IL CYBER CRIME È SOLO UNA PARTE DEL RISCHIO

di MARIA MORO

IL RISCHIO DI INTRUSIONE NEI PROPRI SISTEMI DIGITALI E DI FURTO DEI DATI PREOCCUPA MOLTISSIMO LE IMPRESE. LA "VISIBILITÀ" DI SIMILI EVENTI PUÒ PERÒ METTERE IN SECONDO PIANO ALTRE MINACCE INFORMATICHE, ALLE QUALI L'AZIENDA POTREBBE ESSERE MAGGIORMENTE ESPOSTA IN TERMINI DI IMPATTO SUL BUSINESS. DA QUI LA NECESSITÀ DI UN RISK ASSESSMENT CORRETTAMENTE CONTESTUALIZZATO

Il rischio cyber è una minaccia concreta ma non è uguale per tutti, perché ogni impresa è esposta in modo diverso.

Quando si parla di *cybercrime* ci si focalizza su un fenomeno noto e in continua crescita, ma che riguarda solo alcuni aspetti del più ampio rischio tecnologico che minaccia le aziende, cioè la possibilità che un'entità esterna penetri nel sistema informatico di un'organizzazione con fini criminali di spionaggio, boicottaggio o estorsione. Il tema è degno della massima attenzione, ma non è l'unico aspetto, e spesso neppure il principale, che un risk manager deve considerare per tutelare l'infrastruttura tecnologica della propria azienda.

La vecchia immagine del settore IT che opera come un silos, in maniera indipendente dagli altri comparti aziendali, è stata superata nel tempo mano a mano che le potenzialità dell'informatica si sono sviluppate e che dai software installati sui singoli pc si è passati a sistemi in rete complessi, alla digitalizzazione di molte operazioni, al *cloud*. Nel contesto attuale, la tecnologia IT è un servizio strutturale e pervasivo, spina dorsale operativa di tutti i settori, che riceve da questi degli *input* per trasformarli in *output* corrispondenti alle singole e differenti esigenze. In questo senso, secondo **Marco Avanzi**, socio **Anra** e risk e compliance manager con esperienze in aziende e nella consulenza in materia di rischi, "l'IT è un asset aziendale come gli altri, e i suoi rischi vanno valutati e gestiti così come si fa con ogni ambito di rischio aziendale, ad esempio con la *supply chain*, la reputazione, la sostenibilità, la

governance. Anche di fronte a un aumento della minaccia cyber, l'approccio deve essere quello di rilevarla e inserirla nell'attività integrata di gestione del rischio, in quanto tematica che tocca ogni settore dell'operatività dell'impresa".

DAL CONTESTO INTERNO ALLE TERZE PARTI DELLA SUPPLY CHAIN

Basta vedere quali sono le minacce che afferiscono al rischio tecnologico per comprendere che il cyber crime è solo uno degli aspetti, per quanto importante: la sicurezza delle informazioni, la conformità alla normativa a partire dal Gdpr, la continuità di fornitura del servizio, la centralità dell'infrastruttura digitale negli aspetti amministrativi; a questi si aggiungono i rischi legati alla supply chain, "dove, data l'interconnessione dei sistemi, è consigliabile fare una *due diligence* dei fornitori sui temi IT", e quelli oggi legati ai fattori Esg, "perché l'asset informatico è essenziale per le aziende e il mancato o non corretto funzionamento impatta sulla governance anche della sostenibilità sociale, andando a colpire direttamente il cliente e la responsabilità dell'azienda".

L'integrazione con i diversi ambiti aziendali è quindi fondamentale, perché il rischio non è uguale per tutti. L'*assessment* deve prevedere necessariamente due valutazioni: quella del contesto interno e quella del contesto esterno. La prima permette di conoscere quali sono i processi aziendali più dipendenti dal sistema informatico, quali sono più esposti all'interruzione di attività o al mancato raggiungimento dell'obiettivo a causa della struttura tecnologica.

La valutazione del contesto esterno consente invece di comprendere l'ecosistema in cui l'impresa opera e il livello di esposizione del settore. "Contestualizzare è fondamentale per comprendere quali sono effettivamente i rischi più rilevanti", spiega Avanzi. In sintesi, se l'azienda opera in filiera e l'asset strategico è rappresentato dalla production line digitale, coprire i rischi connessi sarà più urgente (non più importante) rispetto, ad esempio, alla protezione dei dati dei clienti che l'azienda potrebbe gestire in modo molto contenuto e non con operazioni ad elevato impatto. Allo stesso modo, se i fornitori e i partner commerciali dell'impresa hanno base in Europa, è certo che seguiranno le medesime regole sulla privacy e la protezione dei dati personali, riducendo l'esposizione a questo rischio.

"La conferma di quale deve essere la corretta prospettiva rispetto al rischio informatico viene dal *Global Risks Report 2022* del **World Economic Forum**, che tra i rischi nel breve e medio termine colloca il fallimento delle infrastrutture di processo di security (interne) più che il cyber crime in senso stretto (esterno)", precisa Avanzi. Subentra qui un possibile errore di approccio da parte dei risk manager, tra i quali si può manifestare "una sorta di *bias* della disponibilità: c'è la tendenza a concentrarsi sugli aspetti su cui si hanno più informazioni disponibili o che sono più evidenti, a volte anche per rilevanza mediatica o reputazionale, ma non è detto che siano questi l'esigenza prevalente per l'azienda".

BILANCIARE IL PESO REALE DELLA MINACCIA

In ambito di *information technology* sono soprattutto due le situazioni rischiose: la governance del rischio operativo gestionale interno e la supply chain di terze parti.

L'attività IT, e quindi il rischio correlato, permea tutta l'organizzazione ed è necessariamente collegata a terze parti esterne: la gestione di tale rischio deve quindi compenetrare tutta l'azienda ed essere in relazione con la filiera esterna, così da monitorare tutte le possibili minacce.

Si tratta di un rischio altamente pervasivo e dall'elevato impatto strategico, per cui "è importante che sia condiviso con il top management aziendale. In ogni caso, è compito del risk manager sviluppare al massimo la comprensione corretta di tale rischio: dove c'è una visibilità mediatica, come è nel caso del cyber crime, la minaccia viene percepita con chiarezza, ma quello che conta è far capire il rischio reale, quello che potrebbe pesare di più per l'azienda: l'esatta percezione degli scenari del rischio è la grande sfida per i risk manager".

E per far comprendere bene il rischio a cui l'impresa è esposta, il risk manager si assume il compito di interagire con tutti i settori aziendali. Avanzi sottolinea come sia fondamentale in primo luogo "formare una coscienza generale del rischio a tutti i livelli, una volta che tale consapevolezza è presente il secondo passo è tecnico, e riguarda la strutturazione di un modello di gestione del rischio che fornisca dei punti di riferimento osservabili e misurabili, così da dare concretezza all'analisi e evitare di inseguire aspetti magari più visibili ma meno impattanti". La chiave perché questo avvenga è che tra il risk manager e ognuno dei responsabili di linea di business si crei un linguaggio comune, che permetta al primo di conoscere il contesto e ai secondi di comprendere come gestire i diversi aspetti del rischio che toccano il proprio comparto, "in questo senso il risk manager è un facilitatore che aiuta a rendere evidenti le minacce, su cui poi dovranno intervenire le decisioni del top management dall'alto e i singoli responsabili di settore dal basso".