CENTRO STUDI

TIM

## Abstract White Paper

# Verso la NIS 2 - Gli effetti sulle imprese e sull'economia italiana della nuova Direttiva sulla cybersecurity

### Solo il 32% delle PMI è pronto a gestire attacchi informatici

Sempre più spesso gli attacchi informatici sfruttano le debolezze dei sistemi di difesa delle imprese, che possono quindi compromettere il grado di sicurezza complessivo di intere filiere. In particolare, in Italia 4,4 milioni di imprese (circa il 95% del totale) hanno meno di dieci dipendenti e il 61% delle PMI si ritiene bersaglio di attacchi informatici. Tuttavia, solo il 32% è pronto a gestirli. Il 13% dichiara di avere subito un incidente cyber negli ultimi anni, ma non sempre questi vengono rilevati o resi noti. Migliora invece la percezione del rischio: l'86% delle PMI conosce e teme almeno una minaccia tra ransomware, malware DDoS e phishing e il 91% teme conseguenze da un attacco (dati: Cyber Index PMI).

A partire da queste ed altre evidenze, tra cui i dati dell'Agenzia di Cybersicurezza Nazionale (ACN), della Commissione Europea e del Security Operation Center (SOC) di TIM, il Centro Studi TIM ha realizzato il White Paper '*Verso la NIS 2 - Gli effetti sulle imprese e sull'economia italiana della nuova Direttiva sulla cybersecurity*', allo scopo di analizzare gli impatti economici e le esternalità positive derivanti dall'adozione della Direttiva europea 'Network and Information Systems 2' (NIS 2) in Italia.

### Sette imprese su 10 percepiscono attacchi in aumento

Dal 2021 gli incidenti cyber sono il rischio più sentito da parte delle imprese italiane e più di 7 grandi imprese su 10 hanno percepito attacchi in aumento nel corso dell'ultimo anno, anche per una maggiore consapevolezza dovuta al miglioramento degli strumenti di rilevazione: cresce il ruolo dell'intelligenza artificiale utilizzata da quasi 6 grandi imprese su 10 per ragioni di sicurezza informatica, anche se solo il 22% la utilizza in maniera estesa per identificare anomalie, nuove minacce o correlare tra di loro eventi che possono essere causati da un cyberattacco (dati indagine CISO Osservatorio Cybesecurity del Politecnico di Milano).

Tuttavia, l'Intelligenza artificiale può anche essere utilizzata dagli aggressori per rendere più dirompenti gli attacchi.

### Un data breach in Italia ha un costo medio di 3,6 milioni di euro

In Italia un attacco informatico capace di violare i dati (data breach) può comportare un costo medio di 3,6 milioni di euro. A livello mondiale, invece, l'impatto stimato è di circa 4,1 milioni di euro (dati IBM Security). In particolare, i costi relativi ad un data breach sono l'insieme di più fattori: il 30% è imputabile alla perdita di fatturato e ben il 35,5% – la componente con il peso maggiore - è attribuibile alla rilevazione ed escalation dell'incidente. Il 27% è rappresentato dai costi per il ripristino dei dati e, infine, il restante 8,3% dai costi di notifica. Inoltre, i costi aumentano del 27% quando è coinvolta una infrastruttura critica ed esplodono quando i data violati sono dell'ordine dei 50 milioni. Il 5% sul costo viene inoltre influenzato dalla compliance regolatoria.

## La Direttiva europea NIS 2: chi deve adeguarsi e quali misure sono previste

La Direttiva NIS 2 delinea i requisiti di cybersicurezza per le organizzazioni che operano nell'Unione Europea (UE), al fine di garantire un livello elevato e comune di protezione tra gli Stati membri. Una delle novità più importanti è l'applicazione anche alle piccole e medie aziende che rientrano nella catena di fornitura di settori considerati strategici, oltre che a tutte le organizzazioni pubbliche e private con più di 50 dipendenti e ricavi annui superiori a 10 milioni di euro. La mancata conformità alla NIS 2 comporterà sanzioni significative. Le misure previste spaziano dall'analisi del rischio alla gestione degli incidenti, dalla continuità aziendale alla sicurezza della catena di approvvigionamento e dei sistemi informatici. Ulteriore attenzione è richiesta in relazione alle strategie cyber, alla formazione dei dipendenti, alla crittografia e strumenti di autenticazione a due fattori. I settori industriali presi in considerazione sono inoltre più numerosi rispetto alla precedente normativa (NIS 1): manifattura, alimentare, servizi postali, ricerca, chimica, gestione rifiuti, acque reflue, spazio, servizi ICT, digitali e Pubblica Amministrazione, oltre a energia, trasporti, sanità, infrastrutture digitali, acqua potabile e finanza. La nuova Direttiva dovrà essere recepita negli ordinamenti giuridici nazionali entro il 17 ottobre 2024, ma gli Stati membri avranno tempo fino al 17 aprile 2025 per finalizzare l'elenco delle organizzazioni che dovranno conformarsi, anche ampliando il perimetro settoriale o includendo entità minori con un ruolo chiave.

