Guida pratica per l'IEC 62443

Come certificare le macchine in conformità allo standard

Minacce al settore manifatturiero

Negli ultimi decenni le normative e gli standard delle macchine si sono concentrati sulla sicurezza fisica. Ciò ha comportato un aumento delle funzionalità legate ad essa. Le macchine sono più sicure e il danno agli operatori e agli utenti finora è raro. Tuttavia, se da un lato la qualità e la sicurezza delle macchine sono migliorate, dall'altro le sfide sono cambiate: le minacce sono diventate digitali anziché fisiche.

La cybersecurity è diventata una vera sfida per l'industria manifatturiera. Le macchine sono spesso installate in complesse reti di fabbrica con elevati requisiti di uptime, utilizzando software obsoleti e vulnerabili. Pagare un riscatto di solito è più conveniente di un fermo di produzione. Ciò rende il settore manifatturiero il bersaglio perfetto per i criminali informatici.

Nel frattempo, le risorse, le competenze e la motivazione degli hacker sono aumentate. I criminali cercano di chiedere un riscatto dopo aver bloccato le macchine o rubato dati sensibili come dati, ricette di produzione e proprietà intellettuale. Il risultato è un danno economico e di reputazione.

IXON considera lo standard internazionale IEC 62443 come parte della soluzione. In questa guida rapida spieghiamo perché e come iniziare.

Perché l'IEC 62443?

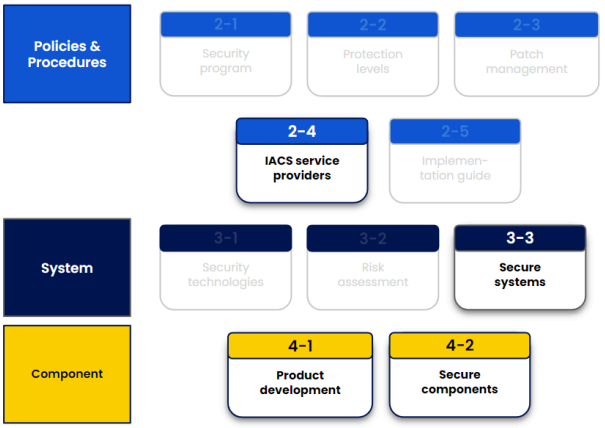
Lo standard IEC 62443 fornisce linee guida, regole e definizioni per affrontare le minacce alla sicurezza, attuali e future, specificamente per i Sistemi di Automazione e Controllo Industriale (IACS). Altri standard di sicurezza più generali come l'ISO 27001 sono destinati a tutti i tipi di aziende, anziché essere adattati alle esigenze di un settore specifico.

Tuttavia uno standard fatto per tutti è uno standard fatto per nessuno. Le linee guida degli standard generali come l'ISO 27001 sono intenzionalmente vaghe e aperte all'interpretazione, perché devono applicarsi a più aziende possibile. Questo li rende meno utili se l'obiettivo è diventare veramente più sicuri.

L'IEC 62443 è specifico, concreto e flessibile. Può essere considerato lo standard di riferimento per l'industria manifatturiera. Il mercato sta iniziando a richiederne la conformità e gli Stati lo usano come riferimento per normative e direttive. Lo standard può anche costituire la base per dimostrare la conformità a diverse direttive e atti europei, come la **NIS2** e il **Cyber Resilience Act.** L'adesione all'IEC 62443 dimostra che un'organizzazione prende la cybersecurity sul serio e che è pronta per qualsiasi regolamentazione in materia.

Come funziona

L'IEC 62443 è un insieme di standard redatti dall'International Electrotechnical Commission (IEC) e organizzati in categorie. Solo alcune delle sottocategorie meritano particolare attenzione. La sottocategoria più importante per i produttori di macchine è l'IEC 62443-3-3 perché elenca i requisiti per sistemi e macchine sicure. Le altre norme forniscono contesto, definizioni o requisiti per i componenti.



Di seguito è riportato un esempio di un requisito della sottocategorie 3-3:

"Protezione delle informazioni di audit - Il sistema di controllo deve proteggere le informazioni di audit e gli strumenti di audit dall'accesso non autorizzato, dalla modifica e dalla cancellazione."

I log di audit sono essenziali per la cybersecurity. Quando qualcosa va storto, occorre scoprire cosa, quando e come è successo, e chi ne è responsabile. Quindi è necessario proteggere i log di audit dagli utenti non autorizzati per ottemperare a questo requisito.

