

CYBERSECURITY PER LE PMI

Presentato il Cyber Readiness Level: lo strumento per prevenire e sostenere la capacità di risposta e di resilienza ad attacchi cyber

Torino, 8 novembre 2022

Denial-of-service and distributed denial-of-service. Man-in-the-middle. Phishing and spear phishing. Drive-by. Sono questi i più diffusi, e spesso sconosciuti, attacchi informatici che ogni anno aggrediscono miliardi di device, cloud e reti. Difendersi richiede un approccio multilivello che parte dallo scegliere password complesse e arriva all'identificazione di attacchi e risposte efficaci.

Alle imprese serve una struttura di difesa sempre più costosa, ma non sempre adatta alle esigenze specifiche di ogni azienda. Da questa pluralità crescente di necessità, è nato **Cyber**, un progetto di **Fondirigenti**, il **fondo interprofessionale per la formazione continua dei dirigenti** a cui si affidano 14 mila imprese e più di 80 mila manager, realizzato da **Fondazione Piemonte Innova** e promosso dall'**Unione Industriali di Torino** e **Federmanager Torino/Apdai**.

In otto mesi di lavoro, 20 pmi guidate da esperti di cybersecurity e di processi organizzativi, hanno collaborato per identificare e poi standardizzare i fabbisogni in tema di cybersecurity, di fronte a minacce sempre più sofisticate. Il risultato di questo lavoro è il *Cyber Readiness Level*, presentato oggi davanti a un pubblico di manager e imprenditori presso Eataly a Torino. Si tratta di **un questionario strutturato su 5 aree tematiche** (protezione, gestione e tecnologie, organizzazione e processi, compliance e normative, fattore umano) per un totale di 25 domande per comprendere il livello di sicurezza aziendale e fornire delle indicazioni pratiche sulle aree dove è necessario implementare le difese. Il *Cyber Readiness Level* fornisce anche una serie di buone pratiche, competenze, strumenti e metodi da adottare, che vengono veicolati alle imprese tramite infografiche e videopillole, per prevenire e sostenere la capacità di risposta e di resilienza ad attacchi cyber.

*“Fondirigenti, in linea con le priorità definite dal PNRR, ha investito nel progetto Cyber con l’obiettivo di aumentare la consapevolezza e le competenze dei dirigenti in materia di sicurezza dei dati – ha dichiarato **Massimo Sabatini**, Direttore Generale di Fondirigenti - l’indagine ha evidenziato l’importanza dell’educazione alla cybersecurity e la necessità di una formazione mirata sul tema rivolta anche al top management. La diffusione della cultura della sicurezza e il fattore umano, oltre alle dotazioni tecnologiche, sono fondamentali per affrontare proattivamente i rischi di attacchi informatici. Un aiuto concreto ai manager nell’identificare i propri fabbisogni viene dal modello di autoanalisi della ‘Cyber Readiness’ aziendale proposto dal Progetto, modello che diffonderemo mediante la nostra Open Innovation Library (on line su www.fondirigenti.it)”.*

*“La cybersicurezza è un tassello fondamentale della trasformazione digitale – ha sottolineato **Massimiliano Cipolletta**, Presidente di Fondazione Piemonte Innova – e sempre più una necessità in tutti i settori; non deve essere appannaggio esclusivo di una comunità specializzata di esperti informatici, bensì deve essere integrata in tutti gli ambiti, incluse le PMI. Grazie a questo progetto abbiamo sostenuto le imprese, in particolare le PMI che sono le più esposte, verso un’articolata evoluzione culturale e progettuale per dotarsi di strumenti e competenze adeguate ad assicurare la protezione dei loro dati, processi e asset. Con Cyber abbiamo proposto un approccio che coinvolge l’intera cultura aziendale, un modello fatto di azioni concrete e buone pratiche da mettere in atto prima, durante e dopo un potenziale attacco”.*

Il questionario è stato testato presso 20 aziende partecipanti a Cyber, mentre alla base del progetto ci sono le risposte arrivate da un’indagine sul tema della cybersecurity a cui hanno risposto oltre 100 aziende, prevalentemente pmi piemontesi. La valutazione emersa era di un livello di sicurezza aziendale medio per una impresa su due (44%), dove i motivi che muovono le imprese a investire in cybersecurity sono ancora di natura esterna: il rispetto delle normative (46%) e l’evidenza – per chi li ha affrontati – di attacchi (32%) o eventi avversi (42%) sono il motore principale. **Cybersecurity** per le aziende interpellate vuol anche dire controllo e verifica periodica dei sistemi (61%), aggiornamento tecnologico (58%) e una cultura aziendale orientata alla sicurezza (57%). Da qui la necessità di una formazione a tappeto, che non escluda azioni specifiche di formazione verso il top management e i profili tecnici.

“I fabbisogni censiti da Cyber – ha aggiunto Sabatini – forniscono preziosi input alla definizione dei futuri Avvisi del Fondo, che da tempo ha messo al centro della propria azione la digitalizzazione e la sicurezza informatica. Abbiamo infatti dedicato ai piani formativi sulla cybersicurezza specifiche linee di finanziamento con l’Avviso 1/2022 (sulla transizione resiliente), che ha evidenziato una robusta domanda di formazione sul tema, e con l’Avviso 2/2022 appena pubblicato (dedicato alla leadership femminile) per il quale ci aspettiamo una conferma delle tendenze positive già registrate a riprova della crescente centralità strategica della cybersicurezza nelle scelte delle imprese e del management”.

Ufficio Stampa

Fondirigenti

Maria Lara Bernardi – 065903910

bernardi@fondirigenti.it

Piemonte Innova

Chiara Cavanna – 3357425800

Jan Pellissier – 3477845273

media@piemonteinnova.it