IVASS
ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI

La resilienza cibernetica del sistema finanziario italiano:

il ruolo dei test TIBER-IT

L’importanza dei test di cyber-sicurezza per il sistema assicurativo italiano

Intervento di Stefano De Polis
Segretario Generale dell’IVASS

Milano, 13 ottobre 2022

La fiducia è una componente essenziale per il buon funzionamento del mercato finanziario e assicurativo. Nel mondo digitale, fiducia significa anche un elevato livello di sicurezza informatica, resilienza agli attacchi *cyber*, tutela della riservatezza e corretto utilizzo dei dati. Tali elementi devono rientrare *by design* nella definizione dei processi e dei prodotti delle aziende.

Una recente ricerca McKinsey[1] indica che il 53% dei clienti che acquistano online lo fanno solo dopo aver verificato la reputazione del venditore specie in termini di protezione dei dati. Un cliente su 10 cambia venditore in caso di *data breach*.

Il report 2022 dell'ISACA sullo "*State of digital trust*"[2] riporta che per il 98% delle imprese intervistate la fiducia digitale è importante, ma solo per il 66% rappresenta una priorità elevata e appena il 12% dispone di personale dedicato per gestire i rischi che derivano da intrusioni e incidenti *cyber*.

Non sempre quindi alla asserita rilevanza della fiducia e della sicurezza corrisponde un reale impegno per garantirle nel continuo.

Con riferimento al mondo assicurativo, siamo consapevoli della complessità dei sistemi informatici, in cui si affiancano sistemi *legacy* e sistemi di nuova generazione dedicati ad esempio alla gestione online delle polizze dematerializzate e dei contatti con i clienti, anche con il supporto di tecnologie innovative quali intelligenza artificiale e *blockchain*.

Tale complessità, unitamente dalla diffusa esternalizzazione di funzioni e attività essenziali in ambito ICT, anche con ricorso alla tecnologia *cloud*, rende necessaria una piena conoscenza da parte dei vertici e dell'organizzazione aziendale dei livelli di sicurezza e degli ambiti di vulnerabilità all'interno delle imprese, una forte capacità di prevenzione e

[1] *McKinsey Global Survey on Digital Trust, May 2022*
[2] *State of Digital Trust 2022 - An ISACA Global Research Report; https://www.isaca.org/digital-trust/state-of-digital-trust*

processi in grado di gestire incidenti *cyber*, intrusioni nei sistemi e attacchi diretti alla sospensione dell'operatività.

La normativa assicurativa (Reg. 38 del 2018), in linea con quella bancaria, stabilisce una specifica disciplina sui sistemi informatici, la gestione dei dati e la *cyber security* aziendale, indicando requisiti di *governance*, *risk management* e *business continuity*. Le imprese assicurative sono tenute a segnalare alla Vigilanza gli incidenti informatici rilevanti.

Le norme IVASS richiedono alle imprese di valutare i rischi *cyber* ai quali sono esposte e di individuare nel Piano ICT processi di monitoraggio sistematico e presidi per prevenire e gestire gli incidenti.

Una indagine IVASS nel 2019 evidenziava che le maggiori imprese valutavano di essere in linea con i requisiti regolamentari. Quasi tutte segnalavano di avere avviato ulteriori progetti per soddisfare gli adempimenti previsti. Il governo dei sistemi informatici e della *cyber security* era ritenuto adeguato dall'83% delle imprese, con un'ampia maggioranza (90%) che aveva approvato il Piano ICT e iniziative di rafforzamento dei presidi di sicurezza.

Una nuova indagine, appena conclusa, sul grado di attuazione degli "Orientamenti EIOPA sulla sicurezza e sulla *governance* della tecnologia dell'informazione e comunicazione" emanati nel 2021, mostra che tutte le imprese assicurative hanno istituito una Funzione dedicata alla sicurezza delle informazioni, spesso esternalizzata all'interno del gruppo di appartenenza. La gran parte delle imprese dispone di meccanismi di autenticazione forte per l'accesso ai servizi. Inoltre, tutte le imprese dichiarano di aver definito un processo di gestione degli incidenti per monitorare e intervenire tempestivamente in caso di violazioni della sicurezza informatica ed *early warning* per la loro individuazione precoce.

