INSURANCE Daily

GIOVEDÌ 10 LUGLIO 2025 N. 2826

PRIMO PIANO

Il fondo di Zurich e Amundi

Zurich e Amundi lanciano il fondo Zurich Global Green Bond. Inizialmente disponibile solo per i clienti di Zurich in Italia e Germania, il fondo offrirà un accesso diversificato agli strumenti a reddito fisso, attraverso investimenti in bond di emittenti sovrani, sovranazionali e corporate, con l'obiettivo di finanziare progetti in linea con la sostenibilità ambientale: energie rinnovabili, efficienza energetica, prevenzione e controllo dell'inquinamento, gestione sostenibile dell'acqua, conservazione della biodiversità ed edilizia green. L'indicatore chiave per valutare l'impatto ambientale sarà la quantità di emissioni di gas serra limitate: almeno il 90% degli asset del fondo, spiegano Zurich e Amundi, "sarà investito in green bond dedicati, mentre i gestori potranno sfruttare anche le opportunità offerte dai social e sustainability bond". Con un approccio di gestione attiva, il fondo punterà a sovraperformare l'indice Bloomberg Msci Global Green Bond, investendo in green bond conformi ai Green Bonds Principles, che, per definizione, delimitano i progetti green idonei e stabiliscono linee guida e direttive a sostegno dell'integrità del mercato.

Il portafoglio sarà monitorato da Zurich e Amundi e si prevede la pubblicazione di un rapporto annuale sull'impatto sostenibile.

Fabrizio Aurilia

RICERCHE

L'impatto finanziario del cyber risk

Un recente report di Aon evidenzia che nel 2024 gli attacchi informatici a società quotate in Borsa hanno causato mediamente una perdita di valore del 27% degli azionisti: pesa soprattutto la crisi di fiducia e reputazione che un simile episodio può innescare. Per questo è fondamentale incrementare i presidi di sicurezza


© Sora Shimazaki - Pexels

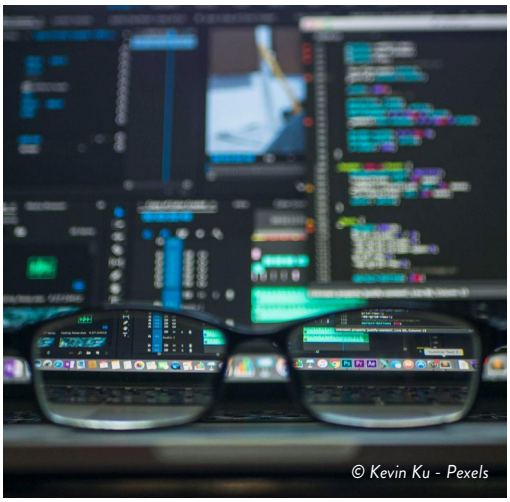
Il rischio informatico si ripercuote anche sui listini finanziari. Lo scorso anno, secondo l'ultima edizione del *Global Cyber Risk Report* di **Aon**, gli attacchi informatici a società quotate in Borsa hanno causato in media una perdita di valore del 27% per gli azionisti. Il tutto, chiaramente, senza tenere conto delle fluttuazioni che possono normalmente verificarsi nei consueti alti e bassi degli andamenti dei mercati finanziari. Nel 2023 la perdita media si era fermata al 9%, a testimonianza della crescente minaccia che il cyber risk pone ormai anche alle tasche di risparmiatori e investitori. Ecco perché, come ha osservato **Brent Rieth**, global cyber leader di Aon, "il rischio informatico non è più soltanto una questione di tecnologia: ormai è una questione anche di gestione aziendale".

Il rapporto è stato realizzato sulla base di oltre 1.400 attacchi informatici raccolti e analizzati da *Cyber Quotient Evaluation* (CyQu), una piattaforma globale di e-submission che si propone di semplificare il processo di assunzione assicurativa e di offrire alle imprese indicazioni e consigli utili per gestire la loro esposizione al rischio informatico. La dinamica messa in evidenza dalla ricerca è semplicissima e si basa sulla crescente risonanza (anche mediatica) che il fenomeno del cyber risk sta riscuotendo in tutto il mondo: un eventuale attacco informatico danneggia la reputazione dell'impresa, ne intacca il capitale immateriale, genera sfiducia sul possibile ritorno dell'investimento e finisce per tradursi in una perdita finanziaria che, come visto, può rivelarsi anche estremamente ingente.

