ASSICURAZIONI & CYBER SECURITY

LA NORMATIVA COME SPINTA ALL'AZIONE

di Giuseppe Rumi, coordinatore del dipartimento di regolamentazione bancaria e assicurativa
e membro del focus team assicurazioni di BonelliErede

AUMENTO DELLA CONSAPEVOLEZZA E DELLA RESPONSABILITÀ RIGUARDO AI RISCHI TECNOLOGICI. IN UN CONTESTO IN CUI L'ATTENZIONE AL CYBER RISK NON PARE ANCORA CONSOLIDATA, POTREBBE ESSERE L'OBBLIGO DI ADEGUAMENTO, DETTATO DA GDPR, DIRETTIVA NIS E REGOLAMENTO IVASS, A SPINGERE VERSO FORME DI PREVENZIONE E PROTEZIONE ASSICURATIVA SU CUI LE COMPAGNIE, PER PRIME, DEVONO ESSERE PREPARATE

Il secondo semestre 2018 verrà probabilmente ricordato come l'anno della svolta per l'attenzione al fenomeno *cyber* nel nostro Paese.
Tre recenti fonti contribuiscono a definire una cornice normativo-regolamentare certa, che affronta una realtà composita dai contorni multiformi, foriera di minacce subdole, inesorabilmente destinata ad accrescersi esponenzialmente, alimentata dell'interconnettività e dalla globalizzazione nonché dalla facilità d'implementazione e dalla remunerativitá delle frodi cyber.
Complice una diffusa sottovalutazione del rischio e una scarsa cultura nostrana di base e, per contro, un'elevata percezione di impunità, la cognizione del rischio cyber è sinora rimasta, a livello domestico, assai acerba e le tecniche di difesa di utenti e prodotti tecnologici spesso relegate a inadeguate forme minimali.
Il divario tra la globalità della minaccia contro il provincialismo degli strumenti di difesa, tra la multiformità del fenomeno a livello tecnologico d'ingresso – caratterizzati da nomi fantasiosamente sinistri (*malicious scans, new malware, phishing, ransomware, hacking*) – e la scarsità, a oggi, di punti di riferimento normativi, ha contraddistinto sinora il fenomeno cyber, caratterizzato da una fenomenologia tecnologico-criminale sviluppatasi in modo esponenzialmente più veloce della cultura del relativo rischio, e alimentato dalla limitatezza di tecnologie di difesa idonee e dalla scarsa affidabilità di strumenti rimediali e risarcitori.
Ciò è destinato a cambiare grazie a due fonti comunitarie rilevanti, quali il regolamento *Gdpr* (General data protection regulation) 2016/679 e la direttiva *Nis* (Network and information security) 2016/1148, implementata con d. Lgs. n.65 del 18 maggio 2018. Inoltre, il settore assicurativo domestico si pone oggi all'avanguardia nel fronteggiare i rischi cyber con il recente *Regolamento Ivass* n. 38 del 3 luglio 2018. Rimandando al diluvio di scritti già editi in materia di Gdpr, mi soffermerò brevemente sulle due ultime citate fonti normativo-regolamentari.

LA NORMATIVA NIS

L'obiettivo della direttiva è incrementare la resilienza delle infrastrutture critiche al cyber-risk facendo leva sulla condivisione delle informazioni e imponendo alle imprese destinatarie (i cosiddetti fornitori di servizi essenziali operanti nei settori ritenuti critici e i fornitori di servizi digitali) l'adozione di misure tecniche e organizzative adeguate alla gestione del cyber risk e la tempestiva notifica, alle autorità competenti, degli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali.
Nell'implementare la direttiva, il legislatore italiano è stato ispirato da un criterio di gradualità, non imponendo obblighi ulteriori rispetto a quelli della direttiva, né estendendo il perimetro dei soggetti destinatari. Inoltre, le sanzioni (da 12 mila a 125 mila euro) si collocano ben al di sotto di quelle previste dal Gdpr, che arrivano fino a 10 milioni di euro o al 2% del fatturato annuo globale.

L'INTERVENTO DEL REGOLATORE

Il nuovo Regolamento Ivass n. 38/2018 sul governo societario dispone, per la prima volta, l'obbligo esplicito per le imprese di tutelare la "cyber-security aziendale", definita come la situazione in cui gli *information*

assets dell'impresa (tra cui hardware, software, dati e utenti) risultino protetti rispetto a eventi (volontari o accidentali) che compromettano l'integrità dei dati ovvero il corretto funzionamento della rete e dei sistemi informativi[1].

