I dati dello studio di I-Com evidenziano l'impatto degli adempimenti sulla competitività

Sicurezza dei dati, troppi oneri

La moltiplicazione di prescrizioni ostacola la compliance

Pagina a cura
DI ANTONIO LONGO

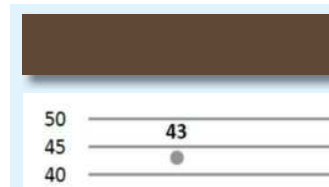
Per il 74% delle imprese italiane il crescente numero di adempimenti previsti dalle normative in materia di cybersicurezza impatta negativamente sulla competitività aziendale. In particolare, ad ostacolare il processo di compliance, ossia l'adeguamento al dettato legislativo, sono la mancanza di competenze idonee (51,2%), l'incertezza interpretativa della normativa (44%) e la moltiplicazione di prescrizioni che impongono adempimenti diversi (41%). Secondo l'81% delle aziende per migliorare l'ecosistema della cybersecurity si dovrebbe puntare sulla consapevolezza e sulla formazione del personale in maniera diversificata per ruolo e competenze.

Si tratta dello scenario delineato dal rapporto "La sfida della cybersicurezza per un'Italia sempre più digitale. Politiche, competenze, regole", realizzato dall'Istituto per la Competitività (I-Com), che fornisce una panoramica sullo stato dell'arte della cybersicurezza in Italia e in Europa in merito a approcci normativi, grado di sicurezza, attacchi subiti da aziende e istituzioni pubbliche, sistemi di certificazione, consapevolezza di aziende e cittadini.

"Cruciale insistere sul rafforzamento della cultura di base in cybersicurezza e investire su iniziative idonee a formare i cittadini, affinché acquisiscano al meglio queste capacità", osserva Stefano da Empoli, presidente I-Com. "Molte delle iniziative già attive in questo campo nascono e si sviluppano anche grazie al settore privato, spesso in collaborazione e/o col patrocinio di enti pubblici. Appare, dunque, utile che queste forme di collaborazione pubblico-privato possano essere rafforzate e messe maggiormente a sistema".

Dai dati Clusit, citati nel focus, si evince come negli ultimi anni il numero di cyberattacchi annuali a livello globale sia cresciuto di oltre il 60%, passando da 1.554 del 2018 a 2.489 del 2022. Inoltre, anche i valori del primo semestre del 2023 appaiono preoccupanti, in quanto si è raggiunta la quota di 1.382 attacchi, ben 637 in più rispetto al primo semestre del 2018. Negli ultimi tre anni, peraltro, prevalgono gli attacchi che hanno prodotto effetti dannosi importanti per le vittime, comprese ingenti perdite economiche e di dati. In Italia, nel primo semestre del 2023, sono stati registrati 132 attacchi di particolare gravità, ossia una media di 22 al mese, circa dieci volte più elevata rispetto a quella rilevata nel 2018.

A rischio la competitività aziendale. In base agli esiti dell'indagine sull'impatto degli adempimenti prescritti dalle normative sulla cybersicurezza sulla competitività aziendale, per il 39% delle grandi imprese la principale criticità è legata agli investimenti tecnico-organizzativi necessari alla compliance, il 54% delle aziende di medie dimensioni si concentra sulla numerosità degli oneri burocratici e amministrativi richiesti, il 29% delle piccole imprese si preoccupa prioritariamente dell'impatto sui rapporti con la filiera. Per quanto riguarda, invece, i fattori che rendono difficoltosa la compliance rispetto alle norme, prevale la mancanza di competenze idonee, sia internamente sia sul mercato del lavoro, a seguire l'incertezza interpretativa della normativa e la moltiplicazione, spesso disorganica, di prescrizioni che impongono adempimenti diversi ma che sono tese al raggiungimento del medesimo obiettivo. Sul fronte dell'eventuale incremento delle risorse destinate alla cybersecurity, il 51,2% dei rispondenti sta ancora valutando tale eventualità, il 36,1% delle imprese ha già deciso di aumentare gli investimenti mentre il restante 12,6% non stanzierà ulteriori risorse. Peraltro, oltre che puntare sulla consapevolezza e sulla formazione del personale, le aziende ritengono che vadano riservati più aiuti finanziari alle imprese e rafforzata la collaborazione pubblico-privata.



