INSURANCE Daily

N. 2972 GIOVEDÌ 2 APRILE 2026

PRIMO PIANO

Calano i costi dei prodotti unit-linked

Eiopa ha pubblicato la sua relazione annuale sulla distribuzione e sulle performance dei prodotti di investimento assicurativi al dettaglio nell'Unione Europea, relativa al periodo fra il 1° gennaio 2020 e il 31 dicembre 2024. Basata su un campione di quasi 6.000 prodotti di 175 imprese, che rappresentano oltre il 60% dei premi unit-linked dello Spazio economico europeo, e di 1.677 prodotti con caratteristiche pensionistiche, la relazione fornisce una panoramica anche dei costi.

I prodotti unit-linked, e i contratti ibridi assimilabili, hanno beneficiato della solida performance dei mercati finanziari e al 2024 hanno conseguito rendimenti netti positivi per i consumatori, con una media del 7,5% per i prodotti a rischio medio-basso (l'80% del campione) e del 16,9% per quelli con indicatori di rischio più elevati. Parlando di distribuzione, la bancassicurazione è rimasto il canale dominante, pesando per il 70% dei premi totali, mentre le vendite online si sono attestate su un modesto 2,4%.

Nel 2024, i costi associati ai prodotti unit-linked hanno registrato una diminuzione media di otto punti base, "a testimonianza – scrive Eiopa – di una maggiore attenzione alla Product oversight and governance e al value-for-money". Tuttavia, l'analisi ha evidenziato che i costi variano tra gli Stati membri, indicando prezzi "strutturalmente più elevati in alcuni mercati, il che richiede ulteriori interventi a livello Ue per garantire risultati equi e coerenti per i consumatori", sottolinea l'autorità.

F.A.

TECNOLOGIE

Il crimine informatico nel 2028 sarà la terza economia al mondo

È la previsione di Munich Re nel suo nuovo "Cyber insurance: Risks and trends 2026". Con un peso globale previsto di circa 14mila miliardi di dollari, supererà il prodotto interno lordo combinato di Germania, Giappone e India. Una minaccia che sa sempre rinnovarsi

Il mondo, nel 2026, non è un posto tranquillo. Se l'avevamo capito ben prima dell'inizio di quest'anno, in cui le paradigmatiche tensioni geopolitiche si sono trasformate in conflitti armati aperti, oggi i rischi politici stanno facendo una concorrenza spietata alle minacce che una volta erano chiamate emergenti. Tra queste, per stare solo ai settori che implicano uno sguardo al futuro, il cyber risk richiede una gestione sempre più consapevole. I rischi informatici, siano essi derivanti da attacchi dolosi o da errori umani (o guasti delle macchine), possono minacciare l'esistenza stessa delle aziende e avere un impatto enorme sull'ecosistema, estendendosi a intere economie e società.

"Se la criminalità informatica fosse un Paese, sarebbe la terza economia più grande del mondo", scrivono gli analisti di **Munich Re** nel loro nuovo *Cyber insurance: Risks and trends 2026*, che inquadra le tendenze in atto nel settore, attraverso una prospettiva globale, partendo dai propri modelli interni, monitorando e quantificando le minacce informatiche.

UNA MANCANZA DI PROTEZIONE GLOBALE

Con un peso globale previsto di circa 14mila miliardi di dollari nel 2028, il valore della criminalità informatica supererà il prodotto interno lordo combinato di Germania, Giappone e India.

Il panorama del rischio informatico continua a essere plasmato dall'aumento della frequenza e dell'impatto degli attacchi e degli eventi non dolosi. "Nel complesso – sottolinea Munich Re – la stragrande maggioranza dei rischi informatici non è protetta".

Dal punto di vista del riassicuratore, le principali perdite assicurate derivano da ransomware, violazione dei dati (data breach), compromissione della posta elettronica aziendale (*Business email compromise*, Bec) e attacchi distribuiti di negazione del servizio (*Distributed denial of service*, Ddos), cioè quando, ad esempio, un sito è sommerso da finti accessi che rendono impossibile l'ingresso a chi davvero vuole consultarlo e deve lavorarci dentro.

