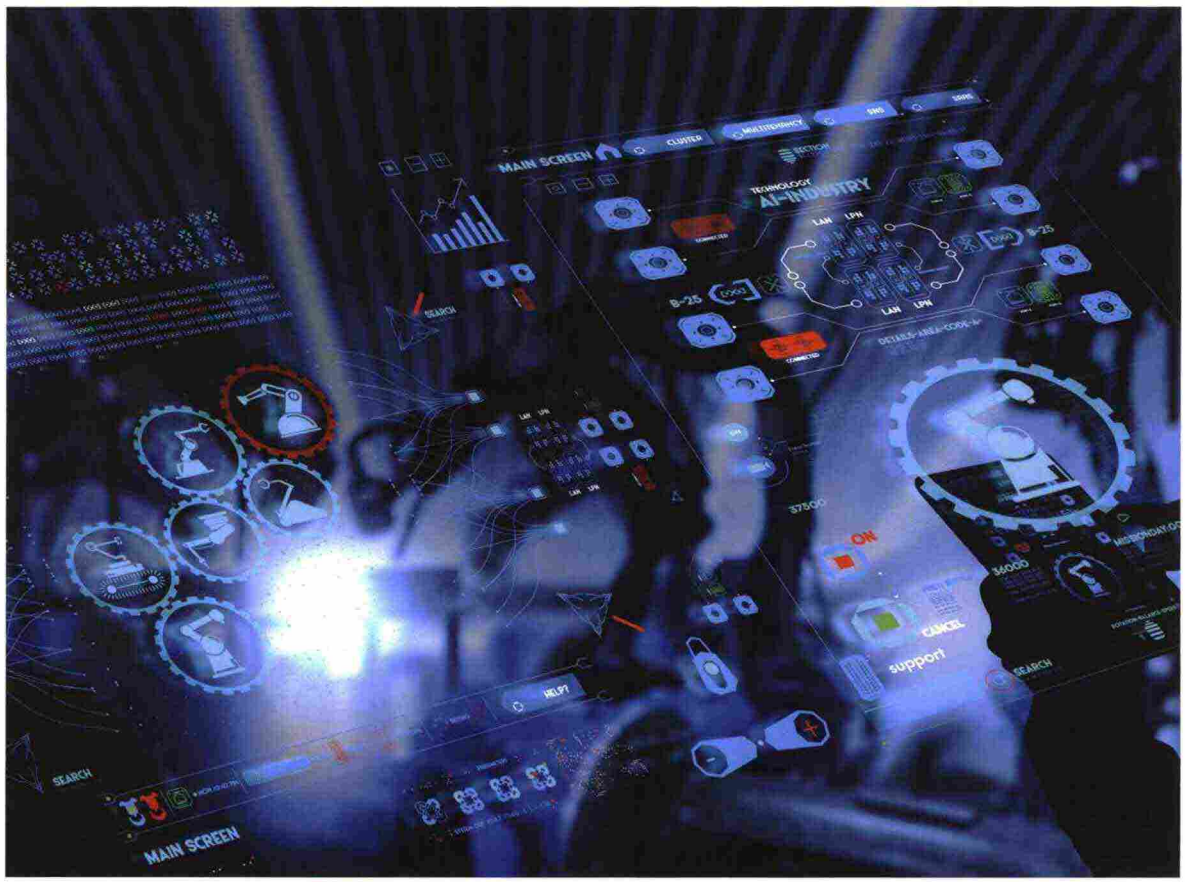
CYBERSECURITY

COME SI PROTEGGONO LE RETI OT?



È FONDAMENTALE L'ADOZIONE DI UNA PROTEZIONE STRUTTURATA PER LE RETI INDUSTRIALI. LA NORMATIVA DI RIFERIMENTO RELATIVA ALLA CYBERSECURITY IN QUESTI CASI È LA IEC 62443

MARCO VECCHIO*

Quando si parla di sicurezza informatica nelle reti di automazione, anche denominate reti OT (Operational Technology), non ci si può limitare ad applicare misure adottate nelle reti IT (Information Technology). Bisogna considerare che la rete OT nasce per supportare la produzione e, in quanto tale, deve eccellere in primis per disponibilità, senza trascurare i requisiti di integrità e confidenzialità. Di assoluta importanza è considerare che un elevato quantitativo di impianti industriali utilizzano, ancora oggi,

controllori progettati e commercializzati prima dell'avvento della connessione in rete delle macchine, quando le esigenze di sicurezza informatica non erano ancora sentite dai sistemi OT.
La rete OT è l'infrastruttura attraverso la quale fluiscono tutte le informazioni e i segnali gestiti dai controllori per lo sviluppo delle logiche di produzione. È evidente, quindi, che un attacco su questa rete si può riflettere in un'interruzione parziale o totale della produzione.
Le minacce informatiche atta a causare il malfunzionamento dei componenti di automazione possono introdurre pericoli per la sicurezza degli operatori, il danneggiamento dell'impianto e l'alterazione dei parametri di processo, portando alla realizzazione di prodotti con difetti. Fondamentale risulta quindi l'adozione di una protezione strutturata anche per le reti OT, per le quali la normativa di riferimento relativa alla cybersecurity è la IEC 62443.