Ciononostante negli ultimi anni sono stati segnalati dalle compagnie italiane 9 seri incidenti informatici, di cui 2 nel 2022. Gli incidenti gravi devono essere tempestivamente segnalati alle Autorità competenti, tra cui l'IVASS, anche per favorire la predisposizione di

contromisure in grado di contenere e prevenire nuovi attacchi, a livello di singola impresa e di sistema.

Indubbiamente è in atto un miglioramento dei presidi dei rischi *cyber*, con un aggiornamento costante delle conoscenze sulle minacce, vulnerabilità, incidenti e dei meccanismi di prevenzione e difesa. Rimangono tuttavia aree di criticità dovute anche all'esigenza di rodare e irrobustire le procedure implementate, specie dei processi di *governance*, di gestione degli incidenti e in generale di verifica della efficacia dei presidi.

In sede europea, l'EIOPA, su sollecitazione della Commissione, sta promuovendo un quadro comune per la segnalazione degli incidenti informatici. Inoltre, il legislatore europeo sta per emanare il regolamento DORA sulla resilienza operativa, che rafforza i requisiti sull'ICT *risk management* e la segnalazione degli incidenti e delle minacce. La norma richiederà la conduzione per i maggiori operatori di test sulla *digital operational resilience* richiamando esplicitamente la metodologia TIBER. Inoltre si stabilisce un regime di sorveglianza dei fornitori e delle terze parti critiche nell'ambito dei servizi ICT.

L'introduzione a luglio 2022 della metodologia TIBER contestualizzata al mercato italiano[3] rappresenta quindi un importante passo avanti nel dotare anche gli operatori assicurativi di strumenti per individuare le vulnerabilità, misurare i rischi e porre in essere azioni di rimedio preventive. Il contesto esterno, sempre più aggressivo e con impatti diretti sul mondo assicurativo che, va ricordato, gestisce dati in misura molto rilevante e fornisce anche protezione sui dati degli altri operatori finanziari ed economici.

La Guida nazionale TIBER-IT[4] definisce la metodologia e il modello operativo per la conduzione di test di tipo *threat-led penetration testing* (TLPT) da parte delle entità finanziarie italiane, individua le fasi in cui si articola il processo di test, definisce i ruoli, le responsabilità e le attività dei diversi attori coinvolti, inclusi i fornitori esterni e le Autorità.

[3] https://www.ivass.it/media/avviso/tiber/
[4] https://www.bancaditalia.it/compiti/sispaga-mercati/tiber-it/Guida_Nazionale_TIBER-IT.pdf

Il TIBER-IT simula potenziali attacchi reali riproducendo tattiche, tecniche e procedure di *hacker* reali, verificando così le capacità di rilevamento, protezione e risposta delle imprese sottoposte a test.

Esprimo con forza l'auspicio che le imprese assicurative nazionali, in considerazione della crescente digitalizzazione dei loro modelli di business, dei servizi forniti e delle interconnessioni informatiche con altri operatori sul mercato, siano pienamente consapevoli della necessità di condurre test avanzati sulla sicurezza *cyber*. Il TIBER-IT rappresenta la metodologia di riferimento per accrescere la resilienza cibernetica, la capacità di difesa proattiva e l'efficacia dei sistemi di protezione a seguito dell'esecuzione di test TLPT.

Ci attendiamo ora – nelle more dell'entrata in vigore del Regolamento DORA - che le compagnie, su base volontaria, mettano in atto attività di test commisurate alla rilevanza e complessità degli scenari di rischio individuali. L'IVASS seguirà da vicino l'attuazione del *framework*, collaborando con il TIBER Cyber Team Italia, con l'obiettivo di rafforzare la sicurezza dei singoli operatori e la stabilità e resilienza dell'intero mercato assicurativo.