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. 1325 del 23/05/2025

Cybersecurity: tra spie, spioni e hacker

Attacchi informatici sempre più sofisticati, uso dell'intelligenza artificiale da parte dei cybercriminali e normative europee in evoluzione. La sicurezza digitale è una sfida globale e condivisa in un'epoca in cui gli attacchi informatici sono ormai parte della cronaca quotidiana.

È quanto emerso durante l'incontro "Cybersecurity: spie, spioni e hacker", al Festival dell'Economia di Trento, in cui è intervenuto per la Fondazione Bruno Kessler Silvio Ranise, Direttore del Centro di Cybersecurity e Professore Ordinario dell'Università di Trento insieme a esperti di primo piano, Emilio Gisondi, Amministratore delegato di Tinexta Defence; Yuri Giuseppe Rassega, Head of Cyber Security di Enel; Fabio Scacciavillani, Fondatore di Nextperience Scf e Giovanni Andrea Toselli, Presidente e Amministratore Delegato di PwC Italia.

Il dibattito, moderato da Simone Casalini, direttore de Il T Quotidiano, ha messo in luce le trasformazioni in corso nel panorama della sicurezza digitale, un tema sempre più sensibile che riguarda tutti gli aspetti delle nostre vite: dalla sicurezza dei dati alla libertà personale.

Ranise (FBK), ha evidenziato le tre principali difficoltà che ostacolano la protezione efficace dei sistemi digitali: l'asimmetria tra attacco e difesa accentuata dall'uso malevolo di tecniche di intelligenza artificiale, l'estrema interconnessione degli ecosistemi digitali e la complessità nell'identificare i responsabili di un attacco informatico. Su tutti questi aspetti è necessario lavorare sia livello tecnico che organizzativo ed umano.

"E' fondamentale che la formazione in questo campo inizi fin dalle scuole elementari, per costruire una cultura digitale consapevole", ha spiegato Silvio Ranise nel suo intervento: "Parallelamente, è cruciale accrescere la consapevolezza di ogni lavoratore: la cybersecurity non è solo affare degli specialisti, ma una responsabilità condivisa. Ogni clic, ogni email aperta, ogni password scelta può diventare un punto di ingresso per un attacco. Le aziende devono investire in formazione continua per rendere tutti consapevoli dei possibili rischi che comportamenti individuali possono portare rispetto alla postura di sicurezza dell'intera organizzazione".

Il tema è delicato e i relatori hanno portato diverse esperienze e diversi punti di vista, tutti però rivolti verso un'unica direzione: la cybersecurity tocca la vita quotidiana delle persone ed è importante agire in modo corale.

La strada da percorrere secondo Emilio Gisondi, Amministratore delegato di Tinexta Defence - azienda privata che è entrata nel campo della sicurezza nazionale - è quella di costruire una sovranità tecnologica nazionale, che ci liberi dalla pericolosa dipendenza mondiale nella tecnologia.

Educazione alla sicurezza e all'uso dei dati - per tutti i cittadini e in particolare per le nuove generazioni che non sembrano essere ancora così sensibili a questo argomento - è la chiave per un digitale più sicuro, secondo Giovanni Andrea Toselli, Presidente e Amministratore Delegato di PwC Italia. Unita a un grande lavoro di sistema. Lo stesso lavoro di sistema - suggerito anche da Yuri Giuseppe Rassega, Head of Cyber Security di Enel - che potrebbe mettere in sicurezza intere filiere ottimizzando gli investimenti. La strada da percorrere in questo senso è ancora molta: la consapevolezza di cittadini e imprese è cresciuta, ma non a sufficienza perché il rischio è continuo e, soprattutto, continua a evolvere.

Un’azienda di medie-grandi dimensioni può ricevere 50 mila tentativi di infiltrazione al giorno, mentre una come Poste Italiane ne riceve 500 mila: sono questi i dati portati da Fabio Scacciavillani, Fondatore di Nextperience Scf ed economista. Il problema, dunque, è molto esteso e non bisogna pensare che riguardi “gli altri”.

L’incontro ha dunque confermato la complessità del tema: la cybersicurezza non è solo una questione tecnologica, ma un impegno sociale, normativo e organizzativo, che richiede un’azione corale tra enti pubblici, imprese, istituzioni di ricerca e cittadini.

(gr)