COME FUNZIONA L'ASSICURAZIONE PER LA CYBER-SECURITY

Si dimostra sempre più vivo ed in crescita il complesso ecosistema che si articola intorno alla cyber-security. Il virus della consapevolezza del rischio informatico è di quelli che dovrebbero diffondersi senza barriere perché le aziende, anche quelle italiane, hanno solo da guadagnare dallo sviluppo di cultura e sensibilità sul tema.

ECONOMIA E CYBERSPAZIO

Il recente rapporto sul framework nazionale di cyber-security [http://formiche.net/2016/02/08/cyber-security-framework-nazionale-sapienza-cis-cini/] tratta ampiamente il tema della sicurezza informatica, non dal punto di vista tecnologico, bensì come metodologia per rispondere in modo strutturato alla sfida. L'economia di una nazione non si sviluppa solo nei domini terra, mare, cielo ma sempre più nel cyberspazio ed esso va protetto anche grazie alle azioni messe in campo da ogni singola azienda.

IL MERCATO SI STA MUOVENDO

La sicurezza assoluta non esiste perché il cyber è un universo in continua e rapida evoluzione, però è fondamentale raggiungere almeno una soglia minima di sicurezza che potrà essere progressivamente migliorata. L'azienda deve avere la maturità di individuare il livello di sicurezza che può raggiungere con maggiore convenienza e trasferire al mercato assicurativo il rischio residuo. Le polizza cyber-risk esistono già da alcuni anni ma da inizio 2016 c'è un forte incremento della richiesta come conferma MARCO VINCENZI, Responsabile Financial Lines di ALLIANZ GCS in Italia: "*abbiamo ricevuto più richieste di polizze cyber nel mese di gennaio 2016 che in tutto l'anno 2015, questo è un segnale che effettivamente qualcosa si sta muovendo.*"

LA POLIZZA È PARTE DI UN PERCORSO

Le aziende devono attivare un percorso integrato di gestione del rischio ed includere l'ambito cyber. La copertura assicurativa di tali rischi è infatti l'ultimo tassello di un processo strutturato, che parte con l'analisi della realtà specifica dell'azienda: tipo di business che conduce, tipo di attività che implementa, mercato di riferimento, fino alle caratteristiche dell'infrastruttura tecnologica.

COME SI PROCEDE

Ai fini dell'implementazione di una copertura assicurativa cyber-risk, l'azienda dovrebbe seguire un percorso che parte sicuramente con un'analisi interna che quantifica e qualifica la propria esposizione. Isolare il massimo danno probabile valutando i danni derivanti da eventi come: furto di dati sensibili di terzi, interruzione di attività per blocco dei sistemi, danno di immagine, frode finanziaria, etc. Questa analisi deve essere effettuata attraverso il lavoro congiunto di tutti i dipartimenti aziendali non solo quelli IT e Risk. Un'opzione è anche valutare il coinvolgimento di un consulente assicurativo perché questo settore non ha ancora standard di riferimento e bisogna trasferire informazioni corrette alla compagnia assicurativa come sottolinea MARCO VINCENZI di ALLIANZ GCS: "*Quando ci spostiamo sull'orbita cyber dobbiamo dimenticarci tutto quello che è l'approccio al business tradizionale anche da parte dell'assicuratore. Il cliente deve essere disponibile a indicarci le soluzioni adottate per proteggersi dal rischio cyber*".

QUESTIONARI VALUTATIVI

Le compagnia assicurative richiedono la compilazione di un questionario valutativo che ha scopo di evidenziare le informazioni necessarie per una prima valutazione del rischio. L'azienda in questa fase deve avere coscienza di quelli che sono i suoi punti di forza e di debolezza. Si raccoglie un primo insieme di informazioni e si ottiene un intervallo di premio assicurativo che potrà poi essere raffinato con il prosieguo della trattiva. Gli argomenti trattati nei questionari valutativi sono tanti e cambiano per ogni compagnia, sono essi stessi **un indicatore della complessità del tema che necessità di una normalizzazione**. Abbiamo chiesto a MARCO VINCENZI di ALLIANZ GCS, se da questo punto di vista, la metodologia del framework nazionale possa essere di supporto: "*Questo strumento ci aiuta, perché crea delle linee guida verso una standardizzazione. Avere delle direttive che portano ad uno standard, sicuramente aiuta il mercato stesso a capire quali sono le necessità, orienta i clienti e allinea gli assicuratori in modo tale che si possano fare paragoni tra le coperture, permettendo al cliente di decidere più agevolmente a chi affidarsi".*

COSA SI CHIEDE

All'azienda viene chiesto di fare un attento esame della propria cyber-postura e questo percorso tocca sempre almeno questi punti: quanti dati sensibili maneggia, le policy di protezione dei dati, la geolocalizzazione delle sedi, sistemi firewall e antivirus, monitoraggio

delle intrusioni, transazioni con carte di credito, gestione della privacy, utilizzo della crittografia, strategie di backup, accesso fisico ai sistemi, accesso da remoto, outsourcing di servizi informatici, esposizione sui social network, strategie di business continuity. Sono tutti temi che devono entrare nel linguaggio aziendale, passo dopo passo **la cyber-security deve uscire dai confini dei dipartimenti IT ed entrare nel DNA dell'azienda**.

