Titolo progetto:

Z4I - Zero Trust Architecture for the Industry landscape

Abstract:

L'Industrial Internet of Things (Industrial IoT) nell'ultimo decennio si è affermato come uno dei principali fattori abilitanti dell'Industria 4.0, la quarta rivoluzione industriale. L'ascesa dell'IoT ha portato alla convergenza di Operational Technology (OT) e Information Technology (IT), che tradizionalmente operavano come domini distinti. Tale convergenza porta non solo nuove opportunità, tra cui migliori prestazioni, flessibilità e interoperabilità, ma anche sfide significative, come le minacce alla sicurezza informatica con possibili risvolti negativi anche sulla safety delle persone. Tali sviluppi hanno anche spinto i legislatori a emanare leggi volte a mitigare i rischi associati alla sicurezza.

Le tradizionali strategie di sicurezza informatica aziendale, incentrate sulla protezione di un perimetro intorno all'azienda, sono sempre meno efficaci nel contesto industriale odierno caratterizzato da lavoro da remoto, utilizzo di dispositivi personali e adozione massiva di servizi cloud. I moderni ambienti industriali devono affrontare le sfide di sicurezza derivanti non solo dalla convergenza tra IT e OT, ma anche dal fatto che non esiste più un unico perimetro a livello aziendale. Zero Trust Architecture (ZTA) è un approccio che elimina ogni fiducia implicita nell'interazione tra dispositivi e sta emergendo come efficace soluzione per la sicurezza informatica aziendale. Tuttavia, l'implementazione di questo approccio in ambito industriale è resa difficile a causa di limitate conoscenze in materia di sicurezza informatica da parte degli operatori in ambito industriale, dei rischi associati al collegamento in rete di sistemi legacy e dei potenziali problemi di prestazioni relativi, ad esempio, agli algoritmi di crittografia che richiedono un uso massiccio di CPU.

Il progetto Z4I propone di adottare l'approccio ZTA in ambito industriale, in particolare indagando l'uso di soluzioni all'avanguardia basate su Digital Twin (DT) e Next Generation Firewall (NGFW). Inoltre intende analizzare gli algoritmi crittografici per identificare quali potrebbero essere adottati sulle macchine industriali, considerando i loro limiti in termini di capacità di calcolo e memoria. Infine, riconoscendo le implicazioni che le minacce alla sicurezza potrebbero avere sulla safety dei lavoratori in ambito industriale, intende analizzare la normativa vigente per fornire una panoramica strutturata ed esaustiva.

Obiettivi e risultati attesi:

Il primo obiettivo del progetto Z4I è quello di applicare l'approccio Zero Trust Architecture (ZTA) adottando congiuntamente soluzioni all'avanguardia come Digital Twin (DT) e Next Generation Firewall (NGFW). Soluzioni open-source per NGFW saranno adottate per creare una topologia sicura ma programmabile, limitando il traffico da/verso macchine e PLC al minimo necessario per il loro corretto funzionamento. Inoltre soluzioni NGFW

supporteranno l'analisi in tempo reale del traffico in transito per identificare tempestivamente possibili attacchi. I DT forniranno l'accesso alle macchine industriali e ai relativi PLC tramite API facili da usare e ben documentate, ad esempio basate su REST e MQTT, nascondendo così la complessità dell'interazione con protocolli industriali eterogenei e spesso proprietari. Inoltre i DT interagiranno con gli NGFW per inviare dinamicamente le configurazioni di sicurezza e raccogliere informazioni per rafforzare le politiche di sicurezza in caso di attacchi.

Il secondo obiettivo del progetto Z4I è analizzare gli algoritmi crittografici per identificare quali potrebbero essere adottati dalle macchine industriali, considerando in particolare i loro limiti in termini di capacità di calcolo e memoria. Questa analisi includerà algoritmi tradizionali (ad esempio, RSA, ElGamal ed ECC) e nuovi algoritmi basati sul calcolo quantistico. L'obiettivo è quello di condurre un'analisi matematica approfondita per identificare sicurezza ed efficienza di tali algoritmi, considerando le capacità di elaborazione e memoria tipiche dei dispositivi industriali.

Il terzo obiettivo del progetto Z4I, riconoscendo le implicazioni che le minacce alla sicurezza potrebbero avere sulla safety dei lavoratori all'interno degli ambienti industriali, è analizzare la normativa vigente. Normativa di interesse comprende il Machinery Regulation, il Cyber Resilience Act e la GDPR, il Cybersecurity Act e la Network and Information Security Directive (NIS2). L'obiettivo è quello di fornire una panoramica strutturata ed esaustiva, con particolare attenzione ai profili riguardanti il diritto penale, la procedura penale e il diritto del lavoro, pensata per essere comprensibile per i non esperti in normative.