IVASS
ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI

SERVIZIO VIGILANZA INTERMEDIARI
DIVISIONE VIGILANZA INTERMEDIARI

Rifer. a nota n. *del*

Classificazione XIII 2 1
All.ti n .

Agli Intermediari assicurativi e riassicurativi iscritti nel Registro Unico degli Intermediari tenuto dall'IVASS

Agli intermediari dell'Unione Europea di cui all'elenco annesso al RUI

e p.c.

Alle imprese di assicurazione con sede legale in Italia

Alle Rappresentanze per l'Italia di imprese di assicurazione con sede legale in uno Stato terzo rispetto allo Spazio Economico Europeo

Alle imprese di assicurazione con sede legale in un altro Stato membro dello Spazio Economico Europeo che esercitano l'attività in Italia in regime di stabilimento o di libera di prestazione di servizi

LORO SEDI

Oggetto Esiti dell'indagine conoscitiva sui presidi degli intermediari tradizionali per la gestione delle informazioni e la prevenzione dei rischi informatici.
Indicazioni per gli intermediari.

Si fa riferimento all'indagine avviata dall'Istituto il 25 luglio 2017 per conoscere il livello di consapevolezza degli intermediari tradizionali con riguardo ai rischi insiti nell'uso di nuove tecnologie e di sistemi informatici sempre più sofisticati, i presidi di prevenzione e protezione adottati e individuare le azioni utili ad accrescere la "*cyber security* aziendale" [1].

L'iniziativa si è avvalsa della collaborazione delle principali Associazioni di categoria degli intermediari alle quali è stato chiesto di diffondere un questionario predisposto dall'IVASS ad un campione sufficientemente rappresentativo di iscritti.

[1] Il DPCM 17/02/2017 "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali" definisce la sicurezza cibernetica come *"condizione per la quale lo spazio cibernetico risulti protetto grazie all'adozione di idonee misure di sicurezza fisica, logica e procedurale rispetto ad eventi, di natura volontaria o accidentale, consistenti nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittima, ovvero nel controllo indebito, danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi";* definisce inoltre lo spazio cibernetico come *"l'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti, nonché delle relazioni logiche, comunque stabilite, tra di essi".*

Nel seguito si illustrano i principali esiti dell'indagine e si forniscono indicazioni di carattere generale sulle possibili azioni da intraprendere per elevare il livello di presidio dei rischi informatici e di protezione dei dati e delle informazioni.

1. Esiti dell'indagine.

Il campione di intermediari che hanno partecipato all'indagine (circa 3.000 tra Agenti e Broker) ha dimostrato, complessivamente, un discreto livello di consapevolezza dell'esistenza del rischio informatico e della necessità di protezione dei dati e delle informazioni della clientela.

Del pari avvertita è l'esigenza di informare dipendenti e collaboratori sulle problematiche inerenti i rischi informatici al fine di:

- ✓ promuovere comportamenti corretti sotto il profilo della raccolta, gestione e conservazione dei dati;
- ✓ accrescere il livello di sensibilità e percezione del *cyber risk* e delle sue implicazioni.

Le risposte ai singoli quesiti dell'indagine hanno fornito indicazioni sulla tipologia delle misure di prevenzione del rischio *cyber* attualmente adottate dagli intermediari.

Ne è scaturito un quadro incoraggiante sul fronte dei presidi e dei processi di acquisizione e protezione dei dati, configurazione e protezione dei sistemi, conservazione delle informazioni. Infatti oltre l'80% dei partecipanti all'indagine:

- ✓ adotta sistemi di protezione dei dati attraverso il ricorso a password alfanumeriche;
- ✓ raccoglie soltanto i dati indispensabili allo svolgimento dell'attività;
- ✓ assegna ai propri collaboratori utenze personali non condivisibili con altri utenti;
- ✓ utilizza sistemi e reti protetti da accessi non autorizzati;
- ✓ effettua periodici *backup* dei dati;
- ✓ affida la configurazione di sistemi e dispositivi a personale esperto.

