Il mercato della security in Italia: in quali aree investono le aziende?

Author : Alessandro Piva

Date : 25 Marzo 2020

Nel corso del 2019 l'*information security* è diventata una delle maggiori **priorità di investimento** nel digitale per le aziende nell'agenda dei Chief Innovation Officer. Basta tale dato a testimoniare come l'attenzione verso questo ambito sia cresciuta in maniera esponenziale anche agli occhi di chi non si occupa, nello specifico, della materia. Parallelamente, è maturata la consapevolezza che si tratti ormai di un **tema strategico** e imprescindibile per le organizzazioni e non più un ostacolo allo sviluppo del business.

In questo scenario si è mosso l'Osservatorio Information Security & Privacy del Politecnico di Milano, che ha condotto durante l'anno appena trascorso un'indagine volta a monitorare il mercato dell'*information security* in Italia con l'obiettivo di fotografarne le principali dinamiche di sviluppo.

Nello specifico, la **Ricerca 2019** dell'Osservatorio ha proposto una *survey* di rilevazione che ha coinvolto 698 CISO, CSO, CIO, Compliance Manager, Risk Manager, Chief Risk Officer e DPO di imprese italiane. In particolare sono state coinvolte 180 organizzazioni grandi (>249 addetti) e 501 PMI (tra 10 e 249 addetti).

L'evoluzione del mercato dell'*information security* e la sua scomposizione

Il mercato dell'*information security* in Italia ha raggiunto nell'anno appena concluso un valore di **1,3 miliardi di euro**, in crescita rispetto ai 12 mesi precedenti. Il 2019 ha registrato pertanto un trend positivo in continuità con gli ultimi anni, con un aumento della spesa di poco inferiore all'11% (Figura 1).

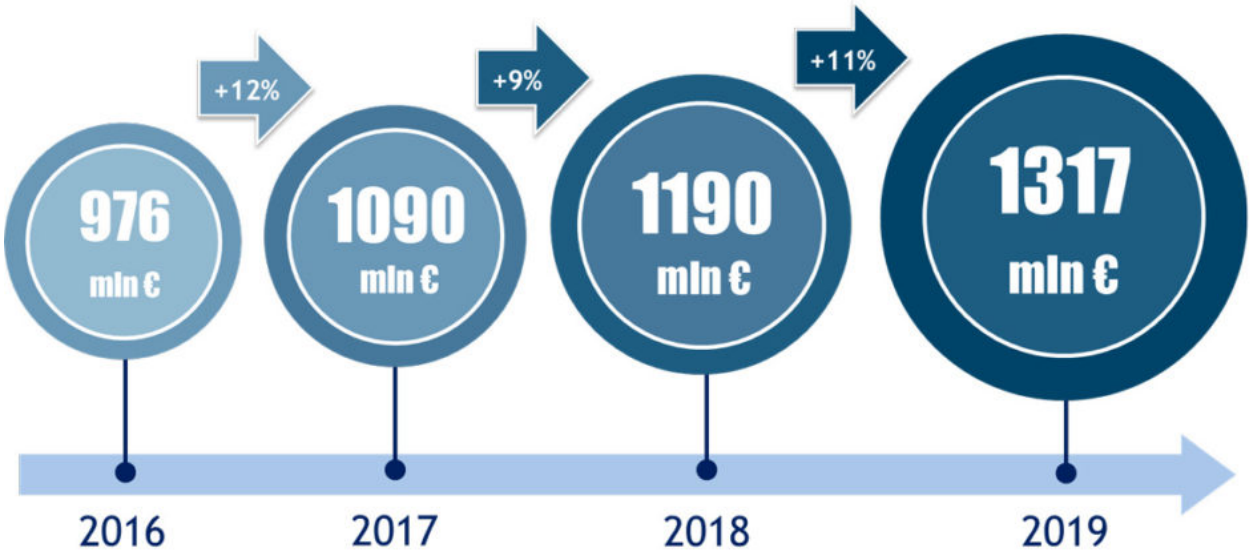

Figura 1: Il mercato dell'information security in Italia nel 2019 – Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano

Ma quali sono le aree su cui le aziende investono maggiormente? Per meglio comprendere le dinamiche all'interno del mercato, l'Osservatorio ha approfondito due viste di dettaglio, una focalizzata sulla **tipologia di sicurezza** e l'altra sulle **componenti di spesa.**

In merito alla tipologia di sicurezza sono state identificate sei categorie principali, in relazione al target da proteggere. Secondo questa categorizzazione, la quota principale della spesa, ossia il 36%, è catalizzata dalla voce *"Network & Wireless Security"*, termine con cui si intende la **protezione della rete** fisica e logica. Al secondo posto, con il 20%, si trova la sicurezza degli *endpoint*, siano essi postazioni fisse o *devices* mobili funzionali allo smart working. Una porzione rilevante, pari al 19%, è invece ascrivibile agli strumenti di supporto alla sicurezza a livello di **applicazioni:** in questa categoria si trovano le logiche di gestione delle implicazioni della *security* in fase di sviluppo (*by design*), così come le misure di protezione attive una volta che il servizio è operativo.

