# Cyber 4.0: Polo della sicurezza informatica già per oltre 800 imprese

*Centinaia di realtà imprenditoriali si sono rivolte al Centro di Competenza nazionale per progetti, servizi e corsi di formazione ad alta specializzazione sulla sicurezza informatica*

*"Le Pmi sono il 76% delle aziende che ottengono gli incentivi Mimit per i nostri servizi; cresce la richiesta di formazione per cybersecurity manager", spiega Matteo Lucchetti, direttore Cyber 4.0*

Roma, 27 marzo 2024 – Un punto di riferimento per la cybersecurity delle Pmi a livello nazionale e un canale di accesso semplificato ai fondi del Pnrr per le aziende con obiettivi di sviluppo in questo ambito: sono circa **800 le imprese ingaggiate da Cyber 4.0** dall'inizio della sua attività, attraverso il finanziamento di progetti di innovazione, lo sviluppo di iniziative di info/ formazione, l'erogazione di servizi co-finanziati a valere sul Piano nazionale di ripresa e resilienza. Oltre **140 i corsi erogati** dal centro.

Numeri che rendono la dimensione del lavoro fin qui svolto dal Competence Center con sede a Roma e che prefigurano **un cambiamento culturale** all'orizzonte: *"La natura delle domande che riceviamo ci rivela che le piccole e le medie imprese italiane cominciano a comprendere che la cybersecurity non è soltanto una tecnologia o l'ennesimo software da aggiungere agli altri, ma un processo continuativo che entra nell'organizzazione aziendale, soprattutto con l'emergere di nuove figure manageriali",* spiega **Matteo Lucchetti, direttore di Cyber 4.0**.

*“**Le Pmi sono il 76% delle aziende che ottengono gli incentivi del Ministero dell’Innovazione e Made in Italy per accedere ai nostri servizi*** – prosegue Lucchetti –*. Fra questi i più richiesti sono di quattro tipi: assessment tecnico e organizzativo, formazione, test before invest e consulenza sull’innovazione. Significa che da un lato c’è l’intenzione di rivedere gli assetti organizzativi interni, per dare maggiore forza alla protezione dei dati e delle informazioni sensibili; dall’altro c’è la volontà di farsi trovare pronti a rispondere a eventuali criticità, sia con una valutazione dello stato attuale delle difese cyber, sia con un aggiornamento attivo delle competenze interne”.*

**In Italia** oltre il 99% delle aziende ha dimensione micro, piccola o media e il 97% di esse ha adottato uno o più sistemi digitali gestiti internamente. Oltre un quarto di esse ha subito attacchi di tipo cyber nel 2022, che ne hanno compromesso l’operatività per periodi di tempo più o meno lunghi.

Nel 2023, l’11% degli attacchi gravi globali è avvenuto in Italia (rispetto al 7,6% del 2022), gli attacchi nel nostro paese sono cresciuti del 65% rispetto all’anno precedente e un quarto del totale di quelli rivolti al manufacturing a livello globale riguarda realtà manifatturiere italiane (dati Rapporto Clusit 2024 sulla sicurezza Ict in Italia).

Secondo uno studio ENISA su base EU, nella grande maggioranza dei casi (più dell’80%) il canale primario attraverso cui è veicolato l’attacco verso le Pmi è quello del **social engineering.**

Non a caso, Cyber 4.0 raccomanda come primo dei 12 punti del **Vademecum sulla Cybersecurity** per le piccole e medie imprese, la necessità di sviluppare una solida cultura sulla cybersecurity, assumendo diverse misure: istituire una figura interna responsabile della sicurezza informatica, coinvolgere il personale, pubblicare le politiche ed eseguire audit per la

cybersicurezza.

*"La tipologia delle richieste di formazione che riceviamo ultimamente rappresenta una novità, in quanto descrive una necessità di lunga durata: sempre più aziende prendono coscienza della necessità di una revisione dell'organizzazione interna, investono nell'aggiornamento del proprio personale e programmano una crescita del proprio organigramma sul tema della cybersecurity* – spiega Lucchetti –*. Questo si realizza principalmente attraverso la modalità del* ***master*** *dedicato allo sviluppo di competenze per profili manageriali, come quelli realizzati da Campus biomedico e Luiss, soci del partenariato Cyber 4.0 che, oltre a essere nella faculty e a definire il programma, può* ***co-finanziare l'accesso delle aziende*** *a questa tipologia di corsi fino al 70%, attraverso fondi PNRR*".

