

CYBER CRIME E IMPRESE: AVANTI PIANO

NON SOLO LA SPINTA DELLE NUOVE NORME ITALIANE ED EUROPEE MA ANCHE LA CONSAPEVOLEZZA CHE NESSUNO È IMMUNE STA MODIFICANDO L'ATTENZIONE VERSO I RISCHI INFORMATICI. RIMANE AMPIO IL GAP TRA LE GRANDI AZIENDE, CHE SI STANNO ORIENTANDO VERSO UNA DIVERSA ORGANIZZAZIONE DI SISTEMA, E LE PMI CHE ANCORA AGISCONO PER OBBLIGHI DI COMPLIANCE

Con l'imperversare di attacchi cyber che ha caratterizzato il 2016, la consapevolezza delle aziende italiane sui rischi tecnologici è cresciuta ma il gap con altre realtà è ancora da colmare. Alcune recenti ricerche mostrano come, seppur lentamente, il tema dei rischi cyber stia facendo breccia nelle imprese, in modo particolare tra quelle che poggiano una parte importante del proprio business sulla gestione dei dati. Il combinato di pervasività delle tecnologie digitali e di crescita delle minacce sta facendo aumentare, soprattutto nelle grandi aziende, la consapevolezza che la difesa dai rischi cyber deve avere un approccio di sistema. Per **Alessandro De Felice**, presidente di **Anra** (Associazione nazionale dei risk manager e responsabili assicurativi aziendali), nelle imprese "troppo spesso manca una cabina di regia che organizzi difese efficaci in un'ottica di medio-lungo periodo e le sottoscrizioni delle polizze assicurative contro i rischi cyber e i danni causati a terzi sono ancora poche, siglate solo da un'impresa su sette".

TRA I RISCHI PIÙ TEMUTI

Secondo l'*Allianz risk barometer 2017*, a livello globale i rischi cyber si piazzano al terzo posto tra i più temuti, che diventa quarto in Italia dove si dà precedenza ai rischi catastrofali; il rischio conseguente che più assume rilievo tra gli intervistati è la *business interruption*. La

tendenza è confermata dal *Marsh continental european Cyber risk survey*, nel quale il 32% delle imprese intervistate dichiara di inserire il cyber risk tra i cinque rischi più considerati dalla propria organizzazione e un altro 41% lo colloca fuori dai Top5 ma comunque in evidenza, e solo il 9% non lo ritiene un rischio da gestire. Un focus sulla realtà italiana emerge dall'edizione 2016 dell'indagine internazionale di **Zurich** sulle Pmi, che registra un aumento della consapevolezza con solo il 10% delle imprese che si ritiene *non a rischio* contro il 17% del 2015. Rispetto al rischio cyber, per le imprese italiane le conseguenze più temute sono il furto di dati dei clienti (20,5%), l'interruzione del business (18,5%), i danni alla reputazione aziendale (17%) e i furti di denaro (11,5%).

VERSO PREVENZIONE E NUOVI INVESTIMENTI

Rispetto alla presa di coscienza sui rischi tecnologici, i risultati della ricerca sul cyber crime svolta dall'*Osservatorio information security e privacy* del Politecnico di Milano mostrano un trend evolutivo guidato dalle grandi aziende (più di 249 dipendenti). La crescente consapevolezza mette al centro l'importanza del dato, orientando gli interventi dalla semplice *compliance* alla prevenzione e gestione del rischio, con nuovi investimenti. Il 18% delle grandi aziende intervistate ha dichiarato di avere un

piano di investimento pluriennale per la sicurezza tecnologica con riferimenti anche nel piano industriale, il 21% ha predisposto un piano di investimenti pluriennale senza richiami nel piano industriale, per il 34% il budget è annuale mentre il 27% lo stanziava all'occorrenza: la somma delle due prime voci è aumentata del 7% rispetto allo scorso anno. Un altro indicatore dei cambiamenti in atto nelle grandi imprese è nella funzione del *ciso*, il *chief information security officer*, un ruolo di responsabilità necessario in presenza di un piano strategico di security: è presente in modo formalizzato nel 46% del campione (ma solo il 10% di questi risponde direttamente al board), nel 12% è un ruolo non formalizzato, il 9% ne prevede l'introduzione entro 12 mesi, negli altri casi il presidio della sicurezza è demandato al *cio* (28%) o a figure esterne all'Ict (5%).

CHI CONOSCE LA CYBER INSURANCE

Punto debole di grandi e piccole imprese sono i prodotti assicurativi a copertura del rischio tecnologico. Secondo il Continental european Cyber risk survey condotto da Marsh, il 13% delle aziende europee ha sottoscritto polizze sul rischio cyber, il 34% ne sta valutando l'acquisto e il restante 53% non ha ancora pensato di farlo. I risultati dell'indagine condotta da **Osservatori.net** confermano per l'Italia questo sostanziale distacco rispetto ai prodotti assicurativi cyber: il 15% delle imprese dichiara di avere delle polizze attive sul rischio cyber, ma solo nella metà dei casi si tratta di prodotti specifici, il 29% sta valutando l'adozione di coperture cyber e il 21% considera la questione non di rilievo. Questi dati sono un indicatore di come la cultura verso la *cyber insurance* sia per la maggior parte delle aziende ancora in fase di crescita, ma un quarto dato fornito apre a una riflessione: il 35% delle intervistate considera "non sufficientemente matura" l'offerta di cyber insurance.

POLIZZE SUL RISCHIO CYBER

● AZIENDE EUROPEE ●



Fonte: Continental european Cyber risk survey, a cura di Marsh

PMI TRA COMPLIANCE E BUON SENSO

Non stupisce nell'analisi dell'Osservatorio che la consapevolezza sui rischi informatici sia proporzionale alle dimensioni dell'organizzazione aziendale. Se le grandi aziende guidano l'evoluzione, i dati rilevati tra le Pmi intervistate confermano una maggiore sensibilità in quelle dai 100 ai 249 addetti rispetto al gruppo 10-49 addetti. Anche se nel complesso il 93% delle Pmi ha stanziato un budget per la sicurezza tecnologica nel 2016, colpisce che la motivazione principale riguardi ancora nel 48% dei casi le ragioni di compliance, mentre il 35% si muove dopo aver subito un attacco, la necessità di aumentare la protezione dei dati aziendali è una motivazione per il 22% delle imprese e per il 31% la spinta è legata a nuove esigenze di business. Il limite è nella scarsa conoscenza dei rischi e delle conseguenze, testimoniata da un 25% di aziende che per la tutela del rischio cyber si affida solo al *buon senso* dei propri collaboratori. **M.M.**