



Costruzione di un modello di valutazione del rischio cybersicurezza per le PMI

SCENARIO DI RIFERIMENTO

In un mondo sempre più interconnesso siamo ogni giorno più vulnerabili. L'accelerazione con cui l'innovazione e l'interconnessione procedono, fa sì che le infrastrutture e gli schemi attuali non riescano a tenere il passo con la rapidità di questa evoluzione: questa situazione rappresenta un alto fattore di rischio. L'epidemia di Covid-19, ancora purtroppo presente a livello mondiale e i recenti mutamenti negli scenari geo-politici internazionali hanno dato ulteriore impulso alla criminalità informatica, che ha saputo sfruttare l'occasione per sferrare numerosi attacchi informatici, ormai con frequenza quotidiana come ci raccontano i fatti di cronaca e minare la sicurezza per i dati delle aziende e quella online dei cittadini.

La cyber-sicurezza è perciò un tassello fondamentale della trasformazione digitale e sempre più una necessità in tutti i settori e deve essere integrata in tutte le aziende, incluse le PMI.

Si conferma quindi come essenziale un cambio di passo e diventa **fondamentale l'investimento in iniziative che siano capaci di sostenere le imprese verso un'articolata evoluzione culturale e progettuale**, che aumenti la conoscenza sui rischi informatici, sugli strumenti di monitoraggio e prevenzione.

TARGET

Le attività, partendo da una survey in materia di awareness delle imprese sui rischi della cybersicurezza, prevedranno il coinvolgimento diretto di **20 imprese** rappresentanti delle

esigenze di prevenzione e gestione della cybersicurezza, provenienti da diversi settori industriali, che parteciperanno a un **percorso guidato di co-progettazione e capacity building della durata di 8 mesi** [maggio-dicembre 2022]. Il percorso si rivolge principalmente a dirigenti e manager d'azienda, in particolare dell'area ICT e con ruoli decisionali nelle funzioni compliance, sicurezza, servizi generali, legal, ricerca.

OBIETTIVI

Il progetto CYBER vuole investigare lo stato dell'arte e le strategie adottate dalle imprese nell'acquisire competenze e prevederà lo studio e l'utilizzo di strumenti e policy che permettano ai manager e alle aziende di prevenire e gestire i rischi cyber acquisendo maggiori competenze e conoscendo tecnologie, processi e modelli organizzativi e di business per resistere a possibili attacchi informatici.

Il progetto CYBER intende, in particolare:

- **investigare lo stato dell'arte e le strategie adottate** dalle imprese nell'acquisire conoscenza e competenze in ambito cyber-security;
- **progettare e testare strumenti e metodi atti a sostenere una concreta evoluzione di competenze** delle imprese e dirigenti coinvolti. In particolare:
- **fornire gli elementi di replicabilità e scalabilità** per rendere tali elementi di sostegno fruibili da un numero di imprese il più ampio possibile su scala nazionale.



ATTIVITÀ CORE

Il progetto prevede un'indagine preliminare volta a investigare la consapevolezza delle aziende sul tema della cyber-security. Dopo un **workshop informativo** sul tema, una serie di appuntamenti con i manager delle imprese coinvolte serviranno a esplorare i fabbisogni di tecnologie e strutturazione dei processi sul tema della cyber-sicurezza. I **metodi partecipativi** scelti, dai focus group ai world café, permetteranno quindi di attivare **reali processi di condivisione di conoscenze e buone pratiche tra interlocutori provenienti da mondi differenti per settore, competenze ed esperienza**. La metodologia è studiata per aumentare le conoscenze e le capacità dei dirigenti in termini di guida dell'azienda in tema di cyber-sicurezza, con sviluppo di competenze di adattabilità e resilienza.

[LINK](#)

RISULTATI

La raccolta e l'analisi dei dati delle prime fasi porterà a strutturare tre principali output:

- il **Cyber Readiness Level**, strumento di analisi - auto-assessment indirizzato in particolare modo alle PMI;
- il **Pattern of Cyber Resilience**, modello composto da un mix innovativo di buone pratiche, competenze, strumenti e metodi da adottare - in grado di indicare possibili strategie che le PMI possono mettere in atto per prevenire e sostenere la capacità di risposta e di resilienza ad attacchi cyber;
- le **Cyber stories**, il racconto, in formato videointervista, di storie e casi di successo in ambito cyber-security.