

Cyber 4.0: oltre 5 milioni di euro per proteggere le Pmi dagli attacchi hacker

2025-03-26 11:32:33 di Marco Gemelli

URL:<https://forbes.it/2025/03/26/cyber-4-0-oltre-5-milioni-di-euro-per-proteggere-le-pmi-dagli-attacchi-hacker/>

Articolo tratto dal numero di marzo 2025 di Forbes Italia. [Abbonati!](#) **Uno scudo da oltre 5 milioni di euro per difendere le pmi italiane dai ripetuti attacchi hacker**, soprattutto provenienti dalla Russia. È con i fondi del Pnrr che attraverso Cyber 4.0 - il centro di competenze per la cybersecurity nazionale, soggetto attuatore del piano per conto del ministero delle Imprese - il nostro Paese tutela le piccole aziende sul tema della sicurezza digitale. Se una volta l'attenzione delle istituzioni era riservata soprattutto alle imprese ritenute strategiche o a quelle direttamente partecipate dallo Stato, ora che nel mirino degli hacker finisce un numero molto più ampio di siti, le maglie della protezione digitale si sono allargate. Gli oltre 5 milioni erogati si traducono in servizi avanzati per la sicurezza di dati, infrastrutture digitali e sistemi applicativi. Solo nel 2024 **Cyber 4.0 ha erogato più di 4 milioni di contributi** attraverso programmi incentivati di consulenza, orientamento e formazione, e negli ultimi quattro anni più di 7 milioni sono arrivati attraverso il cofinanziamento di progetti di ricerca e innovazione. Sempre attraverso Cyber 4.0 l'Agenzia nazionale per la cybersecurity sta per distribuire altri 16,5 milioni per le pmi europee, che dovranno mettersi in regola con la legge Cyber Resilience Act. Cyber 4.0 svilupperà le piattaforme tecnologiche e amministrerà gli incentivi per le pmi, attraverso la pubblicazione di open call per finanziamenti a cascata. **LEGGI ANCHE:** [Il lato oscuro dell'IA: oggi per realizzare un attacco cyber bastano quattro giorni](#)

Imprese e cybersecurity

“In dieci mesi sono finiti i fondi che avevamo previsto di utilizzare fino al 2026”, sottolinea Matteo Lucchetti, direttore di Cyber 4.0. “È netta la sensazione che le imprese siano passate da una fase interlocutoria, in cui la cybersecurity era considerata un tema da valutare per possibili investimenti futuri, a una fase di azione concreta. **Forse anche spinti dagli adeguamenti normativi richiesti da un quadro regolamentare sempre più fitto di obblighi e sanzioni** – in primis quanto previsto dalla direttiva europea Nis 2, che avrà un impatto diretto su decine di migliaia di imprese in Italia, stabilendo una strategia comune di cybersecurity per tutti gli stati membri – manager e imprenditori si stanno muovendo rapidamente per rafforzare i propri presidi di protezione degli asset digitali e le competenze del personale. Con la misura Pnrr che è stata recentemente rifinanziata, e che speriamo di erogare allo stesso ritmo, il ministero ha trovato una chiave per supportare queste imprese concretamente ed efficacemente. Il centro lavora come facilitatore per connettere le imprese ai finanziamenti e come garante della qualità di quanto erogato”.

Il decreto ministeriale

Insomma, il decreto ministeriale che attraverso **Cyber 4.0 supporterà la transizione digitale delle pmi italiane** si tradurrà in incentivi per imprese di ogni dimensione e servizi avanzati per garantire la sicurezza dei dati contro gli attacchi hacker. “Il volume di richieste e attività”, aggiunge Lucchetti, “testimonia da un lato l'efficacia delle misure che sono state predisposte per trasformare i fondi del Pnrr in azioni concrete di immediata fruibilità, e dall'altro come sia cresciuta la consapevolezza da parte delle imprese sui temi di cybersecurity e sulla necessità di agire per proteggere i propri asset digitali strategici”. A fronte di un valore totale di **4,6 milioni in servizi realizzati**, con un contributo medio dell'86% di cofinanziamento, oltre 150

aziende (71% piccole, 21% medie e 8% grandi) hanno usufruito del supporto di Cyber 4.0. Tra gli oltre 280 servizi erogati, quelli più richiesti sono di assessment e valutazione della propria postura, sia in termini di processi organizzativi che di tecnologie adottate o da adottare, ma anche di valutazione delle proprie vulnerabilità e di definizione di un percorso di miglioramento. E poi la **formazione**, su cui è nettamente cresciuta la richiesta non solo di competenze specialistiche, ma anche di educazione digitale di base. Ma quali categorie di pmi sono più esposte agli attacchi hacker? “Alcuni settori”, spiega Lucchetti, “sono meno pronti ad affrontare l’ondata crescente di attacchi alle proprie infrastrutture digitali. E sono quei settori, come il **manifatturiero**, che meno hanno investito in passato in questo ambito, perché non era ancora stata compiuta la trasformazione digitale dei processi produttivi. Tra i settori più critici inserirei anche quelli dei servizi sanitari, per la sensibilità dei dati trattati e quindi il loro valore, e dell’aerospazio, per la forte crescita prevista nel breve periodo e il valore strategico. Infine i servizi alla pubblica amministrazione”.

Cosa possono fare le Pmi per difendersi dagli hacker

Resta da capire quali accortezze possono attuare oggi le pmi per difendersi dagli hacker. “Abbiamo pubblicato un vademecum per la cybersecurity delle pmi e identificato 12 azioni per rendere più sicuro il loro business. La prima raccomandazione è lo sviluppo di una solida cultura sulla cybersecurity, essenziale per proteggersi dalle minacce informatiche. È indispensabile una formazione appropriata e periodica per tutti i dipendenti, in modo che possano riconoscere e affrontare le minacce. È importante, inoltre, affidarne la responsabilità a una persona con visione strategica, perché la cybersecurity deve essere considerata un obiettivo aziendale programmatico. Il responsabile dovrebbe essere coinvolto nei processi aziendali, conoscere l’organizzazione e il suo contesto. È importante sviluppare un piano di risposta agli incidenti che contenga orientamenti, ruoli e responsabilità chiari. Raccomando inoltre di censire gli incidenti informatici in un apposito registro: qualora si tratti di data breach, la normativa privacy richiede al titolare del trattamento di registrare formalmente le tentate o accadute violazioni dei dati personali. È fondamentale rendere sicuri l’accesso ai sistemi, i dispositivi, la propria rete e i back up, ma ancor di più condividere informazioni nella lotta contro la criminalità informatica”.