GIACOMO-ANDREOLI

Momola (ceo DHub e Cybertech - Engineering): «Roma hub della cybersecurity, ora si può accelerare sull'innovazione»

Per il numero uno delle aziende cybertech del gruppo Engineering Roma sta dando una forte spinta a un settore chiave dell'innovazione tecnologica, con un potenziale di crescita sempre più marcato, ma bisogna accelerare sulla capacità di sviluppare tecnologie proprietarie

«La Capitale si sta trasformando in uno dei principali hub italiani della cybersecurity : adesso può rafforzare il proprio ruolo puntando su innovazione, formazione e attrazione di investimenti. E competendo così al livello europeo». Fabio Momola è ceo DHub e Cybertech, aziende chiave del gruppo Engineering , e racconta a Il Messaggero la spinta che Roma sta dando a un settore chiave dell'innovazione tecnologica, con un potenziale di crescita sempre più marcato. Tutto questo in un momento in cui è cambiata «la natura stessa delle minacce cyber: non più solo attacchi informatici isolati, ma una guerra ibrida, che colpisce infrastrutture critiche e servizi essenziali ». Più in generale l'Italia è ancora indietro rispetto al resto d' Europa nella capacità di sviluppare tecnologie proprietarie. Ma, secondo Momola, «la strategia di rilancio è chiara: bisogna puntare su sovranità tecnologica, investimenti mirati e innovazione , soprattutto in ambiti come intelligenza artificiale e automazione».

Roma sta diventando un hub della cybersecurity in Italia? Può crescere ancora?

«Roma sta emergendo come uno dei principali poli della cybersecurity in Italia, con un posizionamento ben definito. La Capitale si distingue per la forte concentrazione di istituzioni, difesa e pubblica amministrazione, che la rendono centrale nelle strategie nazionali di sicurezza digitale. La presenza dell' Agenzia per la cybersicurezza nazionale insieme a università, centri di ricerca e grandi aziende Ict, contribuisce a consolidare un ecosistema sempre più strutturato. Il potenziale di crescita è significativo. La spinta normativa europea, l'aumento degli investimenti in cloud e infrastrutture critiche e la crescente domanda di competenze specialistiche stanno accelerando lo sviluppo del settore. Tuttavia, restano alcune criticità, come una minore presenza di startup e capitali privati rispetto ad altri hub.

In prospettiva, Roma può rafforzare il proprio ruolo puntando su innovazione, formazione e attrazione di investimenti, evolvendo da hub istituzionale a vero centro competitivo a livello europeo».

Quanto contano oggi gli investimenti e la presenza operativa di Engineering a Roma per lo sviluppo della sicurezza digitale? Qual è il valore aggiunto concreto per l'ecosistema romano?

«Grazie a circa 400 professionisti dedicati alla cybersecurity, a un Soc che solo nell'ultimo anno ha analizzato

oltre 2 miliardi di eventi cyber, il gruppo Engineering si pone come partner di rifermento per lo sviluppo della sicurezza digitale nella Capitale. Sempre a Roma stiamo investendo per costruire una control tower per l'adoption sicura dell' Intelligenza artificiale , con una piattaforma che sia in grado di osservare, rilevare e scoprire comportamenti rischiosi o anomali. Quella del gruppo non è quindi solo una presenza commerciale, ma operativa: dallo sviluppo di competenze avanzate alla collaborazione con istituzioni e industria su ambiti come l' IA applicata alla sicurezza . Il valore per l'ecosistema romano è quindi concreto e industriale. Da un lato, si rafforzano le competenze locali soprattutto tra i giovani, radicando sul territorio professionalità altamente specializzate; dall'altro, si crea un'integrazione tra pubblico e privato, che consente di sviluppare modelli operativi replicabili a livello nazionale ed europeo».

Perché la cybersecurity è diventata un tema centrale non solo per le aziende, ma anche per le capitali europee e il loro sviluppo?

«Perché è cambiata la natura stessa delle minacce. Non più solo attacchi informatici isolati, ma una guerra ibrida, che colpisce infrastrutture critiche e servizi essenziali. Capitali europee come Roma sono fortemente esposte. Il recente attacco cyber all' Università La Sapienza lo ha dimostrato bene. La sicurezza digitale è diventata un tema di stabilità economica, sociale e democratica del Paese, elevandosi a driver di sviluppo. Non è solo protezione, ma anche condizione abilitante per la crescita digitale e la fiducia dei cittadini. È fondamentale rafforzare le capacità di difesa , passando da un approccio reattivo a uno proattivo, che protegga dati, sistemi e identità lungo tutta la filiera».

A che punto è l'Italia rispetto ad altri Paesi europei sulla sicurezza informatica? E con quali strategie si rilanciano le azioni di cybersecurity?

«L'Italia ha fatto passi avanti importanti, ma resta ancora indietro rispetto ad altri Paesi europei, soprattutto nella capacità di sviluppare tecnologie proprietarie. Siamo forti consumatori di cybersecurity, ma meno produttori. Dal nostro punto di vista, la strategia per il rilancio è chiara: bisogna puntare su sovranità tecnologica, investimenti mirati e innovazione, soprattutto in ambiti come intelligenza artificiale e automazione. L'IA è un moltiplicatore di potenza sia per chi attacca sia per chi difende. Dobbiamo orchestrarla, non esserne orchestrati. Non serve inseguire modelli sempre più grandi e generici. Servono modelli di IA specializzati, agili e verticalizzabili: un'intelligenza artificiale sovrana, di cui abbiamo la governance totale».

Quali competenze servono oggi e come possono università e centri di ricerca formare nuovi professionisti?

«La cybersecurity richiede competenze sempre più avanzate e interdisciplinari, profili capaci di combinare tecnologia, intelligenza artificiale, analisi dei dati e conoscenza delle normative. Purtroppo, queste figure sono ancora troppo poche rispetto alla domanda delle aziende . Università e centri di ricerca hanno un ruolo strategico: continuare rafforzare i percorsi formativi, renderli più pratici e interdisciplinari, collaborare con le imprese. Senza competenze non c'è sicurezza: il capitale umano resta il vero fattore critico».

Quanto è importante

creare un ecosistema pubblico-privato per far crescere il settore della cybersecurity?

«È un elemento imprescindibile. La cybersecurity non può essere affrontata da un singolo attore, perché le minacce colpiscono interi sistemi Paese, non singole organizzazioni. Serve quindi un ecosistema pubblico-privato forte, basato su collaborazione, condivisione delle informazioni e integrazione tra istituzioni, grandi aziende e pmi innovative , per migliorare la difesa, ma anche per sviluppare una vera filiera industriale nazionale della cybersecurity, capace di generare innovazione, occupazione qualificata e sovranità tecnologica. La sicurezza non è solo una questione tecnica, ma una scelta strategica di sistema».