Ufficio Stampa della Provincia autonoma di Trento
Piazza Dante 15, 38122 Trento
Tel. 0461 494614 - Fax 0461 494615
uff.stampa@provincia.tn.it

COMUNICATO n. 1720 del 05/06/2022

Cyber Security, non solo difesa ma anche strumento di sviluppo economico

FESTIVAL ECONOMIA TRENTO - Con la digitalizzazione in atto, la cyber security diventa un tema di grande rilevanza. Al Festival Economia di Trento, Pierangelo Soldavini, giornalista de Il Sole 24 Ore modera la tavola rotonda dedicata alla cyber security, con Marco Comastri, CEO Tinexta Cyber, con Laura Li Puma, responsabile del Laboratorio di Intelligenza Artificiale di Intesa Sanpaolo, con Andrea Rigoni, esperto di Cyber Security e con Antonio Teti dell'Università degli Studi "G. d'Annunzio" Chieti Pescara.

Nel primo trimestre di quest'anno, gli attacchi hacker sono aumentati del 40%. Stiamo parlando sia di cyber crime, criminalità informatica, ma anche di attacchi di altro genere, come la minaccia costante di bloccare l'intero paese. Dietro questi numeri ci sono inevitabilmente dei fenomeni.

Antonio Teti, esperto di scenari di sicurezza militare ed informatica, ha fornito un quadro molto chiaro di ciò che sta succedendo. "Parlare di cyber war è complicato, spesso se ne parla anche in maniera impropria. Fino ad oggi, proprio per il carattere tradizionale dell'approccio bellico russo, in verità non abbiamo ancora assistito ad una vera cyber war. Questo però non deve farci abbassare la guardia perché il vero impatto non è ancora avvenuto. Siamo più che altro di fronte ad attacchi che mirano alla saturazione delle risorse di un sistema informatico ma che in realtà vengono gestiti e fronteggiati in modo efficace. Il problema reale di questo conflitto - ha spiegato il professore - è che avrà breve durata e non si concluderà finché Putin non avrà conseguito una conquista dei territori a cui tiene, determinato a distruggere il contesto ucraino".

Per concretizzare gli attacchi di cyber war, come ha spiegato l'esperto Andrea Rigoni, devono sussistere ed allinearsi precise condizioni e situazioni. Di base, i principali attacchi sono contro obbiettivi vulnerabili, con target privato, come telecomunicazioni, elettricità, sistema finanziario. Quindi il paese è chiamato a proteggere non solo le infrastrutture sensibili ma tutto il sistema e questo non è un compito facile. Bisogna aggiungere che il digitale ha oltremodo cambiato il modo di erogare servizi critici e se ne sono aggiunti altri, come i social network ad esempio.

Da parte sua, Marco Comastri ha portato il punto di vista delle aziende. "Esiste un tema di fragilità diffusa che coinvolge tutte le imprese. Ogni azienda si sta trasformando in un'azienda digitale e questo porta inevitabilmente all'aumento di rischi. Se poi si calcola l'attuale congiuntura, la problematica si fa urgente. L'obiettivo è creare nel paese un pool sempre più allargato di professionisti che possano aiutare piccole e grandi imprese a gestire queste nuove problematiche per difendere la sovranità digitale di ogni realtà".

L'esempio di una realtà di impresa come Intesa Sanpaolo è stato riportato dalla responsabile del Laboratorio di Intelligenza Artificiale, Laura Li Puma che ha spiegato come Intelligenza Artificiale e Cyber Security debbano andare a braccetto per garantire la protezione e la sicurezza delle transazioni dei dati .

Dagli intervenuti è stato poi affrontato il tema della strategia nazionale di difesa e dei limiti che sembra attualmente presentare. I nodi principali sono la mancanza di esperti e le loro inadeguate retribuzioni. Si pensi che l'Agenzia per la Cyber Security nazionale sta reclutando personale ma in numeri minimali: si

punta a 300 elementi entro il 2026 contro i 1700 esperti già in forze nella rispettiva realtà in Germania e 2000 in quella francese. Si stima inoltre che effettivamente servano 100mila esperti in cyber security. Inoltre, c'è una reale fuga all'estero di queste figure proprio a causa di inadeguate retribuzioni.

Se si pensa che fronteggiare uno scenario di cyber war significa fronteggiare minacce quotidiane di un nemico sempre più competente e versatile, questa risulta essere una sfida costante che bisogna affrontare con un numero adeguato di competenze. Necessari quindi gli investimenti per trattenere i giovani, insinuando loro un senso di appartenenza verso il proprio paese ma anche e soprattutto premiando meritocrazia e competenze sulla base della retribuzione.

Lo scenario attuale prevede che nei prossimi 24 mesi saremo inondati di nuove norme europee che riguardano lo sviluppo sicuro del digitale. Bisogna cogliere gli effetti benefici di questa spinta regolatoria ma va aggiunta un'azione convinta nei confronti delle imprese per innescare consapevolezza e cultura, affinché la cyber security da strumento di difesa venga intesa come strumento di sviluppo che sostiene la nostra economia. Non solo uno scudo quindi, ma uno strumento strutturale per l'economia del futuro.

(ds)