DATA PROTECTION, VANTAGGI E LIMITI DELLA POLIZZA

di FABRIZIO AURILIA

PRIMA DI PENSARE AL CONTRATTO ASSICURATIVO, CHE NON È CERTO LA PANACEA, UN'AZIENDA CHE HA A CUORE LA PROPRIA SICUREZZA INFORMATICA DOVREBBE ASSICURARSI DI AVER ALMENO ASSOLTO AI REQUISITI MINIMI DI GESTIONE DEL RISCHIO CYBER. COME SPIEGA ELENA VACIAGO, ASSOCIATE RESEARCH MANAGER DI INNOVATION GROUP

Sicurezza informatica e tutela della privacy online non sono sinonimi. Sono come due insiemi che solo in certi punti si sovrappongono. La tutela della privacy è regolata da norme e presidii legali, mentre la sicurezza informatica, che presenta problematiche soprattutto di tipo tecnico, è gestita da ingegneri che devono assicurare il corretto funzionamento di sistemi, applicazioni ecc.
Elena Vaciago, associate research manager di **Innovation Group**, sostiene che i due insiemi si sovrappongono quando si parla di aspetti di *data protection*, soprattutto quando ci sono in ballo i dati personali che, oggi, sono tantissimi e di svariate categorie: "il *Gdpr* – sottolinea – ha molto ampliato il concetto di dato personale, in cui ormai rientra anche il tracciamento di navigazione sul web, per esempio. Qualsiasi informazione che possa aiutare a identificare un utente è da considerare dato personale".

LA DOPPIA ESTORSIONE

Tra gli attacchi più diffusi che mettono a repentaglio sia la sicurezza informatica sia la privacy ci sono certamente i ramsonware. Nati come mirate richieste di riscatto nei confronti di un'azienda i cui dati erano stati crittografati, oggi hanno fatto un salto di qualità. "Gli hacker – spiega Vaciago – attuano una doppia estorsione che consiste prima nella crittografia dei dati aziendali e poi nella minaccia di pubblicazione o la rivendita online degli stessi. Questo meccanismo crea evidentemente un doppio problema all'azienda colpita: uno di natura strettamente di business, causandone un'interruzione, e uno di gestione della privacy, con conseguenze immaginabili a livello reputazionale e normativo. La diffusione delle informazioni dei clienti, per esempio, è un illecito per il quale sono previste sanzioni anche molto elevate".
Ormai la gran parte degli attacchi punta proprio a rubare i dati per poi rivenderli ad altri cyber criminali che a loro volta li sfruttano per altri attacchi, secondo uno schema difficilmente arrestabile.

ALMENO LE BASI

In questo contesto, cosa può fare concretamente una polizza cyber contro un attacco di questo tipo? Le compagnie che si pongono il problema di assicurare questi grandi rischi partono sempre da un *assessment*, cioè un'analisi, una valutazione preliminare, fa notare Vaciago. "I rischi informatici – ricorda – sono strettamente legati alla singola realtà: è difficile valutarli in modo standard, occorre fare un assessment completo sul valore dei dati da assicurare, ma anche sulle misure di sicurezza già in essere. Possono essere gli stessi assicuratori,

eventualmente, a segnalare le misure di sicurezza che occorrono all'azienda da assicurare, per poi sottoscrivere la polizza".
Nel momento in cui si procede con l'assessment, è l'assicuratore che si sincera che siano state messe in campo tutte le misure preventive per la protezione dei dati, della rete, degli accessi, cioè tutti i fondamentali della sicurezza informatica. "Sono misure base – commenta Vaciago – note da molti anni a chiunque lavori nel mondo dell'Ict: non c'è bisogno di essere un esperto di sicurezza informatica per conoscerle".

COSTI DIFFICILMENTE SOSTENIBILI

Chi assicura un'azienda, quindi, lo fa solo dopo una verifica dei fondamentali di sicurezza informatica. Tuttavia ci sono ancora molte realtà che non li hanno pienamente adottati. Ma non basta, perché è anche probabile che un assicuratore chieda all'azienda da assicurare altre misure per proteggere dati particolari: per esempio, potrebbe essere necessari monitoraggi costanti per verificare eventuali anomalie negli accessi, oppure strumenti in grado di arrestare un attacco cyber già nelle prime fasi.
La possibilità di essere attaccati è molto alta: la probabilità di subire un attacco informatico è intorno al 20%, mentre quella che si verifichi un incendio è al 2%.
È in base al settore nel quale opera l'azienda e al suo livello di criticità, definito anche dallo storico degli attacchi pregressi e da statistiche utili a soppesare il rischio, che dipende la possibilità di avere una copertura e di che tipo e livello di garanzia. "Se si guardano i grandi sinistri internazionali di cyber risk – rileva la manager – ci si accorge che, pur aumentando il numero di aziende che si dotano della polizza, i risarcimenti non hanno quasi mai coperto l'intero danno, perché i costi di un *data breach* sono spesso molto alti e il mercato assicurativo non è ancora disponibile a prenderseli in carico totalmente".

TRA GESTIONE DEL RISCHIO E REQUISITI MINIMI

Per prevenire il rischio informatico esistono misure minime considerate fondamentali. Accade spesso, però, che le aziende se le dimentichino. Un tempo, la legge italiana sulla privacy aveva prodotto un documento che le elencava tutte. Il Gdpr però ha eliminato il concetto di requisiti minimi e ha fatto discendere tutto dall'analisi del rischio. "Il problema – spiega Elena Vaciago, associate research manager di Innovation Group – è che la cultura della gestione del rischio non è ancora molto diffusa, perché presuppone una formazione specialistica, e anche una certa visione, che in tante piccole e medie realtà imprenditoriali italiane non c'è ancora". Se è indubbiamente più corretto un approccio che si basi sull'analisi del rischio, anche pensare a una sorta di *checklist* di misure minime potrebbe aiutare a far sviluppare proprio questa cultura della prevenzione. Ecco perché, suggerisce Vaciago, un elenco di questo tipo andrebbe reintrodotto.

LA DIPENDENZA DAL DIGITALE

Tra le misure volte ad aumentare la sicurezza, ci sono la formazione delle persone, l'uso del cloud e più in generale tutto ciò che contribuisce a costruire una più solida cultura del rischio.
Negli ultimi mesi, conferma Vaciago, c'è stata una presa di coscienza più convinta presso le aziende, anche legata a una maggiore dipendenza dal digitale. "Eppure – conclude – alcune piccole e micro imprese, durante i mesi del lockdown, hanno dovuto far affidamento sui computer casalinghi dei dipendenti i quali, in certi casi, hanno portato a casa i pc aziendali".
Una polizza cyber, purtroppo, non risolve da sola il problema della sicurezza informatica, ma può aiutare l'azienda colpita a ripartire, soprattutto se nel contratto è previsto l'intervento di una società di ripristino per la gestione del post-sinistro, un'azienda specializzata che stabilisca un piano per la ripartenza. Ci sono imprese che restano ferme settimane e altre che ripartono subito: questo può fare la differenza.