Il risultato dell'indagine si presenta meno incoraggiante per quanto riguarda il grado di percezione dell'importanza di effettuare monitoraggi periodici dei propri sistemi al fine di intercettare eventuali *malware* e accessi non autorizzati. L'analisi delle risposte mostra che il 78% del campione riferito al canale agenziale e il 50% del campione dei broker non dispone di sistemi di monitoraggio per la rilevazione di accessi non autorizzati.

Una riflessione si impone anche in relazione alla diffusa mancanza di una *policy* di gestione del rischio informatico formalizzata in un documento scritto e alla scarsa frequenza dei test anti intrusione. Su tali aspetti, le risposte positive non hanno superato la soglia del 20%. Anche il campione dei grandi broker[2], con percentuali che si attestano al 50%, esprime nel complesso un livello di presidio appena sufficiente, in considerazione delle caratteristiche dimensionali e del conseguente numero di dati trattati.

Emerge un'esiguità delle iniziative formative, effettuate dal 23% degli agenti e dal 30% dei broker (il dato raggiunge l'80% solo per i grandi broker), che è indice di una parziale sottovalutazione del fattore umano come elemento chiave per prevenire gli attacchi. A ciò si aggiunge che soltanto la metà degli agenti intervistati e il 60% dei broker ha informato i propri collaboratori sulle modalità da seguire per prevenire il rischio *cyber*.

Migliorabile è, inoltre, il dato sull'adozione di sistemi e modelli di analisi dei rischi, riguardo ai quali le risposte positive si attestano al 40% per il campione degli agenti ed al 50% per quello dei broker; mentre la percentuale sale al 90% per il solo campione dei grandi broker.

Ancora limitata - avendo risposto positivamente il 30% degli agenti, il 50% dei broker ed il 70% dei grandi broker - è l'attenzione alle tematiche riguardanti il Regolamento europeo n. 2016/679 in materia di protezione dei dati personali, che diventerà definitivamente applicabile in via diretta in tutti i Paesi UE dal 25 maggio 2018.

Risultano del tutto marginali i casi in cui si è fatto ricorso ad una copertura assicurativa a protezione del rischio informatico e delle perdite di dati conseguenti ad un attacco. Solo il 10% degli agenti intervistati dichiara di aver stipulato una polizza assicurativa, percentuale che sale al 12% per il campione broker. Un maggiore utilizzo dello strumento assicurativo si è riscontrato da parte dei grandi broker, con una percentuale del 40% del campione.

Il 15% degli intervistati ha ammesso di aver subito almeno un attacco *cyber*, percentuale che sale al 50% per i grandi broker. Se si considera che molti operatori, non disponendo di idonei sistemi di monitoraggio, potrebbero non essere in grado di accorgersi di aver subito attacchi (anche in forma di sottrazione dei dati), il dato rivela una notevole criticità, soprattutto se associato

[2] Per grandi broker ai fini dell'indagine si è fatto riferimento ai broker con un livello di provvigioni superiori a 2, 2 milioni di euro annui.

alla circostanza - del pari emersa dall'indagine - che il 30% degli agenti, il 15% dei broker e il 20% dei grandi broker del campione hanno risposto che non riuscirebbero in caso di attacco a ripristinare integralmente i sistemi ed a recuperare tutti i dati e le informazioni.

2. Indicazioni per gli intermediari.

L'indagine ha evidenziato margini di miglioramento sensibili nel grado di consapevolezza e nel conseguente livello di presidio dei rischi *cyber* da parte degli intermediari tradizionali.

Gli strumenti e le soluzioni operative adottate per la mitigazione del rischio necessitano di essere implementati nella duplice direttrice della prevenzione e della protezione.