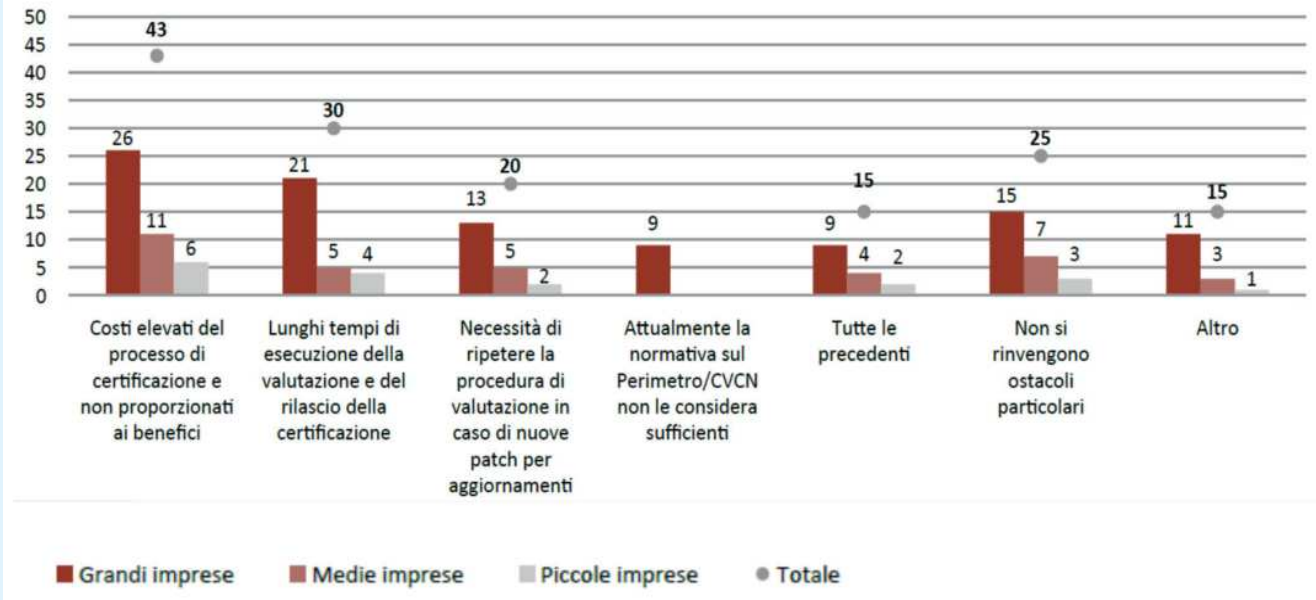
In merito all'adozione di una o più certificazioni volontarie di cybersicurezza, la maggior parte delle imprese delle tre classi dimensionali non ha conseguito alcun tipo di certificazione. Considerando solo le grandi imprese rispondenti, il 36% delle stesse ha già adottato una o più certificazioni di cybersecurity, mentre un ulteriore 8% sta lavorando per ottenere la prima entro un anno. Tra le medie imprese i risultati sono ben diversi, solo l'11% ha acquisito almeno una certificazione, mentre il 14% intende ottenere la prima certificazione entro un anno.

Quanto alle piccole imprese, solo una di quelle che ha risposto all'indagine ha già adottato una certificazione e un'altra punta a perseguire la prima entro un anno. Tra gli ostacoli percepiti dalle imprese per l'ottenimento di una certificazione volontaria, il principale (38%) risiede nei costi elevati che non sono considerati come proporzionati ai benefici che ne possono conseguire. A seguire, quasi il 27% sostiene che i tempi per l'esecuzione della valutazione e il rilascio della certificazione sono troppo lunghi. Tra coloro che hanno dichiarato di avere adottato almeno una certificazione, i principali effetti direttamente riconducibili ad essa sono il miglioramento dell'immagine e della reputazione dell'impresa nei confronti degli stakeholders (45%), una maggiore consapevolezza dei dipendenti e dei collaboratori esterni (39,7%) e più possibilità di partecipare a bandi di gara pubblici o privati (29,5%).

Il panorama legislativo. Vista la crescente importanza del tema si assiste al proliferare di interventi normativi, tanto a livello europeo quanto a livello nazionale. L'Ue sta delineando un ecosistema normativo della sicurezza informatica piuttosto articolato. Il regolamento n. 881/2019 (Cybersecurity Act) ha fissato gli obiettivi, i compiti e gli aspetti organizzativi relativi all'Enisa (Agenzia dell'Unione europea per la cybersicurezza) e ha delineato un quadro per l'introduzione di sistemi europei di certificazione della cybersecurity. Nel 2020 la Commissione europea ha lanciato il "Cybersecurity package", costituito in primis dalla "Strategia dell'Ue in materia di cibersicurezza per il decennio digitale", a cui ha fatto seguito la direttiva n. 2557/2022 sulla resilienza dei soggetti critici (direttiva Cer – Resilience of critical entities). Il 27 dicembre 2022, invece, è stata approvata la direttiva 2022/2555 (Nis2) che ha prescritto l'adozione di misure tecniche, organizzative e operative adeguate e proporzionate in materia di cybersicurezza. La direttiva, inoltre, ha declinato obblighi di segnalazione in caso di incidenti significativi, ha previsto misure di vigilanza e individuato misure per garantire la sicurezza della filiera. Ad integrazione, nello scorso mese di settembre la Commissione europea ha pubblicato i primi orientamenti sull'applicazione di alcune norme fondamentali della direttiva Nis2. Il termine di recepimento per gli Stati membri delle direttive Cer e Nis2 è fissato al prossimo 17 ottobre.

Anche in Italia si è definito un nuovo ecosistema normativo in materia di sicurezza informatica. Il decreto legge n. 105/2019, convertito con la legge n. 133/2019, ha istituito il Perimetro di sicurezza nazionale cibernetica (Psnc) al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori. Nel 2021 è stata, poi, istituita, in attuazione delle previsioni del Pnrr, l'Agenzia per la cybersicurezza nazionale (Acn), mentre proprio nei giorni scorsi ha avuto il via libera definitivo da parte del parlamento Legge di delegazione europea 2022-2023 che si occupa, in particolare, dei principi e dei criteri per l'esercizio della delega per il recepimento della direttiva Nis2.

Gli ostacoli verso la certificazione



Fonte: "La sfida della cybersicurezza per un'Italia sempre più digitale. Politiche, competenze, regole", I-Com