COSA COPRE

Secondo il rapporto annuale dell'ALLIANZ RISK BAROMETER 2016 [http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf] , il cyber-risk è al terzo posto tra i cinque rischi più temuti a livello internazionale ed era già al quinto posto nel 2015. Recenti ricerche [https://www.rims.org/RiskKnowledge/RISKKnowledgeDocs/RIMS_CyberSurvey_May2015_final_6152015_135443.pdf] mettono in evidenza che un danno ai dati viene considerato più pericoloso in termini di reputazione rispetto a un danno materiale ai beni. Una polizza cyber può coprire sia i danni propri: interruzione di attività, proprietà intellettuale, ripristino dei sistemi; sia i danni a terzi: violazione privacy, perdita profitto, frode finanziaria; ma anche i costi per la difesa legale, ripristino reputazione ed altro. Bisogna fare attenzione ad un aspetto importante: **le aziende possono impiegare mesi per capire di essere state vittime di un attacco**, in questo caso MARCO VINCENZI di ALLIANZ GCS ci spiega come funziona: "*Le polizze operano nel regime di claims made, il che vuol dire che fa fede la data di richiesta del risarcimento e non quella del danno procurato. Anche nel caso del cyber la richiesta del danno può avvenire mesi dopo rispetto a quando l'atto dannoso è stato commesso*". Attenzione inoltre ai **virus informatici che prendono in ostaggio i file del computer attraverso tecniche di crittografia e chiedono un riscatto in denaro per riavere i propri file**. In Italia ci sono delle problematiche legislative, perché secondo la giurisprudenza del nostro paese non si può garantire in via assicurativa questo tipo di copertura.

QUANTO COSTA UNA POLIZZA

La polizza assicurativa per i rischi informatici varia sicuramente in base alla cyber-postura dell'azienda ma è ovviamente anche funzione di parametri classici come fatturato e limite di indennizzo. Abbiamo provato ad effettuare qualche simulazione con un'azienda di piccole dimensioni ed una buona maturità dal punto di vista della sicurezza informatica: con un limite di indennizzo di 500.000 euro ed un fatturato fino a due milioni di euro, il premio

richiesto è circa 1.000 euro. Attenzione però senza un lavoro preventivo di strutturazione non si arriva alla stipula di una polizza cyber.

CHI SI ASSICURA

Il beneficio finale che le aziende possono trarre da questo tipo di copertura risiede fondamentalmente nella tutela finanziaria del bilancio d'impresa. Le dimensioni delle azienda che oggi chiedo una polizza cyber-risk è ben diversa come sottolinea MARCO VINCENZI di ALLIANZ GCS: "*Oggi le richieste che stiamo ricevendo provengono da aziende molto grandi, con esposizione all'estero. Parliamo di aziende con fatturato di diversi milioni di euro, ma sono fermamente convinto che una volta che si esaurirà questo flusso di grandi aziende* ***anche quelle midsize inizieranno veramente a prendere coscienza dei propri rischi, soprattutto se fanno parte dell'indotto e della supply-chain delle grandi aziende****. La grande azienda inizia col proteggersi, ma poi comincerà a chiedere che anche il fornitore sia protetto, in un certo modo ci sarà un passaggio in cascata.*"

INTERVISTA COMPLETA

Per approfondire l'argomento è disponibile l'intervista completa rilasciata a Formiche da MARCO VINCENZI, Responsabile Financial Lines di ALLIANZ GCS Italia.

FABIO DE PAOLIS

Fabio De Paolis è esperto in sicurezza informatica con oltre 20 anni di attività nel settore. E' laureato in Sicurezza dei Sistemi e delle Reti Informatiche presso l'Università di Milano; è CERTIFIED ETHICAL HACKER presso EC COUNCIL di Londra; è CHIEF INFORMATION SECURITY OFFICER in un'azienda italiana che offre servizi di ingegneria del software e sicurezza informatica; è consulente di enti ed organizzazioni private per individuare ed esaminare minacce informatiche; si interessa di cyber-security e cyber-warfare con particolare attenzione al mondo dell'intelligence; è attivo sulla Rete da quando la posta elettronica si scambiava solo fra BBS tramite modem analogico.