



Sicurezza informatica industriale: La consapevolezza resta bassa nonostante l'aumento degli attacchi silenziosi di alto profilo

L'afflusso delle soluzioni IT nell'ambito delle tecnologie operative evidenzia il bisogno di sicurezza "by design" piuttosto che sicurezza "by default", secondo Frost & Sullivan MILANO - 21 settembre 2015 - Sebbene le tradizionali industrie manifatturiere non siano state progettate pensando alla sicurezza, la proliferazione di reti e dispositivi, di canali di comunicazione diversificati e dell'utilizzo di software preconfezionato hanno portato la sicurezza informatica sotto i riflettori. Le preoccupazioni relative alla sicurezza associate agli alti livelli di connettività e integrazione iniziano a manifestarsi ora che il concetto di **Internet delle cose** prende forma nelle reti industriali e all'interno degli stabilimenti di produzione. L'allarmante frequenza di minacce persistenti e avanzate, sofisticate e mirate ha dato ulteriore rilevanza al tema della sicurezza nelle industrie sia discrete sia di processo. Una nuova analisi di Frost & Sullivan, intitolata "**The Safety-Security Argument: Expanding Needs in a Connected Enterprise**", rileva che il mercato globale della sicurezza informatica per i sistemi di controllo crescerà, secondo le previsioni, a un tasso **tra il 20 e il 25% ogni anno da qui al 2021**. Il Nord America e l'Europa resteranno all'avanguardia nel creare consapevolezza e avviare innovazioni tecnologiche rivolte agli attacchi derivanti da minacce avanzate persistenti.

Per accedere gratuitamente a maggiori informazioni su questa ricerca, si prega di visitare: http://corpcom.frost.com/forms/EU_PR_AZanchi_MB1B-10_18Sept15

"Attualmente, le aziende impiegano un approccio ampio e stratificato per la protezione degli asset informatici e le organizzazioni del settore stanno lavorando per definire norme adeguate, - afferma Sonia Francisco, analista di Frost & Sullivan. - Le **partnership tra governo, industria e istituti di ricerca** saranno fondamentali per dare forma a standard robusti nel settore, in grado di accelerare lo sviluppo di soluzioni complete per la gestione della sicurezza."

Poiché il concetto di Internet delle cose trasforma l'architettura degli stabilimenti, le strategie per la difesa della sicurezza preconfezionate ("**defense-by-default**") lasceranno spazio alle soluzioni ad hoc ("**defense-by-design**"). Le soluzioni di sicurezza integrate in grado di rilevare, adattare, modificare e rispondere alle minacce sulla base di diversi parametri dell'ecosistema guadagneranno popolarità.

Anche la creazione di soluzioni specifiche per i diversi settori e applicazioni sarà fondamentale, poiché le soluzioni di information technology (IT) continuano ad affluire nello spazio delle tecnologie operative (OT). I fornitori di soluzioni negli **ecosistemi IT e OT** devono unire gli sforzi per implementare soluzioni per la sicurezza informatica a tutto tondo per i sistemi industriali.

"Un tale livello di integrazione richiederà una **forza lavoro di nuova generazione**, con competenze sia IT che OT, - osserva Francisco. - I fornitori di servizi di sicurezza informatica possono offrire soluzioni di formazione e di gestione del cambiamento che colmeranno il divario di conoscenze."

Poiché la maggior parte delle industrie si stanno aggiornando a sistemi e processi intelligenti, la sicurezza informatica industriale farà presto l'inevitabile passaggio da un modello operativo reattivo ad una **filosofia progettuale**

proattiva.

Lo studio **“The Safety-Security Argument: Expanding Needs in a Connected Enterprise”** è un **Market Insight** che fa parte del programma **Industrial Automation & Process Control** Growth Partnership Service. Questo studio offre una visione strategica dei requisiti e delle best practice nell’ambito della sicurezza informatica e nell’era degli asset connessi e delle imprese collegate. Questa analisi di mercato fa luce sulle sfide, le opportunità e le strategie nell’ambito della sicurezza informatica, valutate in seguito a colloqui esaustivi con gli operatori del mercato.