A tal fine l'IVASS si attende che gli operatori si attengano alle indicazioni riportate di seguito, individuando gli opportuni interventi e le iniziative di potenziamento dei propri presidi, commisurati al proprio livello di esposizione al rischio, nell'ambito di un processo di autovalutazione e autocorrezione.

Sul piano della prevenzione l'Istituto raccomanda che gli intermediari si dotino di specifiche policy sul *cyber risk*, che potranno essere individuate anche sulla base di linee guida definite con le rispettive Associazioni di categoria.

E' opportuno che tali *policy*:

- ✓ siano redatte all'esito di un *assessment* approfondito dei processi e dei sistemi informatici in uso;
- ✓ individuino le misure idonee ad accrescere la *cyber security* aziendale;
- ✓ siano condivise con i propri collaboratori e dipendenti;
- ✓ siano sottoposte a revisione con cadenza almeno biennale; in ogni caso, in presenza di modifiche normative o per adeguarsi all'evolversi della tecnologia e ogni qual volta si verifichino "incidenti informatici" che comportino l'inaccessibilità, anche temporanea, ai dati e alle informazioni o la loro perdita anche parziale;
- ✓ abbiano contenuti e livelli di dettaglio commisurati alla complessità dell'attività aziendale e al grado di esposizione al rischio.

E' parimenti opportuno che sia verificata, almeno semestralmente ed anche con l'eventuale ricorso a consulenti esterni, la conformità dell'operatività aziendale alle previsioni contenute nella politica adottata.

Fondamentale, sempre sul piano della prevenzione, sarà l'accrescimento delle conoscenze informatiche degli intermediari stessi e dei collaboratori e dipendenti. A tal fine l'istituto si attende che una quota del 20% del monte ore di formazione biennale obbligatoria per l'aggiornamento professionale, ex articolo 7 del Regolamento IVASS n. 6 del 2 dicembre 2014, sia dedicata, a partire dal 2018, ai temi della sicurezza informatica.

Per quanto riguarda la protezione, al fine di offrire un adeguato livello di resilienza contro gli attacchi informatici, si raccomanda di innalzare la sicurezza dei sistemi utilizzati (configurazione dei sistemi, accessi protetti, ecc.), aumentare la frequenza dei *backup* dei dati (almeno giornaliera), incrementare i sistemi di monitoraggio e il ricorso ai test antintrusione, prevedere un piano di gestione di eventuali crisi.

Considerato inoltre che il rischio *cyber*, per sua natura, è un rischio in continua evoluzione che espone a crescenti minacce, si raccomanda un aggiornamento costante nell'analisi delle vulnerabilità aziendali e nella identificazione di elementi potenzialmente oggetto di attacchi o di tentativi di intrusione.

L'adesione alle raccomandazioni indicate è ritenuta fondamentale per la mitigazione del rischio *cyber*. Al contempo, nella consapevolezza che lo stesso può essere attenuato ma non annullato, permanendo comunque un rischio residuo, si auspica un ampliamento del ricorso allo strumento assicurativo, complementare al sistema dei presidi in essere. Tale ricorso è correlato allo sviluppo di uno specifico segmento di offerta assicurativa da parte delle compagnie.

Nell'individuazione delle concrete misure da adottare per un auto-potenziamento dei propri presidi - in un'ottica di proporzionalità tenuto conto della natura, delle dimensioni e della complessità dell'attività svolta (in relazione al portafoglio, alla struttura aziendale, alla quantità di dati trattati) - gli intermediari potranno valutare di avvalersi del supporto di iniziative e strumenti predisposti dalle Associazioni di categoria e posti a disposizione degli associati.

L'Istituto, entro il 2019, ripeterà l'indagine per valutare il grado di adesione alle misure suggerite e per misurare il livello di evoluzione del settore in materia di sicurezza informatica e di resilienza agli attacchi informatici.

Distinti saluti.

Per il Direttorio Integrato
Il Presidente

Firmato digitalmente da
SALVATORE ROSSI