Il Sole 24 ORE

L'APPUNTAMENTO A TORINO DI NÒVA24

Cybersecurity, le buone pratiche nell'Industria 4.0

—di **Filomena Greco** | 09 ottobre 2018

Il tema della cyber secutity ai tempi di industria 4.0 evidenzia anche modelli di eccellenza. La nuova tappa del road show di Nòva24 organizzata con il Politecnico di Torino per raccontare i rischi dell'economia digitale è stata l'occasione per sottolineare che le buone pratiche, pure su un tema ancora di frontiera, esistono. È il caso della partnership costituita dalla francese Leroy Merlin, protagonista nella grande distribuzione, con la società piemontese AizoOn, specializzata in consulenza tecnologica e attiva sul fronte dei rischi informatici. Oppure della protezione messa in campo dalla multiutility Iren.

Il punto di partenza è duplice: da un lato la crescente consapevolezza dei rischi di attacchi informatici ai danni delle aziende, siano esse manifatturiere o di servizi, dall'altro il forte ritardo delle imprese nella implementazione di sistemi di protezione, a cominciare dalla formazione di operatori ed addetti che spesso , anche involontariamente, possono rappresentare un primo varco verso i sistemi informatici aziendali da parte di hacker o azioni malevole.

Un concetto ribadito da Franco Deregibus, direttore del Digital Innovation hub del Piemonte: «In un anno e mezzo di attività – racconta – abbiamo incontrato circa 360 aziende sui temi della digitalizzazione e sulle tecnologie abilitanti di industria 4.0, ma è stato difficile imporre i temi della cyber security, l'approssimazione resta molto alta, abbiamo ad esempio avuto problemi a trovare delle aziende disponibili a fare prove di penetrazione, pur in presenza di un contributo economico della Camera di commercio».

Una questione che tocca i sistemi di information technology delle imprese ma che si allarga alle applicazioni Iot. «Quando si parla di macchine o robot – aggiunge Deregibus – ci si riferisce a sistemi nati per rimanere *stand alone*, ma anche di una base di macchinari installata che ha una vita media di oltre vent'anni e sistemi operativi spesso datati, impossibili da sostituire». Problema di *security*, dunque, sottolineano gli operatori, almeno quanto di *safety*, se si guarda all'interazione uomo-macchina e al futuro sviluppo dei robot collaborativi.

Il mondo della ricerca in questo ambito non sta a guardare. È il caso della iniziativa promossa a Torino dall'Istituto superiore Mario Boella e da Siti, che hanno deciso di unire le forze e creare un Laboratorio focalizzato su cyber security e Intelligenza artificiale che si chiamerà Links. «Una realtà da 150 ricercatori e 16 milioni di fatturato di fatturato per il60% in Europa – sintetizza Marco Mezzalama, vicerettore del Politecnico di Torino – che avrà tra i suoi temi e le sue linee di ricerca quello della sicurezza degli impianti e delle linee robotizzate».

Diventerà uno degli snodi italiani della rete costituita da diverse università e dal Cini (Consorzio Interuniversitario Nazionale per l'Informatica) al lavoro sulle sfide della sicurezza digitale. Ricercatori di 40 diversi enti diversi, come riassume Paolo Prinetto, direttore del Laboratorio nazionale di Cybersecurity del Cini, impegnati «su progetti e azioni per aumentare la resilienza del sistema paese rispetto agli attacchi informatici». La ricerca, dunque, e la capacità di implementare sistemi di difesa in ambienti in grado di simulare gli attacchi e sperimentare forme di protezione. Tecnicamente si tratta dei Cyber Range descritti da Alessandro Armando, esperto del Cini.