INDUSTRIAL CYBERSECURITY CRITICITÀ ED EVIDENZE

LA GESTIONE DELLA SICUREZZA E DELLA PROTEZIONE DEI DATI È DIVENTATA UN ELEMENTO CENTRALE NELLA TRASFORMAZIONE DIGITALE, MA ANCHE UN DRIVER DI INNOVAZIONE PER IL MONDO INDUSTRIALE, SEMPRE PIÙ ESPOSTO AI CYBERATTACCHI

NICOLETTA BUORA

Convergenza IT/OT, allargamento del perimetro dei sistemi anche fuori dalle fabbriche, IIoT e connessioni da remoto anche secondo criteri Industria 4.0 aumentano sicuramente il rischio informatico di reti e sistemi di controllo e telecontrollo che gestiscono macchinari e impianti nell'Industria come nelle utility. Ci confrontiamo con Marco Vecchio, segretario dell'associazione Anie Automazione, punto di riferimento, con le sue 100 associate, per le imprese fornitrici di tecnologie per l'automazione di fabbrica, di processo e delle reti.

Quali sono le problematiche di cybersicurezza portate alla vostra attenzione?

Se fino a poco tempo fa si tendeva a proteggere macchinari, impianti e infrastrutture secondo la logica della "security-by-obscurity", oggi che abbiamo ormai tutto connesso e accessibile è sicuramente più indicato seguire strategie di "security-by-design" per i nuovi sistemi da progettare ed implementare e soprattutto utilizzare concetti di "security-by-visibility" per affrontare al meglio eventuali incidenti informatici che si possano verificare nel dominio OT (Operational Technology).

Provo a riassumere di seguito i casi più frequenti che vengono portati in evidenza o che a volte vengono sottovalutati dalle aziende. 1. Vulnerability & Patch Management non adeguati: molto spesso, in ambito industriale e non, emergono lacune considerevoli nella gestione degli aggiornamenti e delle vulnerabilità note, esponendo numerosi asset aziendali ad attacchi informatici ad alta probabilità di efficacia. Ciò avviene perché i mondi IT e OT risultano spesso slegati e non gestiti in modo omogeneo, secondo linee guida trasversali. 2. Mancanza di monitoraggio degli eventi di sicurezza: la sorveglianza delle infrastrutture produttive si focalizza, solitamente, sul solo controllo del processo produttivo e sull'intrusione fisica negli impianti. In questo modo non vengono però generati, gestiti, raccolti e monitorati eventi di sicurezza relativi all'infrastruttura informatica degli impianti, ponendo le aziende nelle condizioni di non essere potenzialmente nemmeno a conoscenza di attacchi subiti sul proprio perimetro. 3. Sicurezza delle informazioni non parte integrante del ciclo di vita delle reti industriali: gli aspetti riguardanti la sicurezza informatica non sono spesso considerati

Marco Vecchio,
segretario dell'associazione
Anie Automazione

durante tutto il ciclo di vita delle reti industriali. Si dovrebbe rendere necessaria, dato l'elevato rischio intrinseco dei processi di business coinvolti in ambito industriale e dei potenziali danni causati da attacchi malevoli a queste infrastrutture, l'adozione di una checklist di sicurezza da rispettare durante tutte le fasi dello sviluppo e gestione di un impianto. 4. Procedure di Continuità Operativa non adeguate: i piani e le procedure di continuità operativa devono essere definiti e implementati in modo congruente con la criticità dei vari processi di business coinvolti, anche per quanto concerne le reti industriali, predisponendo soluzioni, tecnologie e processi da mettere in atto in caso di emergenza. 5. Mancata gestione della sicurezza delle informazioni dei rapporti con i fornitori: con l'avvento di Industria 4.0, sempre più spesso ampi segmenti delle reti industriali sono gestiti e manutenuti in toto dai fornitori stessi. È fondamentale gestire la sicurezza nei rapporti e nei contratti con le terze parti coinvolte, in modo che risultino applicate le politiche minime aziendali a tutela del proprio patrimonio informativo.

Tra i vostri associati vi sono fornitori globali di tecnologie e soluzioni per l'OT Security con un background di competenze nella realizzazione di progetti di cybersecurity di alto livello. Quali sfide devono affrontare le imprese industriali per l'OT Security?

Abbiamo ancora oggi la sensazione che la maggioranza di incidenti informatici alle reti OT sia rappresentata da danni collaterali di incidenti (errori umani dovuti a scarsa percezione del rischio informatico, errori di progettazione, configurazione, implementazione della rete e sistema Ics/OT o anche "sabotaggi") o di attacchi alla rete IT che si propagano a quella OT per mancanza di adeguata protezione mediante segmentazione della rete e segregazione di asset critici. Ne abbiamo evidenza negli episodi di sistemi di produzione bloccati in fabbrica dai ransomware (i malware che criptano i file del pc, bloccandolo, e che rimandano ad un riscatto da pagare per tornare alla normalità): spesso il contagio viene dai pc in ufficio sui quali è stato aperto incautamente un allegato di e-mail malevolo. La protezione da rischi informatici di reti e sistemi OT comporta adeguate conoscenze e skill specifici che non sempre sono solo quelli del mondo IT: ci sono standard e procedure per la messa in sicurezza, tecnologie e prodotti specificamente pensati per manufacturing, OT e anche IIoT (Industrial IoT).

Avete messo in campo delle iniziative a supporto dei vostri associati? Se sì, quali?

Il tema della cybersecurity nel mondo industriale viene affrontato nel Gruppo Software Industriale che ormai da quasi tre anni raccoglie le principali aziende OT e IT che operano nel settore della fornitura di prodotti e soluzioni per lo smart manufacturing, smart product, virtual manufacturing e appunto industrial cybersecurity. Il lavoro principale svolto dal gruppo è proprio supportare le imprese associate aiutandole a far comprendere ai clienti il ruolo fondamentale del software nell'Industria 4.0 e l'importanza strategica della sicurezza informatica in questa nuova cultura manifatturiera basata sui dati e sulle informazioni. Due sono i fattori significativi della transizione in corso nel settore manifatturiero. Da un lato, la necessità di innovare processi produttivi e prodotti grazie alle tecnologie digitali per rimanere competitivi a livello globale. Dall'altro, il comparto industriale italiano è caratterizzato da aziende di dimensioni medio-piccole che determinano una caratterizzazione locale dei concetti di Industria 4.0. Si va quindi oltre i presupposti alla base del paradigma 4.0 e si trovano soluzioni software adeguate alla nostra realtà specifica. In tale contesto, la collaborazione tra fornitore e utilizzatore di soluzioni tecnologiche ricopre un ruolo sempre più strategico. L'innovazione deve andare di pari passo con il rispetto della privacy e della sicurezza. Il tema della cybersecurity industriale può oggi essere considerato un fattore di sviluppo, un asset critico per fare business, un servizio fondamentale per chi vuole investire in Italia.

A supporto delle attività dei soci organizziamo eventi periodici e realizziamo, in collaborazione con le università sul territorio, diversi white paper, cito ad esempio due volumi recenti dedicati a smart manufacturing e dinamiche di ritorno dell'investimento del software industriale.

MOLTI INCIDENTI SULLE RETI OT SONO DOVUTI A ERRORI UMANI O A PROPAGAZIONE DI INCIDENTI SU RETI IT