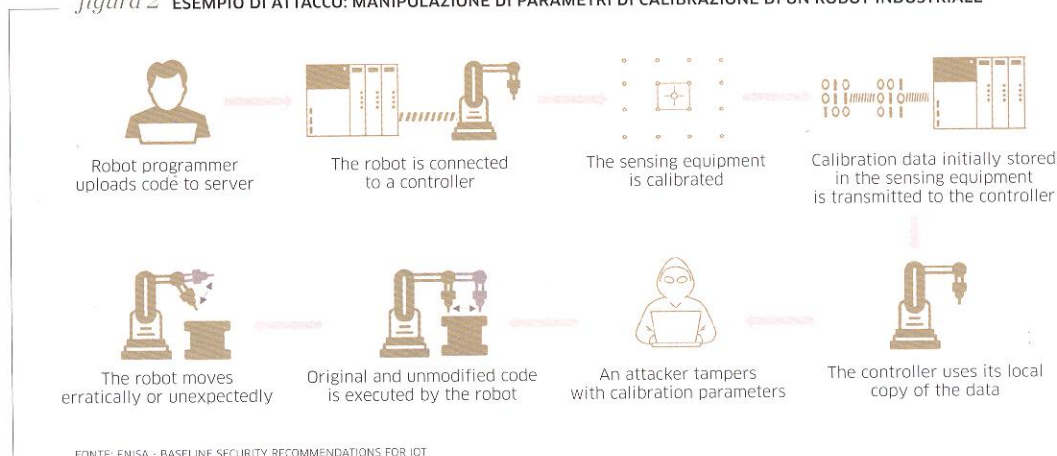


figura 2 ESEMPIO DI ATTACCO: MANIPOLAZIONE DI PARAMETRI DI CALIBRAZIONE DI UN ROBOT INDUSTRIALE



FORNITORE: ENISA - BASELINE SECURITY RECOMMENDATIONS FOR IOT

sicurezza visto che le particolarità dell'interfaccia utente non consentono i tradizionali meccanismi di update. Questo aspetto, come pure la gestione del ciclo di vita dei sistemi, è ulteriormente aggravato dalla difficoltà di identificare le responsabilità, visto che i sistemi sono inseriti in dispositivi che operano in settori estremamente diversificati a opera di una molteplicità di attori. Da

parte loro, i vendor dovrebbero almeno fornire ai clienti alcuni suggerimenti semplici, come ad esempio cambiare la password di default al primo utilizzo, e introdurre possibilità di aggiornamento senza però complicare troppo l'interfaccia utente perché i clienti si aspettano una semplicità di utilizzo dei dispositivi.

OKI punta a retail e healthcare diffondendo colore e integrazione

Conquistare i mercati retail e healthcare, favorire la diffusione della stampa a colori e offrire soluzioni fortemente integrabili con applicazioni di terze parti. Ecco la strategia OKI in ambito printing raccontata da Romano Zanon, General Manager South Europe Regional Marketing, OKI Europe (Italia)

Cosa sta accadendo nel mercato del printing e che strategia sta adottando OKI per affrontare le evoluzioni in atto? "Stiamo assistendo a un forte cambiamento - spiega Romano Zanon, General Manager South Europe Regional Marketing, OKI Europe (Italia) - La diffusione di soluzioni per ottimizzare i flussi di stampa ha portato a un'effettiva riduzione dei volumi di carta

stampata e imposto alle aziende produttrici di hardware un'evoluzione della propria strategia di business". Nel caso di OKI, quest'evoluzione ha portato l'azienda a concentrarsi su alcuni segmenti verticali dove la stampa ha mantenuto un ruolo importante, retail e healthcare: "In questi settori i consumi sono i più alti - spiega Zanon. Nel retail sono finalizzati alla produzione di materiali di visual communication, signage, banner ecc., nell'healthcare soprattutto alla realizzazione di stampe destinate ai pazienti relative a diagnosi e visite". Per soddisfare le esigenze di questi ambiti verticali, l'azienda sta stringendo partnership con system integrator che conoscono le esigenze specifiche dei due settori e, sul piano tecnologico,

punta a valorizzare alcune caratteristiche peculiari delle proprie soluzioni. Per esempio, racconta Zanon, solo OKI produce stampanti dotate di interfaccia DICOM [standard diffuso in ambito biomedico - ndr]: "Nel mondo healthcare è un aspetto molto apprezzato perché consente alle nostre macchine di dialogare con le apparecchiature medicali con lo stesso linguaggio, senza alcuna intermediazione, con vantaggi prima di tutto sul piano della qualità delle immagini stampate". La strategia OKI si esprime però anche attraverso due parole chiave, "colore" e "integrazione":