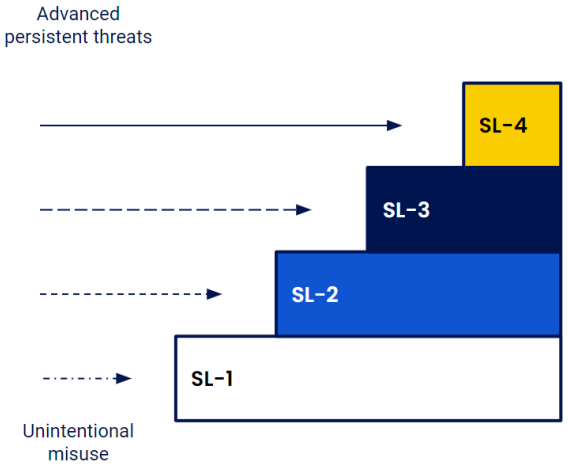
Security Levels

Per ogni requisito dell'IEC 62443, è possibile raggiungere un "Security Level" (SL). Un SL è una misura concreta di sicurezza e può essere comunicato ai partner e ai clienti. È un punteggio da 1 a 4 che misura le difese contro la forza, la capacità e la motivazione di un hacker. Tra tutti i requisiti, quello con il SL più basso conta come il livello totale del sistema, perché la sicurezza è forte solo quanto il suo punto più debole. Gli hacker tendono a concentrarsi sulle parti più deboli delle vostre difese.

È possibile raggiungere un livello di sicurezza più elevato con i "Requirement Enhancements", che sono un'aggiunta al Requisito di Base. In questo esempio, il seguente Enhancements vi porta dal Livello 3 al Livello 4:

"Registri di audit su supporti non-sovrascrivibili - Il sistema di controllo deve fornire la capacità di produrre registri di audit su supporti hardware dedicati non-sovrascrivibili ."

Questa struttura a SL è ciò che conferisce all'IEC 62443 la sua flessibilità. Vi consente di puntare a misure di sicurezza che sono a un livello realistico per voi.



I passi per la certificazione della macchina

I passi seguenti vi aiutano a iniziare e a lavorare per certificare la vostra macchina.

Step 1: Leggere lo standard

Gli standard sono disponibili presso il webstore dell'IEC o presso fornitori terzi. Questa guida può aiutarvi a iniziare, ma i documenti ufficiali saranno alla fine necessari per descrizioni e spiegazioni dettagliate.

Step 2: Decidere il Security Level obiettivo

Suggeriamo il SL-1 o 2 come obiettivo realistico. Consultate la sottocategoria IEC 62443-3-2 per ulteriori dettagli su come impostare questo obiettivo. Consigliamo di basare il vostro obiettivo SL sulle potenziali conseguenze degli attacchi.

Step 3: Analisi delle lacune

Per iniziare rapidamente ad analizzare le lacune rispetto allo standard, utilizzate il nostro template gratuito. È disponibile su www.ixon.cloud/securitytools. Per facilitare questo step, abbiamo già compilato alcune parti con esempi su come una macchina può essere tipicamente conforme.

Step 4: Assegnazione delle priorità & risoluzione delle lacune

Assegnate una priorità più elevata alle implementazioni semplici, per migliorare complessivamente la sicurezza della macchina. Affrontate successivamente i problemi più complessi.

Step 5: Supporto di terze parti

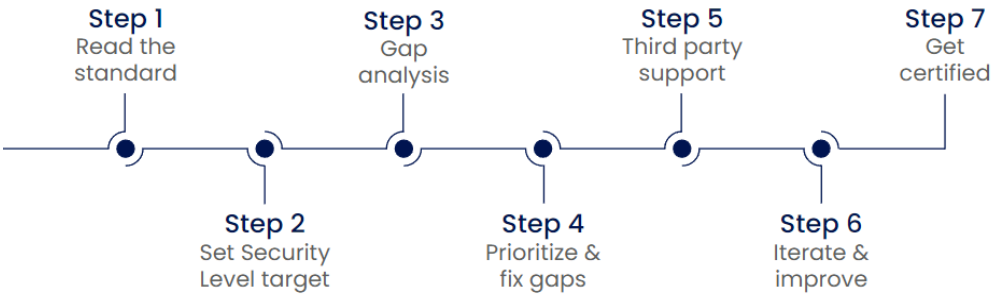
È normale restare bloccati o confusi. Alcuni requisiti possono essere interpretati in più modi e alcuni possono sembrare tecnicamente impossibili. Lavorare con un esperto esterno per guidare il processo è un aiuto importante.

Step 6: Iterare e migliorare

Implementa miglioramenti al sistema per raggiungere un Livello di Sicurezza più alto.

Step 7: Ottieni la certificazione

Il passo finale nell'adozione dell'IEC 62443 è certificare ufficialmente la conformità da parte di un revisore terzo. In alternativa, comunica un indice trasparente delle contromisure nel tuo sistema ai partner e ai clienti per rafforzare la fiducia.



Iniziare è difficile, ma diventa più facile una volta che hai una base da cui partire. Una volta raggiunto un determinato Security Level, è più semplice migliorarlo. Anche se non sarete del tutto conformi all'IEC 62443, ma implementate solo alcuni dei suoi requisiti, le vostre macchine saranno comunque più sicure di prima. Quello deve essere l'obiettivo finale.

Risorse utili e link

Template e altri strumenti: www.ixon.cloud/it/securitytools

Documenti ufficiali presso l'IEC webstore: https://webstore.iec.ch/publication/7033

Per feedback e domande potete scrivere a security@ixon.cloud.