20-MAG-2026
da pag. 20 / foglio 1

Libero

Quotidiano - Dir. Resp.: Mario Sechi
Tiratura: 46851 Diffusione: 16727 Lettori: 224000 (Data Stampa 0006901)

IL COMMENTO

Una pandemia cyber può infettare le Pmi e devastare il Paese

BRUNO VILLOIS

Di cybersecurity si comincia a parlare oltre 50 anni fa, con la nascita delle prime reti dalle quali sorgerà Internet. A livello aziendale, la cybersecurity è fondamentale per la strategia di gestione del rischio informatico, dalle minacce comuni fino ad arrivare all'AI. Minacce sempre più sofisticate e frequenti obbligano ogni tipo di organizzazione ad intensificare massicciamente gli investimenti di prevenzione e mitigazione del rischio. Nel triennio in corso la spesa per la sicurezza informatica supererà i 400 miliardi di dollari. Bene ricordare che, secondo stime attendibili, il costo annuale a livello globale causato dalla criminalità, dovuto alle carenze della cybersecurity, nel 2025 avrebbe superato i 10 trilioni di dollari. C'è inoltre una convinzione da parte dei vertici dei sistemi economico-finanziari che l'instabilità geopolitica globale potrebbe portare ad attacchi catastrofici, difficilmente contenibili, in assenza di una straordinaria crescita dell'utilizzo della cybersecurity.

Le nazioni evolute aumentano continuamente le risorse finanziarie da destinare alle protezioni e alle difese informatiche. Un uguale impegno finanziario, forse anche maggiore, hanno adottato tutte le principali aziende globali, obbligando i componenti delle loro filiere a fare altrettanto. Impegni che impongono investimenti che da noi già le Pmi, figurarsi le micro imprese, non sono in grado di sostenere. Serve ricordare che, seppur con obiettivi diversi, ad inizio dell'attuale lustro, i sistemi pubblici e privati si stavano incamminando verso la messa in atto dell'ESG, acronimo che indica i tre pilastri fondamentali utilizzati per valutare l'impegno di un'organizzazione o di un'azienda in termini di sostenibilità e responsabilità etica. Il suo utilizzo è totalmente naufragato a causa dei costi che imponeva la sua adozione alle piccole e medie imprese. Nel caso della cybersecurity, per evitarne il fallimento, le cui conseguenze sarebbero drammatiche, è necessario che il Governo preveda risorse pubbliche, a fondo perduto, dedicate alle piccole e micro imprese, in modo che si possano dotare di adeguate forme di cybersecurity. Parimenti le maggiori rappresentanze datoriali, a cominciare da Confindustria e Confcommercio, dovrebbero stimolare i propri associati a disporre sia delle opportune conoscenze, istituendo programmi di formazione e aggiornamento permanente, sia di accordi con il sistema bancario per finanziare gli investimenti in cybersecurity senza che l'erogazione sia vincolata al merito creditizio. Importante che lo Stato attribuisca una certificazione, utilizzabile da chi si impegna ad inserire la cybersecurity tra i suoi costi non derogabili, e parimenti ne conceda le condizioni per l'accesso sia ai finanziamenti pubblici che a quelli bancari agevolati. L'intrusione su dati non adeguatamente protetti può innescare un catena di danni che possono coinvolgere a cascata infrastrutture critiche, catene di approvvigionamento e sistemi interconnessi, con conseguenze sistemiche sull'economia e sulle imprese. Il così detto Forum di Davos considera il rischio di una "pandemia cyber" come una minaccia strategica primaria. Investire a creare le condizioni per proteggere i soggetti operativi meno abbienti, come lo sono sovente le microimprese e le PMI, è necessario per evitare danni di dimensioni incalcolabile all'intera collettività.