(continua a pag. 2)

(continua da pag. 1)

"Dato che il cyber risk si fa ogni giorno più complesso e interconnesso con altre minacce, è necessario che le imprese abbiano una visione chiara della loro esposizione al rischio, un più forte allineamento fra sicurezza informatica e strategia assicurativa, e strumenti che possano consentire loro di prendere decisioni migliori e guidate dai dati a disposizione", ha aggiunto Rieth.


© Kevin Ku - Pexels

UNA QUESTIONE DI REPUTAZIONE

Stando ai dati della ricerca, sono 56 gli attacchi informatici che nel 2024 hanno attirato l'attenzione dei mass media in tutto il mondo e che si sono tradotti in una crisi reputazionale in grado di generare una perdita di valore per gli azionisti. "I danni al brand o alla reputazione rientrano nella top 10 dei rischi che le imprese di tutto il mondo si trovano oggi ad affrontare", illustra il rapporto di Aon che, a questo riguardo, cita la graduatoria stilata nell'ultima edizione della *Global Risk Management Survey* sempre del broker.

In un simile scenario, anche un solo evento catastrofico, come appunto un attacco informatico, "può indurre il mercato finanziario a rivedere le proprie proiezioni sui futuri flussi di cassa, incidendo sul valore offerto agli azionisti". Le conseguenze diventano poi estremamente dannose se l'evento non è gestito a dovere. In questo caso, prosegue il rapporto, "il danno può andare ben oltre la reputazione: la fiducia di clienti e collaboratori può finire per erodersi, con effetti a catena su vendite e valore del brand". Il rischio informatico, in pratica, non è più soltanto una minaccia circoscritta all'ambito cyber.

ATTENZIONE A MALWARE E RANSOMWARE

Sono numerosi gli episodi citati all'interno del rapporto: gli attacchi informatici dello scorso dicembre a una serie di servizi e infrastrutture critiche degli Stati Uniti, l'intrusione nei sistemi del dipartimento del Tesoro che ha dato accesso ad alcuni documenti non classificati e alle postazioni di lavoro dei dipendenti, persino un'operazione coordinata di spionaggio informatico contro almeno nove società di telecomunicazioni che, sempre negli Stati Uniti, ha consentito agli hacker autori dell'attacco di registrare e geolocalizzare le telefonate di milioni di cittadini. Bastano pochi esempi per capire che gli obiettivi e le tecniche di un cyber attack possono variare in maniera significativa fra loro. Il risultato, però, resta sempre lo stesso: se l'intrusione innesca una crisi di fiducia, allora è lecito attendersi anche una qualche perdita finanziaria.

Il rapporto, a tal proposito, si sofferma in particolare sul possibile impatto di malware e ransomware. "Sono di gran lunga la tecnica più diffusa di attacco informatico", si legge nel rapporto. E sono anche, prosegue la ricerca, "quelli che possono scatenare con maggior probabilità una crisi reputazionale": oltre il 60% dei 56 episodi citati nel report sono stati provocati da un attacco ransomware o malware. Il rapporto evidenzia che attacchi di questo genere hanno il 20% di possibilità di tradursi in un danno alla reputazione dell'impresa colpita, contro l'8%, per esempio, dei system exploit. "Nei cyber attack, come del resto in altri tipi di eventi catastrofici, c'è più possibilità di ricevere una grande risonanza mediatica quando sono in gioco questioni emotive o di interesse pubblico: gli attacchi malware e ransomware – sottolinea lo studio – rientrano in entrambe queste categorie".

QUALCHE CONSIGLIO UTILE

In un simile scenario c'è però almeno una notizia positiva: la risonanza mediatica riservata in tutto il mondo al fenomeno del cyber risk è quantomeno servita a incrementare la consapevolezza delle imprese sulla portata della minaccia. E così le società si sono mosse (e si stanno muovendo) per tentare di innalzare il livello della propria sicurezza informatica. Il rapporto evidenzia che il mercato ha registrato in un solo anno un miglioramento del 5% nei controlli critici di sicurezza informatica, ossia quelli più importanti per il settore assicurativo, con una punta dell'11% nel cosiddetto middle market.

