostre persone, degli impianti, dell'ambiente e dei nostri processi nell'industria come nelle utility e nelle infrastrutture critiche.