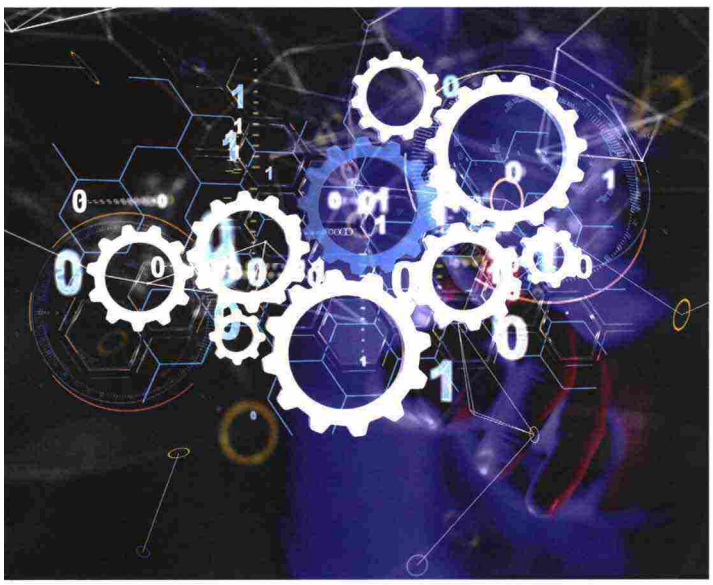
UN APPROCCIO A PIÙ LIVELLI

La normativa sottolinea il coinvolgimento di tutti gli stakeholder nella gestione della sicurezza informatica: dall'utilizzatore finale, che deve operare secondo policy strutturate, al system integrator, il quale deve ingegnerizzare una soluzione di cybersecurity per macchine e impianti, ai fornitori di tecnologie, i quali devono garantire prodotti con funzionalità di sicurezza integrate.
Dal punto di vista dell'ingegnerizzazione della soluzione, IEC 62443 consiglia una protezione strutturata su più livelli e con misure di difesa complementari tra loro. Un primo livello riguarda la protezione da intrusioni in impianto. La trattazione interessa sia misure per limitare l'accesso fisico, come l'uso di key card, sia le intrusioni informatiche. In quest'ottica si inserisce il monitoraggio continuo della rete con software in grado di effettuare anomaly detection, ossia rilevare comunicazioni inattese tra i componenti di rete.
Soffermandosi sugli aspetti di networking, una delle sfide chiave è stabilire un'adeguata protezione dei sistemi assicurando al contempo le comunicazioni funzionali all'esercizio d'impianto e allo svolgimento del processo produttivo. In quest'ottica si inseriscono le misure di segmentazione di rete, di firewalling, le connessioni sicure tramite Vpn (Virtual Private Network), la creazione di Dmz (Demilitarized Zone) e così via.
Necessarie sono anche le misure di rafforzamento dei sistemi, tra le quali troviamo aggiornamenti e installazione di patch. L'argomento è di ampia trattazione, ma nello specifico in questo articolo affronteremo gli aspetti legati all'intrusion detection e al firewalling.

SONO TUTTI COINVOLTI NELLA GESTIONE DELLA CYBERSECURITY: OEM, END-USER, FORNITORI, SYSTEM INTEGRATOR

LA FASE DI SECURITY ASSESSMENT

Un metodo efficace per affrontare la sicurezza informatica industriale richiede di iniziare con un assessment completo di tutti i dispositivi OT, IoT e IT gestiti all'interno dell'ambiente industriale di un'azienda, dei relativi rischi e delle possibili vulnerabilità.
Il ciclo di vita della sicurezza industriale secondo lo standard ISA 62443 - una serie internazionale di standard che affrontano la sicurezza informatica per la tecnologia operativa nei sistemi di automazione e controllo - include tre fasi. Di queste, la prima è proprio quella di assessment, alla quale seguono lo sviluppo delle contromisure, la loro implementazione e la gestione: un processo continuo necessario per minimizzare i rischi. La fase di assessment include un'analisi dettagliata del rischio informatico che richiede di identificare tutti gli asset e le loro vulnerabilità. Ottenere un livello di visibilità adeguato per tutti gli asset è, per diversi motivi, un'impresa complessa che va accuratamente pianificata.
Consideriamo che le soluzioni e i metodi di scansione adottati in ambito IT siano in genere incompatibili e non sicuri per le reti industriali e anche le soluzioni di assessment industriali richiedano spesso un hardware complesso con tempi di installazione piuttosto lunghi. La complessità potrebbe essere accentuata dal fatto che molte reti industriali sono geograficamente isolate e disconnesse e questo ne rende difficile l'inclusione nell'analisi.
Fra i metodi di assessment degli asset industriali tradizionali andrebbero privilegiati quelli che permettono una raccolta dati passiva che tipicamente è compatibile con le reti industriali e i casi d'uso tipici senza introdurre alcuna latenza. In commercio esistono anche data collector estremamente flessibili installabili sui sistemi operativi più diffusi per le workstation industriali che offrono una visibilità completa degli asset industriali senza necessità di macchine server dedicate allo scopo e uso di sensori di alcun tipo.
Molte soluzioni permettono oggi alle aziende di scegliere fra installazioni on premis o SaaS, più semplice e rapido. Un sistema di Asset Inventory, in ogni caso, deve identificare e catturare informazioni da sistemi Windows, come da apparati di rete (switch, router e firewall), controllori programmabili, I/O remoti, azionamenti e ogni altro asset collegato alla rete OT.
Questi dati sono utilizzati per individuare le aree di un sistema di controllo OT che richiedono la messa in atto di contromisure adeguate al livello di rischio.
Un'analisi correttamente eseguita permette la gestione dei rischi e delle vulnerabilità di ciascun asset: dalla mancanza di patch critiche agli indicatori di obsolescenza, alle Common Vulnerability and Exposure (Cve) che interessano un as-