COME EVOLVONO LE MINACCE

Il ransomware rimane la principale causa di richieste di risarcimento per attacchi informatici. Secondo i dati di Munich Re e **Mandiant**, il numero di attacchi segnalati è aumentato di quasi il 50% nel 2025 rispetto all'anno precedente e il trend è in continua crescita. Ma, come noto, gli attacchi ransomware si sono da tempo spinti oltre la semplice crittografia dei dati: per aumentarne l'efficacia, gli

aggressori sono sempre più interessati alla pura esfiltrazione dei dati senza crittografia. I data breach possono derivare da eventi informatici dolosi, ma anche non volontari, come la divulgazione o la raccolta di informazioni personali. Lo studio *Munich Re Global Cyber Risk and Insurance Survey 2026* ha rilevato che il 64% dei dirigenti C-level coinvolti nel sondaggio era preoccupato per le violazioni dei dati nella propria organizzazione, mentre il 25% ne era già stato colpito.


© Markus Spiske - Pixabay

Le frodi Bec, che spesso si traducono in frodi sui trasferimenti di fondi (Ftf), sono una delle principali preoccupazioni per gli amministratori: nel *Global Cybersecurity Outlook 2026* del **World Economic Forum** (Wef), si scopre che il 73% degli intervistati è stato direttamente colpito, o conosce qualcuno che lo è stato, da frodi informatiche nel 2025. Di fatto, i vertici ora considerano le frodi Bec e il *phishing* più rischiose del ransomware.

Gli attacchi informatici coordinati, lanciati da una rete di dispositivi compromessi e infetti da malware, sono più che raddoppiatI nel 2025 rispetto all'anno prima. I fornitori di sicurezza hanno segnalato attacchi massicci, sempre più mirati alle infrastrutture e alle risorse di rete per saturare i sistemi. In questo ambito, sono ormai da tempo disponibili servizi Ddos a pagamento, che facilitano il compito di chi, anche non esperto, vuole compiere un attacco informatico di questo tipo. Questi atti possono servire a diversi scopi: dalla pressione sulle vittime per ottenere un riscatto, ad attività più sofisticate, fino a fare interessi geopolitici nelle guerre ibride.

LA MAGGIOR PARTE DEI SINISTRI RIGUARDA MICROIMPRESE E PMI

Analizzando i dati di Munich Re relativi a tutti i sinistri gestiti attivamente nel suo portafoglio, quelli subiti direttamente da un'organizzazione rimangono predominanti con il 62% rispetto ai sinistri che coinvolgono terzi e che quindi innescano un meccanismo di responsabilità per danni a terzi. Il rimborso dei sinistri assicurati è determinato principalmente da interruzione dell'attività, responsabilità in materia di privacy e gestione degli incidenti.

"Sebbene l'attenzione generale sia ancora focalizzata sulle grandi aziende – fa sapere la compagnia di riassicurazione –, la maggior parte degli incidenti informatici e delle relative richieste di risarcimento riguarda le microimprese e le Pmi".

Osservando l'andamento dei sinistri dal 2021, i casi dolosi sono dominanti, con il quadro generale fortemente influenzato dal crescente numero di attacchi ransomware. Tuttavia, anche le richieste di risarcimento per sinistri non dolosi stanno acquisendo importanza: sono attribuibili a errori umani, software difettosi o, sempre più spesso, a *pixel litigation*, cioè contenziosi, spesso *class action*, intentati contro aziende che utilizzano strumenti di tracciamento web, per raccogliere dati degli utenti senza il loro consenso esplicito.

UN'ALLENZA TRA GEOPOLITICA E CRIMINALITÀ ORGANIZZATA

Vale la pena, infine, concentrarsi brevemente su uno degli ambiti più problematici di cui si è solo accennato in apertura: la geopolitica. Nel contesto di estreme tensioni, che possono sfociare, come si è visto, in conflitti, il cyberspazio sta diventando un'arena fondamentale per ottenere vantaggi politici, economici e militari. Il confine tra minacce sponsorizzate dagli Stati e gruppi di criminali che operano a favore di Stati che li tollera si sta facendo sempre più labile, così come le motivazioni di chi colpisce: spionaggio, sabotaggio di infrastrutture critiche e catene di approvvigionamento, o semplice guadagno personale.

Le campagne Ddos da parte di hacker-attivisti che si muovono spontaneamente sono spesso attacchi di basso-medio livello, mentre le compromissioni delle catene di fornitura e il lancio di malware su larga scala sono quasi sempre attribuibili ad hacker sponsorizzati da Stati che operano insieme a nuovi gruppi in ecosistemi di attacco e difesa. Ma gli attacchi sono anche il risultato di alleanze che integrano obiettivi geopolitici in sistemi criminali, a scopo di lucro.