## I benefici per azienda fino a 900 mila euro annui, a fronte di un costo medio di adeguamento di circa 280 mila euro

Secondo le stime del Centro Studi TIM su dati ENISA e della Commissione Europea, l'introduzione della Direttiva NIS 2 genererà una diminuzione degli incidenti del 6% annuo. Per una grande azienda che subisce 60 incidenti annui, con un costo che può variare dai 3 milioni ai 15 milioni di euro a seconda della percentuale degli incidenti severi, il beneficio annuo con NIS 2 può valutarsi dai 180 mila ai 900 mila euro annui. Ciò prefigura un ritorno positivo sugli investimenti in cybersecurity (Return on Security Investments - ROSI) già a partire dal secondo anno. In generale, i costi di adeguamento alla NIS2 possono variare da meno di 100 mila euro sino a oltre 5 milioni di euro in base alla dimensione dell'azienda, al settore di appartenenza e a seconda che l'impresa sia già nel perimetro di applicazione della precedente Direttiva NIS 1 o meno. Il costo medio di adeguamento a livello europeo è di 283 mila euro per un'azienda media o grande. Si tratta di un costo complessivo che include la formazione del personale, l'acquisizione di competenze non presenti nel perimetro aziendale, l'acquisto di soluzioni software e di nuovi apparati, gli eventuali servizi di consulenza per l'adeguamento ed altre spese.

## Errori umani, scarsa formazione e sistemi non aggiornati i principali fattori di rischio

I fattori di rischio di attacchi cyber sono molto variegati per le aziende di qualsiasi dimensione. Quello principale è il fattore umano, dovuto spesso ad una non adeguata formazione e cultura della sicurezza dei dipendenti. Ma complessivamente sono i fattori tecnici quelli alla base dell'alta vulnerabilità delle aziende al pericolo cyber. Sistemi IT non aggiornati con le ultime patch di

sicurezza e sistemi operativi obsoleti sono i fattori più impattanti, seguiti da una scarsa attenzione alla sicurezza della filiera.

## DATI DI SCENARIO

### Un fenomeno in esplosione: nel 2023 gli incidenti informatici sono aumentati del 141%

In Italia il numero di attacchi informatici è in forte crescita e nel 2023 si è registrato un aumento degli incidenti del 141% . Secondo i dati di CSIRT Italia - la struttura tecnico operativa dell'Agenza di Cybersecurity Nazionale (ACN) –sono stati inoltre 3302 i soggetti target di attacchi informatici (+187% rispetto all'anno precedente) e sono in rapido aumento gli asset a rischio: 3624, quasi 4 volte quelli del 2022 (764). L'accelerazione è dettata dalla maggior dipendenza di imprese e cittadini dal digitale, ma anche dal deterioramento del quadro geopolitico globale che ha portato ad un forte impulso del cybercrime. Le dimensioni del fenomeno sono in generale più grandi rispetto alle rilevazioni ufficiali riferibili essenzialmente ai danni resi noti da enti pubblici o aziende medio-grandi. Rimangono fuori dal conteggio gli incidenti non rilevati o non riportati da entità che non hanno l'obbligo di comunicazione (ad esempio le PMI), anche per evitare danni reputazionali.

### Nel 2023 è raddoppiato il 'peso' degli attacchi ad alta intensità

Nel 2023 in Italia gli attacchi ad alta intensità di tipo DDoS - cioè quelli in cui i criminali sovraccaricano siti web, server o risorse di rete con un elevato volume di traffico dannoso – hanno rappresentato il 29% del totale degli attacchi, secondo i dati rilevati da TIM, pari al doppio rispetto all'anno precedente. Più in generale, l'Italia è il terzo Paese in Europa (e sesto al mondo) per numero di attacchi DDoS (263), e primo Paese UE per attacchi ransomware (176) caratterizzati dalla richiesta di riscatto. Anche a livello europeo, gli attacchi DDoS e ransomware (rispettivamente il 21% e 31% del totale) sono i più diffusi. L'UE, inoltre, rappresenta il secondo bersaglio a livello mondiale (884 attacchi ransomware) dopo gli Stati Uniti.

### Italia indietro per investimenti in cybersecurity. La sanità è il settore con la maggiore crescita attesa

La vulnerabilità del nostro Paese in termini di sicurezza informatica è fortemente influenzata dal livello di investimenti di aziende e Pubblica Amministrazione in cybersecurity. Nel 2023, la spesa in cybersecurity in Italia è stata di circa 2 miliardi di euro, pari a circa lo 0,12% del PIL nazionale. Si tratta di un valore particolarmente basso in rapporto ad altri Paesi di riferimento: in Francia e Germania la spesa in cybersecurity si attesta attorno allo 0,24% - esattamente il doppio rispetto all'Italia – e negli USA questo valore cresce fino allo 0,3% del PIL. Il panorama italiano degli investimenti in cybersecurity è molto variegato: il settore con la maggior crescita attesa (+19% in media l'anno tra il 2023 ed il 2026) è la sanità, mentre i settori che investono di più in cybersicurezza nel nostro Paese (circa 400 milioni di euro nel 2023) sono le banche e l'industria.