Resilienza organizzativa e prevenzione dei rischi cyber, i trend secondo Spike Reply

intervista a Sonia Crucitti, Partner e CEO di Spike Reply

Ci può parlare di Spike Reply e delle sue attività nel mercato italiano?
Spike Reply è la società del Gruppo Reply focalizzata sulla Cybersecurity e sulla Data Protection.
Dal 2002 la nostra missione, grazie al contributo dei nostri professionisti specializzati sulle principali tecnologie e soluzioni di cyber security e attivi presso i principali organismi e istituti internazionali è quella di supportare i nostri clienti nel prevenire e rispondere agli attacchi cyber, nonché quella di aiutarli ad innalzare la loro security posture e nel rendere la sicurezza un fattore abilitante nei percorsi di digital transformation.
Questi obiettivi vengono raggiunti grazie ad un'offerta completa e integrata, che coniuga l'anima tecnica di Reply, tramite il disegno e l'implementazione di soluzioni di sicurezza innovative, con servizi di advisory e di consulenza strategica per la definizione di programmi di gestione dei rischi cyber in linea con gli obiettivi strategici e il risk appetite dei nostri clienti.

La recente indagine che avete sviluppato con Everbridge sul livello di resilienza delle aziende italiane evidenzia che ci sono ampi margini di miglioramento in termini di preparazione per gestire eventi critici. Dal vostro punto di osservazione, cosa sarebbe opportuno fare per migliorare la situazione, sia a livello aziendale che di sistema?
Dal nostro punto di osservazione confermiamo che vi sono ancora diversi ambiti su cui lavorare per migliorare la gestione di un evento critico e riteniamo che le aziende possano effettuare ulteriori step decisivi per incrementare la propria capacità di resilienza facendo sinergia tra le diverse discipline che, a vario titolo, indirizzano queste tematiche in azienda (corporate e cyber security e business continuity in primis).
In primo luogo, per quanto riguarda le azioni di natura preventiva, molte aziende non hanno ancora messo in campo,

o lo hanno fatto solo parzialmente, attività di simulazione e test delle proprie procedure di gestione degli eventi critici, con il conseguente rischio di non essere adeguatamente preparate.
A nostro avviso, la definizione di un programma di simulazioni e stress test delle procedure di risposta ad un evento critico è una delle azioni fondamentali per il corretto monitoraggio dell'efficacia della propria strategia di resilienza.
Le simulazioni, siano esse table top o test reali (ad esempio in ambito cyber attività di red teaming) sono dal nostro punto di vista tra le iniziative più efficaci e concrete per mettere alla prova le reali capacità di un'azienda di rispondere ad un evento critico.
Sono degli strumenti al contempo di testing e di formazione e awareness che, per essere efficaci, devono utilizzare scenari "threat and risk-intelligence-led" e coinvolgere tutta l'organizzazione, compresi il top management e la supply chain.

Per migliorare la situazione, occorre anche investire sulle tecnologie adottando soluzioni che favoriscano la gestione centralizzata delle crisi, mettendo i team preposti nella condizione di governare tramite un'unica interfaccia gli stakeholder e le risorse necessarie per accelerare i tempi di ripristino, mantenendo il comando e il controllo qualora la crisi evolva in modo inatteso e garantendo la continuità delle attività business-critical.

Il corretto funzionamento di processi e tecnologie non può inoltre prescindere da fonti informative e attività di risk intelligence adeguate, utili a garantire una migliore comprensione dell'evento critico.

Infine, in ottica di miglioramento continuo, risultano esservi spazi per migliorare la raccolta e la sistematizzazione dei KPI, adottando processi e tecnologie per raccogliere dati in maniera automatica e standardizzata, in modo da utilizzare le evidenze raccolte per correggere eventuali criticità ma, soprattutto, per implementare modelli predittivi che consentano di anticipare la manifestazione di un evento critico (analisi predittive "data driven").

L'implementazione di questi spunti di miglioramento porta benefici non solo al livello di resilienza della singola azienda ma anche a livello di sistema, andando a incrementare la capacità complessiva di interi settori e, in una logica più ampia, della supply chain, consentendo così di rispondere ad eventi critici con impatto sistemico.

Il fattore chiave perché questo avvenga è che le diverse realtà che popolano gli ecosistemi aziendali collaborino tra loro in ottica di scambio e cooperazione, condividendo informazioni, partecipando ad attività comuni (ad esempio, esercitazioni e simulazioni) e concordando degli standard da applicare a tutti gli attori della catena di approvvigionamento.

Parlando di prevenzione dei rischi cyber a livello generale, quali trend prevedete nel prossimo futuro?

Per il prossimo futuro prevediamo il consolidamento di tre trend che, seppur in modo diverso, abbiamo già avuto modo di osservare sul campo.

Il primo riguarda uno shift degli investimenti in cybersecurity, shift che vede lo spostamento dello spending dalle contromisure necessarie alla prevenzione dell'attacco, agli investimenti necessari a migliorare le capacità di risposta e gestione dello stesso. Questo cambiamento nelle priorità è, se vogliamo, collegato al concetto stesso di resilienza e, quindi, non alle abilità che consentono di prevenire eventi avversi, ma allo sviluppo di quanto necessario ad affrontarli e superarli con successo. Nel contesto attuale le aziende hanno ormai capito che quando si parla di attacchi cyber la variabile non è più "se" ciò avverrà, ma "quando".

Il secondo trend riguarda invece la visione della cybersecurity come elemento pervasivo e nativamente integrato nell'organizzazione e nei propri prodotti/servizi digitali. Sulla falsa riga di quanto già fatto in passato per la qualità, le organizzazioni più virtuose hanno iniziato a considerare la cybersecurity come un elemento pervasivo, in grado di contagiare ed essere integrato in tutte le attività dell'organizzazione stessa. La sicurezza non è più qualcosa da aggiungere a difesa e protezione, ma una caratteristica intrinseca di ogni asset e processo.

Il terzo ed ultimo trend riguarda invece una visione di stampo sistemico per quanto riguarda gli aspetti di security impattanti sulla propria organizzazione. Ogni organizzazione, ed in particolare i servizi digitali che ne rappresentano il cuore pulsante, sono ormai composti attraverso la creazione di ecosistemi complessi e dinamici, ecosistemi che prevedono l'integrazione e l'interazione con fornitori di varia natura. Questo implica che il perimetro da considerare nelle valutazioni di sicurezza debba necessariamente considerare la supply chain nella sua interezza. La capacità di resilienza non dipende più solo da quanto sotto il controllo di un'organizzazione, ma dal livello di resilienza di ogni attore coinvolto il tale ecosistema. L'anello più debole, anche se apparentemente non rilevante, potrebbe infatti compromettere la resilienza di un intero ecosistema.

REPLY SPIKE