Circa il 64% delle organizzazioni prese in considerazione nello studio del Wef pensa di essere un potenziale bersaglio di attacchi informatici a sfondo geopolitico. Coloro che sono coinvolti nelle catene di approvvigionamento e nelle infrastrutture critiche, ad esempio nei settori della difesa, dell'energia, della finanza e delle telecomunicazioni, sono, quindi, particolarmente a rischio.

Fabrizio Aurilia

Per approfondire su www.insurancetrade.it:

- *La Francia mette in guardia sull'hacking di Stato*
- *Furto di dati, cresce il pericolo di truffe più complesse*

INSURANCE Daily

N. 2972 GIOVEDÌ 2 APRILE 2026

RICERCHE

L'equilibrio precario delle materie prime critiche

I settori delle energie rinnovabili e del digitale, in piena transizione, necessitano di minerali strategici per la produzione. Si tratta di un mercato soggetto a rischi importanti, a partire dal controllo dell'estrazione e dalla vita residua dei giacimenti fino agli impatti geopolitici. L'Europa è in rincorsa, ma ne va della vitalità dei comparti produttivi di alta tecnologia

Le complessità geopolitiche ed economiche degli ultimi anni hanno un impatto diretto sull'approvvigionamento di alcune materie prime, definite critiche in quanto fondamentali per le produzioni strategiche e in particolare per le tecnologie per la produzione di energia rinnovabile, l'elettronica, le batterie. A questo limitato ma essenziale comparto economico, l'**Area Studi Mediobanca** ha dedicato un'analisi pubblicata a marzo dal titolo *Materie prime critiche e impatto sulle imprese italiane*. Le materie prime critiche (mpc) sono individuabili in un elenco stilato dall'Unione Europea per identificare i materiali rilevanti per l'industria ma a rischio di approvvigionamento. Si tratta di 34 minerali, 26 dei quali sono utilizzati nella fabbricazione di tecnologie per la produzione energetica da fonti rinnovabili. Più nel dettaglio, nel gruppo delle 34 mpc la Ue ne identifica 17 considerate materie prime strategiche (mps) per la transizione verde, quella digitale, la difesa e l'aerospaziale. Le mps per la transizione energetica trovano a oggi utilizzo, spesso prevalente, anche in altri settori produttivi, ma in prospettiva la quota destinata al green andrà aumentando. Secondo l'**Agenzia internazionale dell'energia** (Iea), la domanda in volumi dei sei minerali fondamentali per la transizione crescerà del 48% entro il 2040 nello scenario base, ma del 90% se si perseguiranno in maniera coerente gli obiettivi net-zero al 2050. In questo modo, la quota destinata alle tecnologie energetiche pulite sul totale dei volumi passerà dall'attuale 28% al 42% (scenario intermedio) nel 2030.

Un controllo del processo sempre più critico

La definizione di materie prime critiche è legata tanto alla funzione fondamentale che svolgono nei settori tecnologici quanto alle difficoltà di approvvigionamento. In questo senso, alcune peculiarità fanno comprendere sia gli aspetti economici sia quelli geopolitici legati alle mpc.

In primo luogo, si tratta di minerali scarsamente disponibili tanto in termini di mercato quanto, in prospettiva, in termini assoluti. Guardando al mercato, l'attività estrattiva è complessa e costosa, quindi conveniente a determinate condizioni, a partire dai volumi. Nel 2023 il mercato delle prime sei mpc era stimato in 350 miliardi di dollari, ma se si guarda al 2030 nella prospettiva net-zero il valore salirebbe a 1.100 miliardi. L'altro aspetto, ancor più centrale, riguarda la vita residua delle riserve di tali minerali: al ritmo di estrazione attuale si valuta per il rame una disponibilità in natura per altri 43 anni, 36 anni per il nichel, 128 per il litio. In realtà, i tempi descritti di esaurimento delle riserve si ridurranno in maniera molto sensibile all'aumentare dei quantitativi richiesti al 2030. Vanno poi considerati la complessità estrattiva e l'impatto ambientale della lavorazione, che crescono in proporzione allo sfruttamento e comportano costi ingenti.

In questa visione, si apre il tema della sostituibilità delle mpc con altre (naturali o artificiali), un aspetto che attiene alla ricerca scientifica e industriale e che è in ampio sviluppo.

Un altro fronte geopolitico

Due temi chiave sono la localizzazione dei luoghi di estrazione e la provenienza delle imprese estrattive, che attivano una relazione diretta con gli equilibri geopolitici. Considerando 24 mpc, il 71% è prodotto in soli quattro paesi; la Cina è tra i primi tre produttori per 16 mpc, con minore frequenza

ma alta rilevanza appaiono anche Russia, Brasile, Congo e Australia. L'Asia, l'Africa e l'America si suddividono quasi tutta la quota mondiale di mpc e, a parte la Russia, l'unico paese europeo che compare tra i principali produttori è la Norvegia (3% della quota mondiale di silicio).

