CASE- Center for Social and Economic Research

Mappatura delle minacce informatiche per le micro, piccole e medie imprese nell'UE

Executive summary

La strategia della Commissione Europea per le PMI per un'Europa Sostenibile e Digitale ha riconosciuto la vulnerabilità delle PMI alle minacce informatiche e ha identificato la cybersecurity come uno degli aspetti chiave dell'upskilling digitale. Anche a livello globale, le minacce informatiche emergono tra i principali rischi globali a breve termine (World Economic Forum, 2021) e diventano una minaccia costante per la maggior parte delle imprese in mezzo all'accelerata trasformazione digitale indotta dalla crisi Covid-19 (OECD, 2021).

Questo rapporto identifica gli incidenti su internet, tra cui phishing, malware e attacchi sul web, come **le più frequenti minacce informatiche** rilevanti per le micro, piccole e medie imprese dell'UE. In linea con ENISA (2020), altre importanti minacce informatiche includono anche lo spam, il denial of service, il furto di identità, le violazioni dei dati, la minaccia insider, i botnet, la manipolazione fisica e i danni, la fuga di informazioni, il cyberespionage e il cryptojacking. Allo stesso tempo, mentre l'accesso a Internet e le modalità di lavoro a distanza potrebbero aumentare l'esposizione delle micro, piccole e medie imprese ai rischi della sicurezza informatica, il fattore umano è un'altra importante fonte di vulnerabilità digitale, dato che circa l'84% di tutti i cyberattacchi nell'UE si basa sull'ingegneria sociale per attirare le persone a divulgare informazioni sensibili o a cliccare su un link che potrebbe contenere file dannosi (ENISA, 2020).

Le **analisi dei Paesi** presentate in questo rapporto sottolineano ulteriormente la crescente importanza dei temi della sicurezza informatica a livello nazionale e confermano un livello relativamente basso di conoscenza della sicurezza informatica tra le micro, piccole e medie imprese. Secondo i risultati dell'Eurobarometro 2020, la quota di intervistati che ha riferito di essere "non ben informata" sui rischi del crimine informatico si attesta al 67% per la Romania e l'Italia, al 55% per la Spagna e al 43% per la Polonia. Inoltre, a livello aziendale, solo il 7% delle PMI in Romania ha reso i propri dipendenti consapevoli dei loro obblighi in materia di sicurezza ICT attraverso corsi di formazione obbligatori. Le PMI in Spagna, Polonia e Italia, a loro volta, hanno ottenuto risultati più vicini e anche al di sopra della media UE con cifre del 20%, 30% e 34%, rispettivamente. Quando si considera il divario tra le PMI e le grandi imprese, tuttavia, la Romania e l'Italia hanno uno dei più piccoli divari a livello UE - solo 21 pp e 23 pp, rispettivamente. Mentre la Spagna ha un divario relativamente più alto al 27%, è riuscita a rimanere al di sotto della media di 30 punti percentuali dell'UE-27 e del divario di 35 punti percentuali registrato in Polonia.

Pertanto, le micro, piccole e medie imprese dell'UE spesso rimangono indietro rispetto alle grandi imprese in termini di **consapevolezza** e **prontezza** nell'affrontare le proliferanti minacce informatiche. Ancora più importante, le maggiori e più frequenti minacce informatiche sono anche quelle su cui il livello di consapevolezza nell'UE rimane più basso. La mancanza di consapevolezza e impegno da parte del management, in particolare, è la sfida comune e più spesso citata (ENISA, 2021). Di conseguenza, solo il 30% delle PMI dell'UE ricorre a misure di cybersecurity avanzate e meno del 30% delle PMI

With the support of the Erasmus+ programme of the European Union. This document and its contents reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the Erasmus+ Programme of the European Union

dell'UE-27 sensibilizza i propri dipendenti sugli obblighi di sicurezza ICT attraverso corsi di formazione obbligatori - quasi il doppio in meno rispetto alla grande impresa.

Altre **sfide strutturali** che minano una maggiore preparazione delle micro, piccole e medie imprese includono anche una bassa consapevolezza di cybersecurity del personale, una protezione inadeguata delle informazioni critiche e sensibili, la mancanza di budget, la mancanza di specialisti dedicati all'IT e alla cybersecurity, e la mancanza di linee guida adeguate alla cybersecurity specifiche per le PMI.

Un certo numero di **iniziative a livello UE**, tra cui, tra l'altro, la Strategia UE per la Cybersecurity, l'Agenzia UE per la Cybersecurity, così come i quadri SMESEC e Make_SME_Digital, permettono di colmare i divari di competenze e rafforzare la resilienza collettiva contro le minacce informatiche. Questi sono ulteriormente supportati dalle **iniziative a livello nazionale** - ad esempio, la Piattaforma Nazionale Polacca per la Cybersecurity e il Programma di Cooperazione per la Cybersecurity PWCyber e il Quadro Nazionale Italiano per la Cybersecurity e il Consorzio Interuniversitario Nazionale per l'Informatica (CINI) - che stabiliscono quadri nazionali di cybersecurity e sostengono lo sviluppo delle competenze digitali a livello locale.

Tuttavia, come discusso in questo rapporto e nei profili dei singoli Paesi, sono necessarie azioni strategiche più complete per affrontare la mancanza sistemica di capacità di cybersecurity tra le micro, piccole e medie imprese dell'UE. Queste dovrebbero concentrarsi sul rafforzamento di:

(i) **consapevolezza informatica** tra le MSME, promuovendo una migliore comprensione della sicurezza informatica in generale e adattando il contenuto e i canali delle campagne di sensibilizzazione al contesto e alle esigenze settoriali delle MSME.

(ii) **resilienza informatica** delle MSME, creando standard e linee guida di sicurezza informatica incentrati sulle MSME, promuovendo l'uso di quadri di gestione del rischio informatico nelle MSME e rendendo la sicurezza informatica più accessibile.

(iii) **reattività informatica** delle MSME, promuovendo la formazione volontaria e obbligatoria dei dipendenti e sostenendo lo sviluppo di protocolli di sicurezza semplificati.

With the support of the Erasmus+ programme of the European Union. This document and its contents reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the Erasmus+ Programme of the European Union