CYBER, UN RISCHIO COMPLESSO DA SFIDARE SU PIÙ FRONTI

di FEDERICA MARIA RITA LIVELLI,
business continuity & risk management consultant/Clusit Direttivo & Comitato Scientifico, Bci
Sig Cyber Resilience Committee, Ferma digital committee member, Enia – Comitato Scientifico

LA CYBERSECURITY SARÀ UN TEMA DI PRIMO PIANO ANCHE PER IL 2025. SI VA VERSO UN APPROCCIO SEMPRE PIÙ STRUTTURATO, CHE CONSIDERA PROBLEMI GIÀ NOTI, E COMUNQUE SEMPRE APERTI, NUOVE TENDENZE E NOVITÀ NORMATIVE FINALIZZATE ALLA SICUREZZA INFORMATICA DELLE ORGANIZZAZIONI E DEL SISTEMA SOCIALE NEL COMPLESSO. UN CONTESTO CHE COINVOLGE IL SETTORE ASSICURATIVO, CHIAMATO A DARE UN SOSTEGNO NELLA GESTIONE DEL RISCHIO E AD ATTUARE UNA RIDUZIONE DELLE BARRIERE LINGUISTICHE

Nel 2025 le sfide della cybersecurity diventeranno più complesse, a causa dell'evoluzione tecnologica e dell'aumento della connettività globale. Inoltre, le organizzazioni dovranno anche adeguarsi all'insieme di normative europee che adottano sempre più un approccio risk-based e resilience-based.
ll panorama della sicurezza informatica si sta evolvendo rapidamente, plasmato da progressi tecnologici, cambiamenti normativi e minacce emergenti. Per tenere il passo, le organizzazioni devono anticipare questi sviluppi. Per i leader e le organizzazioni della cybersecurity, restare al passo con le tendenze del settore della sicurezza informatica è fondamentale per salvaguardare le risorse e mantenere la fiducia. Di seguito alcune delle principali tendenze di cybersecurity da tenere in considerazione nel 2025.

- *Sicurezza basata sull'Intelligenza Artificiale (IA):* l'IA sarà centrale nelle strategie di difesa e attacco. La sicurezza delle applicazioni IA sarà cruciale, con investimenti in piattaforme di *threat intelligence* e soluzioni di risposta automatizzata.
- *Decentralizzazione dei diritti decisionali:* la decentralizzazione sta cambiando i modelli tradizionali di supervisione, richiedendo un approccio flessibile e una gestione distribuita del rischio.
- *Elemento umano:* il comportamento umano continua a essere un punto debole significativo. Nel 2025, le strategie di sicurezza si focalizzeranno sull'aspetto umano e sulla scienza comportamentale.
- *Carenza di talenti:* la domanda di professionisti della sicurezza informatica continuerà a crescere, rendendo cruciale attrarre e trattenere talenti qualificati.
- *Architettura Zero Trust (Zta):* la Zta continuerà a espandersi come best practice, concentrandosi sulla gestione dell'identità e degli accessi, autenticazione multifattoriale e micro-segmentazione.
- *Attacchi ransomware:* tali attacchi rimarranno una minaccia significativa, con criminali informatici sempre più organizzati. Pertanto, le organizzazioni dovranno rafforzare ulteriormente le protezioni e sviluppare strategie di risposta e di recupero.
- *Sicurezza della supply chain:* la supply chain continuerà a rappresentare un rischio significativo. Ne consegue che le organizzazioni investiranno in

strumenti di gestione dei rischi di terze parti per monitorare i fornitori.

- *Privacy e protezione dei dati:* si tratta sempre più di proteggere i dati e la privacy investendo in soluzioni di crittografia, di anonimizzazione e di mascheramento dei dati per conformarsi alle normative.
- *Sicurezza degli ambienti cyber-fisici:* la digitalizzazione e l'integrazione dei sistemi cyber-fisici aumentano i rischi. Sarà fondamentale implementare protocolli di sicurezza specializzati in grado di salvaguardare gli ambienti IT e OT.
- *Sicurezza cloud:* la migrazione verso il cloud rende la protezione degli ambienti cloud una priorità, con focus su gestione della sicurezza del cloud e sistemi di orchestrazione, automazione e risposta.

IL RUOLO DELLE NORMATIVE NELLA SICUREZZA INFORMATICA

Le normative di cybersecurity svolgono un ruolo fondamentale in un panorama sempre più dominato da minacce sofisticate e pervasive, stabilendo standard di sicurezza e responsabilizzando le organizzazioni. Nel 2025, entreranno in vigore importanti normative come Nis2, Dora, *Cyber Resilience Act* (Cra) e *AI Act*, tutte orientate a migliorare la resilienza digitale e rafforzare la sicurezza informatica. Per affrontare le sfide poste da queste normative, le organizzazioni dovrebbero: condurre la valutazione del rischio atta a identificare vulnerabilità specifiche; implementare misure di sicurezza tecniche e organizzative; sensibilizzare il personale sull'importanza della cybersecurity; fornire formazione adeguata.


© LV4260 - iStock

UNIFORMARE IL LINGUAGGIO DELL'ASSICURAZIONE CYBER

La crescente complessità del panorama digitale ha aumentato la domanda di assicurazioni cyber. Oggi il mercato offre polizze che coprono responsabilità civile, danni a sistemi, interruzioni di servizio e perdite di fatturato. Nel 2025 si prevede un aumento della domanda di assicurazioni cyber, in considerazione del fatto che sempre più organizzazioni riconoscono l'importanza di proteggere i propri asset digitali e di conformarsi a normative più rigorose. A fronte di ciò, si assisterà al proliferare di polizze cyber integrate con i servizi di cybersecurity. Inoltre, le compagnie assicurative, per essere competitive, dovranno sviluppare sempre più prodotti personalizzati allo scopo di soddisfare le esigenze specifiche dei clienti, oltre a incentivare le misure di prevenzione con sconti per chi mantiene alti standard di sicurezza.

In ogni caso, è fondamentale che le compagnie assicurative si accordino sul linguaggio tecnico da utilizzare. È inaccettabile che le coperture cyber presentino, ancora oggi, definizioni diverse tra loro. Esiste un linguaggio comune disponibile, come il *Cyber lexicon* del **Financial stability board** (Fsb), che offre definizioni consolidate e accettate dalla comunità digitale e già adottate dall'**Ivass**. Di fatto, utilizzare queste definizioni sarebbe un ottimo punto di partenza per semplificare la comunicazione con i clienti e prevenire fraintendimenti costosi sia per loro, sia per la reputazione del settore assicurativo.

VERSO UNA GESTIONE OLISTICA DEL RISCHIO

I trend di cybersecurity per il 2025 delineano un panorama in costante evoluzione, sempre più digitalizzato e soggetto a frequenti attacchi informatici, che comporta da parte delle organizzazioni lo sviluppo di un framework di cyber resilience efficace, scaturito dall'intersezione del risk management, della business continuity e della cybersecurity. Urge adottare un approccio olistico, con il risk manager che, insieme alle altre funzioni di sicurezza, usufruendo di veri e propri cruscotti intelligenti, sia in grado di gestire il rischio cyber in tempo reale, guidare l'implementazione di una cultura aziendale forte, agile e flessibile, trasformando l'incertezza in un'opportunità di crescita.