Il Sole 24 ORE
Fondato nel 1865
Quotidiano Politico Economico Finanziario
QUOTIDIANO: MILANO

CAPITALE UMANO

***

Pmi e Cybersecurity tra sicurezza nazionale e competitività

di **Max Bergami*** e **Michele Colajanni****

La sicurezza informatica è un punto di debolezza del sistema produttivo italiano ampiamente sottostimato, almeno dalla maggioranza dei manager e delle imprese. La consapevolezza dei rischi derivanti dalla vulnerabilità informatica sta crescendo nell'opinione pubblica, non fosse altro per le polemiche sulle presunte ingerenze di alcuni paesi nei processi elettorali di altri, ma il sentimento dominante è che si tratti di problemi remoti o comunque riguardanti altri. Mentre è ragionevole attendersi una minore sensibilità da parte di chi possiede una cultura informatica limitata, è sorprendente riscontrare un grado di disinteresse ancora troppo elevato tra chi riveste ruoli di responsabilità manageriale, sia nel settore privato, sia in quello pubblico.

A livello nazionale si stanno compiendo alcuni passi significativi nella direzione di una strategia paese che includa difesa, polizia, intelligence, infrastrutture critiche, pubblica amministrazione e imprese, così come hanno fatto altri paesi, tra cui Germania e Regno Unito. Questo sforzo, coordinato dalle istituzioni, rappresenta la necessaria risposta alla crescita delle attività informatiche criminose, terroristiche, di spionaggio e di hacktivism a cui ogni paese è recentemente esposto in maniera crescente. Anche se verosimilmente, siamo solo all'inizio di una nuova era di inedite sfide alla sicurezza, l'accelerazione nell'introduzione di nuove tecnologie digitali porterà a una crescita esponenziale dei rischi. Si pensi, ad esempio, ai problemi che dovranno affrontare gli ospedali del futuro, per garantire sicurezza e privacy con il procedere della trasformazione digitale (ruolo dei dati, della robotica e dell'intelligenza artificiale nel settore della salute). Volendo limitarsi al mondo delle imprese, indubbiamente le (poche) grandi imprese italiane hanno preso atto del problema e si sono organizzate.

Se è vero che, di fronte ad alcune minacce generate da una grande disponibilità di risorse finanziarie e umane, il concetto di sicurezza è comunque probabilistico, le grandi imprese hanno creato strutture interne almeno in grado di alzare il livello di sicurezza e di presidiare le variabili rilevanti. La stessa cosa non si può dire per le Pmi, dove la cybersecurity è interpretata prevalentemente come un problema che riguarda la direzione sistemi informativi e la consapevolezza dei rischi attuali e imminenti è molto contenuta. È certamente vero che un attacco a una media impresa probabilmente avrebbe un impatto meno grave di quanto non possa accadere nel caso in cui fosse interessato un grande operatore finanziario o dell'energia, ma a ben vedere la situazione non è così trascurabile. Anzitutto le PMI rappresentano oltre il 90% delle imprese italiane, inoltre in molti casi producono prodotti e servizi rilevanti per la società, ma soprattutto rappresentano segmenti fondamentali delle filiere produttive dei settori più competitivi del Paese. Trattandosi di soggetti più vulnerabili, un attacco che possa contagiare porzioni rilevanti del sistema potrebbe avere conseguenze di gravità simile a possibili attacchi a imprese di maggiore dimensione.

In questo quadro, in cui non è stato ancora risolto il problema della sicurezza informatica, ci si troverà molto presto a fronteggiare nuovi rischi derivanti dai sistemi cyber-fisici. Pensando allo sviluppo dell'Industry 4.0 e in particolare all'internet of things, agli smart objects e alla connessione dei sistemi produttivi, è chiaro che l'industria (e di conseguenza la società) si appresta ad "accogliere" miliardi di oggetti dotati di capacità di connessione. In questo campo, sta partendo una corsa all'oro che rischia di ripetere gli errori compiuti in passato nell'ambito della sicurezza informatica, ma con possibili conseguenze molto più rilevanti, in quanto i rischi non riguardano solo l'efficacia delle risorse investite in sicurezza informatica, eventuali furti di informazioni o truffe di vario tipo, ma anche la sicurezza dei cittadini che si troveranno a interagire fisicamente con oggetti connessi e dunque, per definizione, vulnerabili. Lo stesso

STRUTTURE FRAGILI

Le piccole imprese sono le più vulnerabili e non sempre hanno una piena consapevolezza dei rischi che corrono

Il Sole 24 ORE
Fondato nel 1865
Quotidiano Politico Economico Finanziario
QUOTIDIANO: MILANO

concetto di sicurezza sviluppato da alcune grandi imprese (automotive, industria del bianco, tecnologie per il wellness,...) richiede di essere radicalmente ripensato. Ci si chiede dunque se l'avvento dei sistemi cyber-fisici rappresenti da questo punto di visto un incontro tra mondo industriale e mondo informatico o possa diventare uno scontro tra una cultura solida e dunque regolamentata e soggetta a cambiamenti graduali e una cultura immateriale, più allergica alle norme e geneticamente in mutazione continua.

La sicurezza di questi sistemi è indubbiamente un nuovo problema di sicurezza che va affrontato a livello istituzionale, ma le minori dimensioni delle imprese italiane obbligano ad affrontare il problema anche dal punto di vista della competitività del paese.

La Cybersecurity delle imprese non è problema del responsabile dell'IT, ma un tema di strategia d'impresa che deve entrare nell'agenda del top management; ovviamente servono anche competenze tecniche per gestire questi aspetti e ruoli nuovi (analoghi ai Chief Information Security Officer delle grandi imprese) che sappiano governare questa variabile a livello alto e trasversale.

Come sempre il grande problema è la formazione, se consideriamo che la grande maggioranza dei laureati non ha avuto neppure la possibilità di un'alfabetizzazione di base su questi aspetti (e neppure su quelli della sostenibilità). Tuttavia, ancora una volta, non basterebbero i neolaureati perché siamo di fronte ad aspetti che devono essere affrontati oggi e non tra qualche anno, per cui si rende necessario un investimento massiccio nella formazione dei manager a cui anche il settore pubblico dovrebbe prestare attenzione.

*Bologna Business School, Università di Bologna
**Università di Modena e Reggio Emilia


IMPRESA & TERRITORI
Basilicata, nuovo stop all'Eni in Val d'Agri
La ceramica rilancia sugli Usa
«Il rischio dati non ci preoccupa»