24-NOV-2025
da pag. 1-6 / foglio 1 / 3

Il Sole 24 ORE
Quotidiano - Dir. Resp.: Fabio Tamburini
Tiratura: 54208 Diffusione: 113068 Lettori: 657000 (Data Stampa 0006489)

SICUREZZA INFORMATICA: INCENTIVI FRENATI DALL'EFFETTO BUROCRAZIA

di **Ivan Cimmarusti**
—*a pagina 6*

Cybersicurezza: incentivi a metà fra burocrazia e spese escluse

Il quadro. Dal maxi ammortamento con detrazione dei costi al voucher del Mimit con plafond da 150 milioni: tutte le misure a sostegno delle imprese per il 2025-2026. Fuori gli oneri per servizi It. Procedure complesse e tempi di accesso frenano l'utilizzo

Il Fondo di garanzia Pmi copre fino all'80% dei prestiti per progetti It, riducendo costi e assorbimento di capitale

Pagina a cura di
Ivan Cimmarusti

Non è solo una questione di quanti soldi ci sono in campo. Il punto vero, quando si parla di cybersicurezza delle Pmi italiane, è come quelle risorse sono progettate, rese accessibili, strutturate nel tempo.

Le misure pubbliche oggi in vigore sono davvero adeguate a proteggere le imprese, mentre gli attacchi informatici si moltiplicano e diventano sempre più sofisticati? Quanto lo Stato accompagna concretamente queste realtà produttive nell'investimento – spesso oneroso – in infrastrutture di sicurezza? E soprattutto: gli strumenti messi sul tavolo sono davvero all'altezza della minaccia o stiamo combattendo ransomware e phishing con armi spuntate?

Per capire quanto e come il sistema pubblico stia aiutando le imprese in questa transizione, Tinexta – gruppo specializzato in trasformazione digitale e crescita delle Pmi – tramite le aziende del Gruppo Tinexta Cyber e Tinexta Innovation Hub ha elaborato per il Sole 24 Ore una mappa dettagliata di agevolazioni, contributi, finanziamenti e programmi Ue disponibili tra il 2025 e il 2026 per potenziare la cybersicurezza aziendale (si veda la tabella). Perché se è vero che una parte della partita si gioca sulla consapevolezza – riconoscere ed evitare un'email anomala resta essenziale – è altrettanto vero che non basta: senza investimenti in sicurezza informatica (sistemi aggiornati, infrastrutture, gestione professionale) il confine tra tentato attacco e disastro resta sottilissimo. La "geografia degli incentivi", pur rappresentando un punto di svolta, dimostra però un quadro incompleto.

Le misure in campo

Il perno è il nuovo maxi ammortamento 2026 – previsto allo stato dal Ddl di Bilancio –, che aumenta le quote deducibili per beni strumentali nuovi, inclusi software, sistemi e piattaforme per proteggere reti, dati e impianti, secondo gli allegati A e B della legge 232/2016 (legge di Bilancio 2017) in tema cyber. In base al testo attuale del Ddl, vale per investimenti effettuati nel 2026 (con possibile coda al 30 giugno 2027) e prevede maggiorazioni decrescenti, ma con intensità massima su investimenti fino a 2,5 milioni di euro. È la misura chiamata a rimpiazzare progressivamente Transizione 4.0 e 5.0, restando cumulabile con altri incentivi entro il costo del bene.

Sul fronte dei contributi diretti spicca il voucher "Cloud & Cybersecurity" del Mimit (2025), che rimborsa fino al 50% delle spese per servizi cloud e soluzioni di sicurezza (Mfa, firewall, cifratura, Siem, backup), con importi tra 4mila e 40mila euro per impresa e una dotazione di circa 150 milioni, rivolto a Pmi e microimprese.

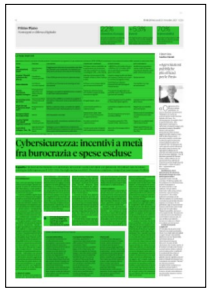
Accanto a queste leve agiscono strumenti finanziari già noti ma orientabili al cyber: Nuova Sabatini (contributo in conto interessi su finanziamenti per tecnologie digitali); finanziamenti Simest per progetti di digitalizzazione per la competitività internazionale con quota a fondo perduto; Fondo di garanzia Pmi, che copre fino all'80% dei prestiti per progetti It, riducendo costi e assorbimento di capitale.

A livello locale, bandi regionali e camerali (ad esempio i Voucher digitali I4.0) coprono audit, consulenze e soluzioni di sicurezza con incentivi tra il 40% e il 60 per cento. Nei grandi contratti di sviluppo e nelle Zes/Zls, infine, la componente cyber è finanziabile se integrata nei progetti industriali sopra i 20 milioni di euro.