Sebbene la scelta delle modalità concrete con le quali tutelare la cyber-security sia rimessa all'autonomia delle imprese, il Regolamento 38/2018 fornisce alcune indicazioni, prevedendo[2] in primo luogo la conformità del piano strategico Ict agli standard e linee guida nazionali e internazionali; poi la valutazione del cyber risk connesso alle varie funzioni, attività, prodotti e servizi anche in relazione alle attività svolte da terze parti, che recano rischi di contagio su tutta la filiera produttiva; e l'implementazione di un sistema di monitoraggio sistematico per identificare tempestivamente gli incidenti e valutare la resilienza al cyber risk, anche mediante *penetration test*, audit ed esercizi di simulazione.

Per quanto riguarda gli *incidenti informatici*, si impone alle imprese lo sviluppo di sistemi di risposta tempestivi ed efficaci, soprattutto in ottica di continuità operativa, e l'obbligo di immediata notifica all'Ivass di incidenti di sicurezza informatica gravi[3].

Ove poi l'incidente riguardi anche la violazione di dati personali, si pone un tema di coordinamento tra gli obblighi di notifica imposti dal Gdpr e quelli previsti dal Regolamento 38/2018, con una duplicazione degli oneri informativi anche al *Garante della privacy* in modo coordinato e tempestivo dal momento in cui l'impresa è venuta a conoscenza dell'evento[4].

UNO STIMOLO PER IL MERCATO ASSICURATIVO

Dati recenti riferiti al 2017 suffragano l'attualità del fenomeno cyber sia a livello globale, con gli attacchi informatici verso le aziende che sono raddoppiati nell'arco di cinque anni, generando costi nell'ordine di 600 miliardi di dollari, pari allo 0,8% del Pil globale; sia in Italia, dove 16 milioni di utenti della rete hanno subito attacchi informatici, con perdite economiche per 3,5 miliardi di euro.

In questo quadro, le richiamate novità normative fungeranno da stimolo su un mercato caratterizzato da previsioni di crescita elevate, e da un ridotto posizionamento che ha origini lontane e cause variegate.

Quali destinatarie dei nuovi requisiti **Ivass**, le compagnie sono chiamate ad adeguarsi entro fine del prossimo anno, una volta esaurite le numerose e complesse attività preparatorie, quali: (i) l'individuazione degli *information assets* cruciali per l'azienda; (ii) valutazioni delle misure e politiche di sicurezza esistenti; e (iii) *gap analysis* per individuare le fragilità di sistema, anche tramite appositi test di penetrabilità.

Dal punto di vista commerciale, la direttiva Nis si presenta come occasione importante di ripensamento delle polizze specifiche a copertura del cyber risk già in essere, e nella formulazione di nuovi prodotti.

Negli Stati Uniti, i premi relativi alla *cyber insurance* sono cresciuti in un anno del 37%, raggiungendo 1,84 miliardi di dollari nel 2017 ed elevati tassi di penetrazione di mercato (superiore al 75%) per le imprese dei settori finanziario, sanitario e *retail* con fatturati superiori al miliardo di dollari.

Anche considerando le raccomandazioni dei regolatori nazionali e sovranazionali, è giusto aspettarsi un nuovo boom nel settore anche in Italia, secondo un dato di crescita che a livello globale si prevede raggiunga, nel 2020, i 7,5 miliardi di dollari di vendite annuali, triplicando il dato del 2015, e superare i 20 miliardi nel 2025.

La definizione di polizze adeguate dovrà tenere conto di una pluralità di aree di attenzione, tra cui la straordinaria rapidità dell'innovazione tecnologica e corrispondente necessità di sistemi e procedure flessibili, le opportunità e i rischi legati agli *outsourcer* e la rapida evoluzione delle regolamentazioni di dettaglio e delle *best practice* legali.

1. *Cfr. art. 2, comma 1, lett. f), Regolamento 38/2018.*
2. *Cfr. art. 16, Regolamento 38/2018, che descrive i contenuti minimi del piano strategico sulla Ict, che deve essere approvato dall'organo amministrativo.*
3. *Tale obbligo di notifica costituisce una delle declinazioni dell'obbligo, più generico, di comunicazione immediata all'Ivass di "ogni evento che possa ragionevolmente comportare, o abbia già comportato cambiamenti sostanziali dell'attività e dei risultati del sistema di governance, del profilo di rischio o della condizione finanziaria e di solvibilità dell'impresa" (cfr. art. 32 del Regolamento Ivass n. 33/2016).*
4. *Cfr. Relazione al Regolamento 38/2018.*