■ colore - L'azienda punta a "conquistare" i mondi dove si stampa molto a colori

Le raccomandazioni di Enisa

Queste criticità potrebbero essere mitigate seguendo alcune raccomandazioni rivolte agli stati, ai produttori, alle imprese utilizzatrici, di seguito sintetizzate:

- 1) Promuovere l'armonizzazione delle iniziative di sicurezza e regolamentazione in ambito IoT.
- 2) Far crescere la consapevolezza della necessità di cybersecurity anche in questo ambito.
- 3) Definire linee guida per lo sviluppo sicuro di software e hardware IoT.
- 4) Ottenere ampio consenso sull'interoperabilità all'interno dell'ecosistema.
- 5) Promuovere incentivi economici e amministrativi per la sicurezza IoT.
- 6) Definire la gestione del ciclo di vita di prodotti/servizi IoT.
- 7) Chiarire la condivisione delle responsabilità fra i soggetti coinvolti.

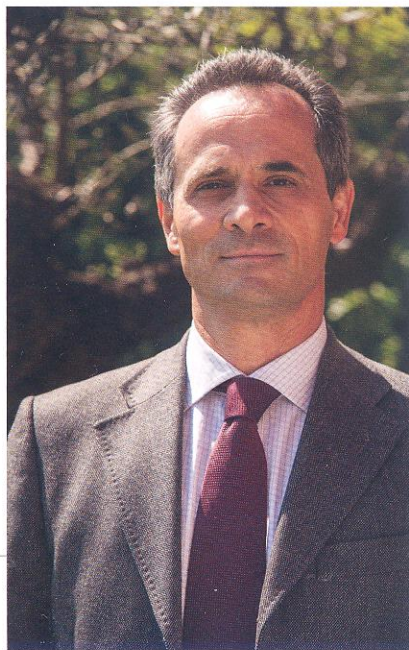
Visto che nel frattempo la diffusione dei dispositivi avanza, pur senza generare

allarmismo, è urgente diffondere la sensibilizzazione fra gli utilizzatori e i produttori. Anche i singoli stati potrebbero prendere iniziative: in Italia il **Ministero per lo Sviluppo Economico** sta ad esempio studiando una sorta di certificazione basata su alcuni test di base per i sistemi IoT con l'obiettivo di verificarne la robustezza. ■

[1] Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, Enisa, novembre 2017. Enisa è l'agenzia europea che concentra le competenze nel campo della sicurezza e ha come principale obiettivo aumentare la resilienza dei sistemi informativi attraverso l'implementazione di misure per proteggere gli stati membri, le imprese e i cittadini.

NOTA: Si ringrazia Giancarlo Caroti, partner Neumus, per le informazioni e i preziosi suggerimenti.

ROMANO ZANON
GENERAL MANAGER SOUTH EUROPE
REGIONAL MARKETING, OKI EUROPE (ITALIA)



(come quello dell'etichettatura, o gli stessi retail ed healthcare) promuovendo contemporaneamente l'utilizzo di multifunzione (MFP a colori anche in quelle realtà dove l'esigenza dominante è il bianco e nero, ma che potrebbero avere l'esigenza di stampare anche a colori (la strategia OKI è quella di offrire soluzioni a colori con un costo delle stampe in bianco e nero uguale a quello delle stampanti monocromatiche che, generalmente, hanno prezzi più bassi degli MFP)

■ **integrazione** - Tutti i dispositivi Smart hanno incorporata una smart Extendable Platform (sXP) che consente una rapida integrazione delle macchine con applicazioni di terze parti. "Abbiamo reso le nostre apparecchiature aperte - spiega Zanon - ben integrabili con le diverse

soluzioni di cui ciascuna azienda può aver bisogno". In ambito healthcare, per esempio, dove si trattano dati sensibili, è forte la domanda di applicazioni per la sicurezza. Da questo punto di vista, spiega Zanon, OKI offre embedded alcune funzionalità fondamentali ("I lavori di stampa - dice il top manager - possono essere protetti attraverso codice Pin o tramite l'utilizzo di smart card, consentendo un rilascio sicuro dei lavori solo quando l'utente si autentica fisicamente sui multifunzione"), ma grazie a sXP gli sviluppatori, partner di OKI compresi, possono soddisfare esigenze di sicurezza maggiori e funzionalità specifiche integrando alla piattaforma anche soluzioni e applicazioni di sicurezza più avanzate, disegnate su misura per l'ambito healthcare. (V.B.)