È già qualcosa, ma non è sicuramente sufficiente per garantire la salvaguardia delle imprese contro il rischio informatico e, soprattutto, contro le eventuali crisi reputazionali e le perdite di valore finanziario che potrebbero derivare da un simile episodio. Il rapporto, nelle battute conclusive, invita dunque il mercato ad adottare strategie che possano consentire di prevenire e mitigare il rischio, anche con la consapevolezza che non tutte le minacce potranno mai essere assicurate. Il consiglio di Aon si basa su cinque punti: preparazione, leadership, proattività, comunicazione e cambiamento. "Le aziende che riescono a sfruttare bene queste leve possono mitigare la perdita di valore per gli azionisti e magari raggiungere persino un miglioramento della loro reputazione", si legge nel rapporto. "La nostra indagine del 2023 – conclude la ricerca – ha evidenziato che alcune aziende sono riuscite a superare con successo 17 dei 47 attacchi informatici presi in esame, centrando un aumento di valore del 18% per gli azionisti".

Giacomo Corvi

INSURANCE Daily

GIOVEDÌ 10 LUGLIO 2025 N. 2826

EVENTI

Come tecnologia, AI e dati cambiano l'assicurazione

Appuntamento giovedì 18 settembre a Milano per un evento speciale organizzato da Insurance Connect in collaborazione con Octo: si discuterà di come le innovazioni stanno rivoluzionando l'ecosistema della mobilità e l'offerta di servizi assicurativi

Dati, intelligenza artificiale, telematica: la tecnologia è sempre più importante nell'assicurazione motor. Forse non c'è un ambito assicurativo in cui le innovazioni tecnologiche sono così centrali sia nei processi interni sia nel business, sia nell'esperienza del cliente.

Per il settore, si tratta di trasformare le potenzialità delle innovazioni in nuovi modelli di business, di offerta e di gestione dei rischi. Underwriting e pricing, marketing e gestione sinistri: la centralità dei dati e la capacità di selezionarli e analizzarli sono veri e propri abilitatori per la competitività nell'assicurazione auto.

Se ne discuterà ampiamente con tanti ospiti, addetti ai lavori e personalità del mondo assicurativo in un evento speciale organizzato giovedì 18 settembre da **Insurance Connect** in collaborazione con **Octo**, uno dei principali provider tecnologici attivi anche nel settore assicurativo.

Il workshop, intitolato *L'assicurazione che cambia: AI, dati e tecnologia*, si terrà a Milano dalle ore 14 presso l'*Hotel Bianca Maria Palace* e sarà interamente curato e moderato da **Maria Rosa Alaggio**, direttore delle testate di Insurance Connect.

Dopo l'apertura dei lavori affidata a **Corrado Sciolla**, ceo di Octo, i momenti principali saranno due ricche tavole rotonde precedute da un keynote speech di **Matteo Carbone**, fondatore e direttore dell'*IoT Insurance Observatory*, in cui i relatori si confronteranno sui temi della mobilità, le policy e le strategie delle compagnie, la digitalizzazione del business, i prodotti e i servizi, nonché sulla relazione con il cliente.

Il primo dibattito indagherà l'ecosistema della mobilità in relazione ai prodotti e ai servizi assicurativi abilitati dall'analisi dei dati, mentre a seguire spazio al confronto sull'intelligenza artificiale, la telematica e le nuove possibilità di sviluppo dell'assicurazione motor in Italia.

In conclusione, si terrà un cocktail dove relatori e partecipanti potranno scambiarsi opinioni e pareri in un clima informale e rilassato.

Per tutte le informazioni e per registrarsi all'evento, clicca qui.

INSURANCE Daily

GIOVEDÌ 10 LUGLIO 2025 N. 2826

Insurance Daily
Direttore responsabile: Maria Rosa Alaggio alaggio@insuranceconnect.it
Editore e Redazione: Insurance Connect Srl – Via Montepulciano 21 – 20124 Milano
T: 02.36768000 **E-mail:** redazione@insuranceconnect.it
Per inserzioni pubblicitarie contattare info@insuranceconnect.it
Supplemento al 10 luglio di www.insurancetrade.it – Reg. presso Tribunale di Milano, n. 46, 27/01/2012 – ISSN 2385-2577