Lo scenario tuttavia non è dei migliori, in tema di prevenzione: negli ultimi 12 mesi mediamente **appena il 15% delle aziende ha organizzato per i propri dipendenti corsi di formazione** o eventi di sensibilizzazione in merito ai rischi della criminalità informatica (19% in Ue, dati Eurobarometro Pmi e criminalità informatica).

La mancanza di competenze in questo settore è ben più vasta che nella sola Italia. **Nell'Unione europea mancano 300mila profili cyber**, un gap che non può essere colmato con l'attuale numero di laureati nel settore, quindi sono necessari ulteriori investimenti nel re-skilling e nell'upskilling.

*"Ed è quanto Cyber 4.0 permette di fare alle aziende italiane con i suoi* ***corsi di formazione, cofinanziati dal Pnrr*** – afferma Lucchetti –*. Mantenere le competenze è vitale in ambito cyber, attraversato da evoluzioni tecnologiche rapidissime e costanti, anche nell'arco di un solo anno. Tra gli altri corsi che il Centro può erogare, ci sono l'alfabetizzazione di base per imprese di qualunque settore; gli aggiornamenti tecnici avanzati per la formazione del personale su certificazioni professionali (standard Iso,*

*normative di settore, privacy…) delle aziende che producono software o servizi digitali; piani di awareness del personale attraverso corsi e attività più ampie per le grandi aziende".*

Cyber 4.0, va ricordato, è **soggetto attuatore Pnrr per conto del Ministero delle Imprese e del Made in Italy**, i cui fondi sono erogabili in forma di incentivi alle imprese e di co-finanziamento di progetti di ricerca e innovazione. Tra le altre attività in vista nei prossimi mesi, vi sono il lancio di una piattaforma di servizi per aziende attraverso la sottoscrizione di un abbonamento e i nuovi bandi di progetto, da sempre attività istituzionale del Centro di Competenza.


Matteo Lucchetti, direttore di Cyber 4.0

*"I numeri a livello nazionale offrono un quadro non*

*incoraggiante* ***le opportunità di crescita non mancano*** *e ci sono diverse condiz*

*io*
*ni*
*ch*
*e*
*fa*
*vo*
*ri*
*sc*
*on*
*o*
*un*
*a*
*ri*
*pr*
*es*
*a*
*de*
*ll*
*a*
*cy*
*be*
*rs*
*ec*
*ur*
*it*
*y*
—
co
nc
lu
de
Lu
cc
he
tt
i
-.

*Ci so no in pa rt ic ol ar e tr e fa tt or i mo lt o at tu al i in am bi to no rm at iv o: la di re tt iv*

*a* ***NIS2*** *, per un livello comune elevato di cybersicurezza in tutta l’Unione, che*

*dovrà essere recepita entro il prossimo ottobre; il* ***Cyber Resilience Act****, appena ap*

*provato dal Parlamento europeo, sui requisiti di security dei prodotti connessi*

*onentidigitaliimmessisulmercatoconformiamarchioCE,chelascia36mesidi*

*tempo ai produttori per adeguarsi; infine* ***l’Artificial Intelligence Act****, appena ap*

*provato, che introduce ulteriore livello di analisi del rischio per le tecn*

*ologie che utilizza nol' Intelligenza artificiale. In questo scenario, Cyber 4.0*

continuerà a essere un punto di riferimento affidabile per accompagnare policy ma

*ke*
*r,*
*im*
*pr*
*es*
*e*
*e*
*PA*
*in*
*un*
*pe*
*rc*
*or*
*so*
*di*
*cr*
*es*
*ci*
*ta*
*ve*
*rs*
*o*
*un*
*a*
*di*
*gi*
*ta*
*li*
*zz*
*az*
*io*
*ne*
*si*
*cu*
*ra*
*,*
*gr*

*azie a soluzioni concrete, strategiche e sostenibili”.*

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/cyber-4-0-polo-della-sicurezza-informatica-gia-per-oltre-800-imprese/