Sull'accessibilità alle risorse influisce soprattutto la proprietà delle società che controllano l'estrazione e in questo caso il mondo occidentale riconquista un po' di spazio. Oltre alla Cina che è la vera protagonista del mercato delle mpc, i paesi che esercitano un più ampio controllo societario sono Usa, Australia, Francia, Sudafrica e Regno Unito, solo marginale il ruolo degli altri paesi Ue. Quello minerario è un comparto fortemente oligopolista. Secondo quanto riportato nello studio di Mediobanca, "circa due terzi dei paesi con dotazioni di minerali critici vedono oltre il 50% del proprio settore minerario societariamente controllato da entità straniere. A ciò si aggiunge che circa un terzo di questi paesi non è in grado di esercitare alcun controllo sulla propria produzione di minerali critici".

Dalla Ue scelte strategiche insufficienti

Per colmare il gap di disponibilità delle mpc, l'Unione Europea si è mossa su più fronti, affidando la propria politica al *Regolamento sulle materie prime critiche* e stanziando finanziamenti che tuttavia sono gestiti in maniera frammentata, riducendo la loro efficacia.

Secondo lo studio di Mediobanca, il Regolamento presenta dei limiti di governance e di struttura delle disposizioni, limitandosi a trattare solo di materie prime strategiche mps, con obiettivi al 2030 non vincolanti, stabiliti in aggregato e non per singolo minerale. I macro obiettivi previsti riguardano la diversificazione delle importazioni di materie prime da paesi extra Ue; il potenziamento delle attività estrattive interne all'Unione; l'incremento delle attività di trasformazione; il miglioramento del recupero e riciclo delle mps. Nei fatti, attualmente solo il rame ha raggiunto gli obiettivi in tutte le fasi indicate.

Un'ulteriore criticità riguarda la costruzione di rapporti di partnership con i paesi produttori, su cui, al contrario, gli Usa si sono bene strutturati. Dal 2021 a metà 2025 la Ue ha avviato partenariati strategici con 14 paesi ma con esiti contradditori, tanto che nello stesso periodo le importazioni delle mpc utili alla transizione energetica sono aumentate solo per la metà dei componenti e per l'altra metà sono calate.

Un impatto sulla fascia alta delle imprese italiane

Una situazione di carenza di mpc o un aumento del loro costo a causa di restrizioni sul mercato impatta direttamente


© Nic Wood - Pexels

sul sistema produttivo italiano. Importiamo poco più di 21 miliardi di euro di minerali critici, 18,7 dei quali sono attribuibili a specifiche filiere. Il comparto che ne beneficia di più è il manifatturiero ed estrattivo, nel quale confluiscono 11,3 miliardi di mpc e mps distribuite nei sistemi produttivi di 17 filiere e 43 settori, oltre 77 mila imprese per un fatturato di 489 miliardi di euro.

I settori più interessati sono metallurgia, siderurgia, produzione di cavi, di componenti elettronici, aeronautica e spazio, chimica; oltre al manifatturiero ne beneficiano il comparto energetico, le infrastrutture, il recupero dei materiali. Considerato che le mpc importate valgono in media appena il 3,2% dei costi d'acquisto dei prodotti finali, la loro rilevanza pesa soprattutto in quanto indispensabili e difficilmente sostituibili. C'è poi un tema di qualità delle filiere: le imprese che utilizzano le mpc hanno un livello tecnologico superiore, con il 52% che opera in settori a tecnologia alta e medio alta (35% la media del manufatturiero) e il 48% a tecnologia bassa e medio bassa (65%).

Maria Moro

Per approfondire su www.insurancetrade.it:

- *I rischi della green energy*
- *Aon, un piano per le energie rinnovabili*

INSURANCE DAILY
Direttore responsabile: Maria Rosa Alaggio alaggio@insuranceconnect.it
Editore e redazione: Insurance Connect Srl – Via Montepulciano, 21 – 20124 Milano
T: 02.36768000 email: redazione@insuranceconnect.it
Per inserzioni pubblicitarie contattare: info@insuranceconnect.it
Supplemento al 2 aprile di www.insurancetrade.it – Reg. presso Tribunale di Milano, n. 46, 27/01/2012 – ISSN 2385-2577