I nodi da sciogliere

Secondo Tinexta Innovation Hub, c'è grande attesa per i nuovi maxi ammortamenti 2026, che possono realmente alleggerire il peso degli investimenti tecnologici sui bilanci aziendali. E si iniziano finalmente a vedere misure specifiche, pensate proprio per la cybersicurezza delle Pmi.

Tuttavia, molte agevolazioni – pur citando la cybersicurezza tra gli obiettivi – non coprono in modo pieno tutte le spese effettivamente



Il Sole 24 ORE
Quotidiano - Dir. Resp.: Fabio Tamburini
Tiratura: 54208 Diffusione: 113068 Lettori: 657000 (Data Stampa 0006489)

necessarie per garantire livelli adeguati di protezione. Restano spesso ai margini i costi ricorrenti per servizi It, attività di governance, gestione del rischio e servizi gestiti: elementi ormai indispensabili per un approccio maturo e continuativo alla sicurezza informatica.

Come ricordano gli esperti, la cybersecurity non è un intervento "una tantum", né un progetto che si conclude con la consegna di un software. È un processo continuo, che richiede prevenzione, monitoraggio costante e adattamento alle nuove minacce. Se gli incentivi non seguono questa logica, rischiano di mitigare solo parzialmente il problema.

A tutto questo si aggiunge un altro ostacolo ben noto agli imprenditori: la complessità delle procedure e i tempi di accesso alle misure. Bandi complicati, documentazione stratificata, finestre temporali ristrette e iter lunghi scoraggiano molte imprese, che spesso non hanno un ufficio interno dedicato solamente a intercettare e gestire incentivi pubblici.

Un quadro, insomma, che dovrà essere modellato. Anche perché c'è un livello più alto che inquieta: le intelligence europee registrano il proliferare di attacchi di natura "statuale". Sono offensive condotte da Paesi come Russia, Cina, Corea del Nord, Iran con l'obiettivo esplicito di indebolire le economie del continente europeo (secondo la società Crowdstrike l'Italia è tra i primi cinque Paesi europei per numero di attacchi). Una forma di guerra ibrida che colpisce al cuore i sistemi produttivi, con attacchi alle imprese, e mina la fiducia dei cittadini verso le istituzioni, anche attraverso campagne di disinformazione che tendono a mitizzare altre economie rivali, come nel caso della Russia. Temi oggetto del Consiglio supremo della difesa della scorsa settimana, presieduto dal presidente della Repubblica, Sergio Mattarella. Si pensi che secondo l'Agenzia per la cybersicurezza nazionale, nei primi sei mesi del 2025 gli eventi sono aumentati del 53% rispetto allo stesso periodo dello scorso anno.

22%

Obiettivo Europa

Secondo Crowdstrike, società Usa di cybersicurezza, le economie europee rappresentano il 22% degli obiettivi globali

+53%

Eventi

Per l'Agenzia per la cybersicurezza nazionale, in sei mesi del 2025 gli eventi cyber sono aumentati del 53% rispetto allo scorso anno

70%

Vulnerabilità

Secondo Tinexta Cyber, il 70% degli attacchi alle Pmi sfrutta vulnerabilità facili da intercettare

EURO-ECONOMIE SOTTO ATTACCO

Le analisi della Difesa
«Il comparto manifatturiero risulta particolarmente bersagliato, in gran parte a causa della prevalenza di piccole e medie imprese prive di strutture di difesa adeguate, che lo rendono uno dei settori più colpiti dai ransomware». È questo uno degli allarmi contenuti nel "Non paper" del ministero della Difesa, illustrato dal ministro Guido Crosetto nel Consiglio supremo della Difesa della scorsa settimana.
Il principale varco resta la posta elettronica: email costruite ad arte vengono usate per sottrarre informazioni sensibili, aprendo la strada al ricatto

Il comparto manifatturiero
In Europa, quest'anno, il ransomware è già cresciuto del 48% rispetto al 2024. Colpisce soprattutto i Paesi economicamente più appetibili: Regno Unito e Germania, con l'Italia terza seguita da Francia e Spagna. I dati sono della società di cybersicurezza Crowdstrike. Nel 92% dei casi l'incursione combina cifratura dei file ed esfiltrazione dei dati. I bersagli non cambiano: manifatturiero, servizi professionali e tecnologici, industria. Con sfumature locali. In Italia, i più colpiti sono manifatturiero, vendita al dettaglio, mondo universitario e industria