set specifico. Gestire queste informazioni consente di proteggere meglio le reti industriali riducendo l'esposizione ai rischi. Questa modalità supporta inoltre in modo efficace, semplice e rapido le richieste di verifica e fornisce informazioni sulla conformità della rete industriale agli standard esistenti, aumentando così la conformità e la "postura" di sicurezza generale.

Un assessment completo unito alla valutazione dei rischi e delle vulnerabilità consente di ottimizzare le azioni di riposta in caso di incidente valutandone immediatamente gli impatti possibili. Consideriamo sempre che, secondo i maggiori analisti, il cyberrischio più elevato è relativo agli attacchi opportunistici di breve durata e grande ritorno economico piuttosto che alle Common Vulnerability (Cve).

METTERE IN SICUREZZA I PROCESSI OT RICHIEDE L'ADOZIONE DI SOLUZIONI SPECIFICHE

Mentre i sistemi IT nascono per interfacciarsi con un operatore umano, le architetture OT si interfacciano con sistemi e processi "fisici", basti pensare alle reazioni chimiche, al flusso di un liquido, al processo di riscaldamento/raffreddamento, alla validazione di ulteriori processi.

Anche le priorità dei due ambienti sono differenti. Nell'IT si tutela l'integrità del dato, nell'OT la continuità del processo. Proprio per questo motivo, l'approccio classico alla security industriale, che prevede l'impiego di strumenti e soluzioni IT, mal si coniuga con le caratteristiche di sistemi Scada e Ics. La problematica principale di questo approccio non risiede tanto nelle differenze tecniche tra soluzioni aspecifiche e specifiche bensì nella capacità di comprendere il comportamento dell'intero ambiente OT, ovvero quali sistemi si interfacciano con quali e con quale protocollo, che informazioni vengono scambiate e con quale frequenza. Competenze essenziali per determinare in anticipo - in base ai dati rilevati - il livello di criticità del potenziale impatto di una vulnerabilità e prendere contromisure adeguate, specie nei tanti ambiti OT in cui l'aggiornamento dei sistemi non è un'opzione.

A fronte dell'iperconnessione e dell'estensione della superficie di attacco delle infrastrutture OT dovute all'impiego indiscriminato di componenti IT nel segno di Industria 4.0, qualora si opti per soluzioni Ids (Intrusion Detection System) e di firewalling occorre che queste siano in grado di analizzare sia i protocolli industriali sia i protocolli IT e, quindi, non solo di identificare il contenuto di qualsiasi comunicazione, ma anche di valutare correttamente il comportamento delle componenti monitorate. Soluzioni di questo tipo contribuiscono in massima parte alla segmentazione dei vari comparti di produzione e alla loro separazione dagli ambiti squisitamente IT come l'amministrazione, le vendite, la progettazione, la logistica, fino alla gestione dei dispositivi per l'erogazione di bevande connessi a Internet. Sono elementi che vanno nettamente separati dai sistemi di produzione, per escludere potenziali "movimenti laterali". Ma non solo, sempre in ottica di circoscrizione dell'area esposta a potenziali rischi, vanno segmentate anche le diverse aree dell'ambiente OT, i cui processi non presentano interdipendenze o per cui non è prevista intercomunicazione.

Un altro beneficio dei sistemi di firewalling di classe industriale è la capacità di realizzare architetture Zero Trust (Zta) anche in presenza di dispositivi non dotabili di soluzioni Hips (Host Intrusion Prevention System) o altre misure di rafforzamento dei sistemi tramite software specifici.

Così, mentre attendiamo una nuova generazione di macchinari e componenti industriali sviluppati secondo i criteri della security-by-design, l'impiego di firewall industriali è quindi uno dei pochi work-around che consente anche ai sistemi e alle componenti OT meno flessibili e più datate di essere integrate in Zta.

Altrettanto rilevante è la funzione specifica degli Ips (Intrusion Prevention System) industriali: essi individuano in tempo reale anomalie del flusso di dati IT/OT, bloccandole immediatamente (modalità proattiva), o inviando un allarme tempestivo all'amministratore di sistema (modalità reattiva). ■

*Articolo a cura di Marco Vecchio, in collaborazione con il Gruppo Software Industriale di Anie Automazione.