I Paesi ostili
I conflitti armati, dalla guerra in Ucraina alle tensioni in Medio Oriente, stanno alimentando l'ondata di attività cyber in Europa. I gruppi legati agli Stati - Russia, Corea del Nord, Cina, Iran, in particolare - usano soprattutto il cyberspazio per spiare governi ed eserciti, sostenere lo sforzo bellico e amplificare campagne di informazione e disinformazione. In alcuni casi l'accesso alle reti viene "armato" per colpire infrastrutture critiche e funzioni essenziali dello Stato. Parallelamente continuano le operazioni di spionaggio digitale e gli attacchi opportunistici a scopo di profitto

Il Sole 24 ORE
Quotidiano - Dir. Resp.: Fabio Tamburini
Tiratura: 54208 Diffusione: 113068 Lettori: 657000 (Data Stampa 0006489)

La mappa degli aiuti

Agevolazioni fiscali, contributi a fondo perduto, finanziamenti e programmi Ue per sostenere nel biennio 2025-2026 gli investimenti in sicurezza informatica delle imprese (in particolare Pmi)

MISURA	TIPOLOGIA	COSA PREVEDE	CYBERSECURITY AMMISSIBILE	INTENSITÀ/IMPORTI	NOTE/CUMULABILITÀ
Maxi ammortamenti 2026*	Agevolazione fiscale	Maggiorazione del costo di acquisizione dei beni strumentali nuovi (materiali e immateriali) con deduzione più alta di ammortamenti o leasing	Software, sistemi, piattaforme e applicazioni per protezione reti, dati, programmi e macchine (allegati A e B L. 232/2016)	+180% fino a 2,5 milioni di euro; +100% tra 2,5-10 milioni; 50% tra 10-20 milioni; premialità green fino 220%	Sostituisce progressivamente crediti d'imposta Transizione 4.0/5.0. Cumulabile nel limite del costo
Voucher "Cloud & Cybersecurity" (Mimit)	Contributo a fondo perduto	Fino al 50% per servizi cloud e cybersicurezza	Soluzioni di sicurezza It (Mfa, firewall, cifratura, Siem, backup e altri)	Importo massimo del contributo per impresa: 20mila euro. Importo minimo di progetto: 4mila	Gestione Mimit
Nuova Sabatini	Contributo in conto impianti	Contributo su finanziamenti-leasing per beni strumentali	Software e tecnologie digitali per sicurezza informatica	Contributo su interessi (parametrato alla tipologia di investimento)	Cumulabile con maxi ammortamenti
Simest – Transizione digitale/ecologica	Finanziamento agevolato con quota a fondo perduto	Sostegno a progetti di digitalizzazione a supporto dell'internazionalizzazione	Spese per cybersicurezza ammissibili a supporto della transizione digitale	Finanziamento agevolato con possibile quota a fondo perduto (percentuali variabili)	
Fondo di Garanzia per le Pmi	Garanzia pubblica su finanziamenti bancari	Garanzia fino all'80% su prestiti per progetti di sicurezza It, riducendo costo e assorbimento di capitale	Progetti digital-cyber	Copertura garanzia fino all'80% (in base alle regole vigenti)	Complementare a prestiti e altre misure
Digital Europe Programme 2025–2027	Programma Ue – bandi	Bandi su cybersicurezza, competenze digitali, infrastrutture dati. Partecipazione in consorzi	Linee-bandi specifici su cybersicurezza	Contributi a progetto secondo bando	Regole Ue; cumulabilità secondo bando
European Digital Innovation Hubs	Servizi	Servizi gratuiti o scontati	Assessment cyber, test-before-invest, formazione e supporto tecnico	Sconti/erogazione servizi (no contributi diretti)	Riduce costi di consulenza; complementare ad altre misure
Voucher Digitali I4.0 e bandi regionali/camerali	Contributo a fondo perduto	Spese per audit, consulenze e soluzioni di sicurezza informatica	Acquisto prodotti di cybersicurezza	Frequentemente 40-70%; importi: 5mila-10mila euro	Regole di cumulabilità definite dai bandi locali
Contratti di sviluppo / Zes / Zls	Agevolazioni per grandi investimenti	Sostegno a nuovi stabilimenti, ampliamenti, diversificazioni; la componente cyber è ammissibile se parte dell'investimento produttivo	Componente cyber integrata nell'investimento industriale	Secondo schema agevolativo previsto	Regole specifiche per ciascuno schema (Contratti/ Zes/Zls)

(*) Regole attualmente previste dalla bozza della legge di bilancio - Fonte: Tinexta Innovation Hub per il Sole 24 Ore