La crescente diffusione dei **servizi Cloud** richiede strumenti all'avanguardia dal punto di vista della protezione delle informazioni: non stupisce quindi che il 13% della spesa sia dedicata a questa categoria che rappresenta peraltro l'area in cui il maggior numero di organizzazioni dichiara una crescita di spesa. Altro tema di interesse, per un 5%, è rappresentato dai dispositivi connessi dell'***Internet of Things***, ormai diffusi in svariati ambiti che spaziano dalla casa, alla città o ai veicoli, solo per citare gli esempi più rilevanti.
Infine vi è un'ulteriore categoria residuale, non indagata esplicitamente, in cui rientrano svariate voci, relative prevalentemente ad **aspetti di *governance*,** che occupa il restante 7% (Figura 2).

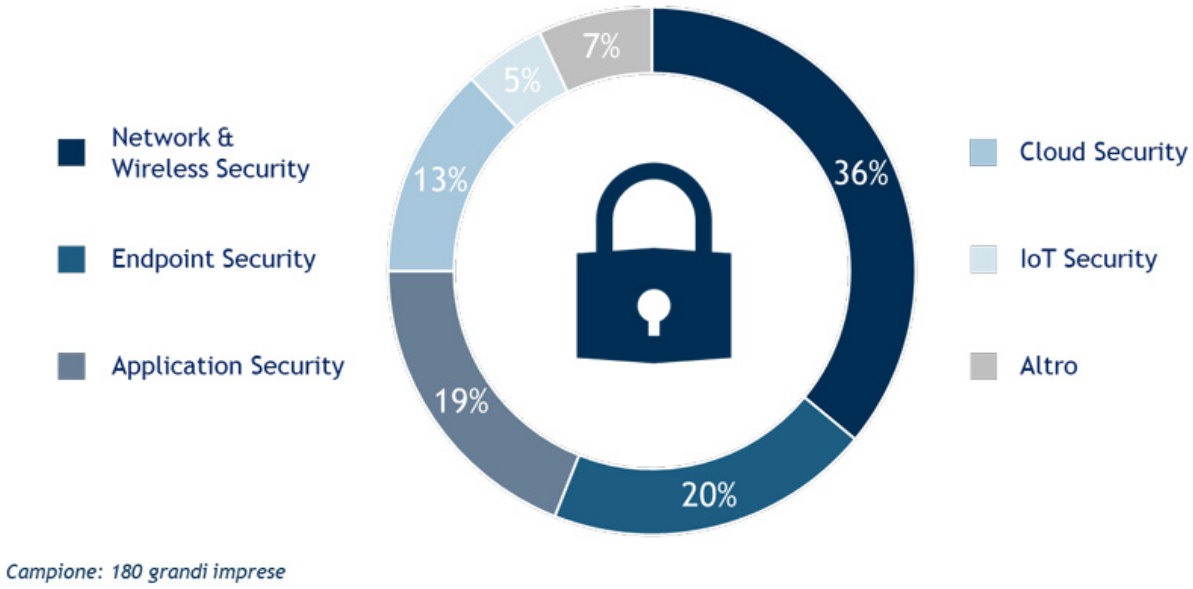

Figura 2: La scomposizione della spesa in information security per tipologia di sicurezza – Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano

La seconda classificazione, come anticipato, riguarda le componenti di spesa, a loro volta suddivise, a un primo livello, in **soluzioni**, per il 52% della spesa totale, e in **servizi**, per il restante 48%.

Tale vista è stata scomposta ulteriormente: in particolare, per quanto riguarda le soluzioni sono state approfondite otto categorie riferibili alla tipologia di prodotto offerto (Figura 3).

A catalizzare le quote maggiori di spesa sono innanzitutto le soluzioni di *Identity and Access Management*, che permettono la gestione e il monitoraggio degli accessi degli utenti a infrastrutture, applicazioni e dati critici, seguite dai prodotti di *Vulnerability Management/Penetration Testing,* volti a individuare e misurare il grado di gravità delle vulnerabilità e testare la sicurezza di sistemi, applicazioni o reti, anche attraverso la **simulazione di attacchi** da parte di soggetti malintenzionati e dalle soluzioni appartenenti alla categoria *Risk and Compliance Management,* volte ad analizzare il livello di esposizione al rischio cyber dei sistemi informatici aziendali e garantire la **conformità a standard, framework e normative** in materia di sicurezza delle informazioni e protezione dei dati.

Leggermente più in basso dal punto di vista dell'incidenza sul budget si trovano le soluzioni di *Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)*, che monitorano il traffico di rete per identificare e bloccare gli accessi non autorizzati a un determinato sistema o dispositivo e quelle di *Security Information and Event Management (SIEM)*, in grado di raccogliere e analizzare dati provenienti da vari fonti e segnalare in tempo reale eventuali anomalie e criticità al personale che si occupa di security; quest'ultima componente, peraltro,

rappresenta la principale voce su cui le organizzazioni dichiarano di voler aumentare i propri investimenti.

Le altre tipologie di soluzioni indagate appartengono alla categoria *Unified Threat Management (UTM)*, in cui rientrano prodotti per una **gestione integrata delle minacce di sicurezza** che includono normalmente funzionalità come antivirus, anti-spyware, anti-spam, firewall di rete, rilevamento e prevenzione delle intrusioni, filtraggio dei contenuti e protezione dalle perdite di dati, e alla categoria *OSS Risk Prevention (CVE)*: quest'ultima voce, più di "nicchia", racchiude soluzioni volte a mitigare i rischi per la sicurezza attraverso la valutazione dei gap e delle vulnerabilità note presenti nelle componenti software open source.

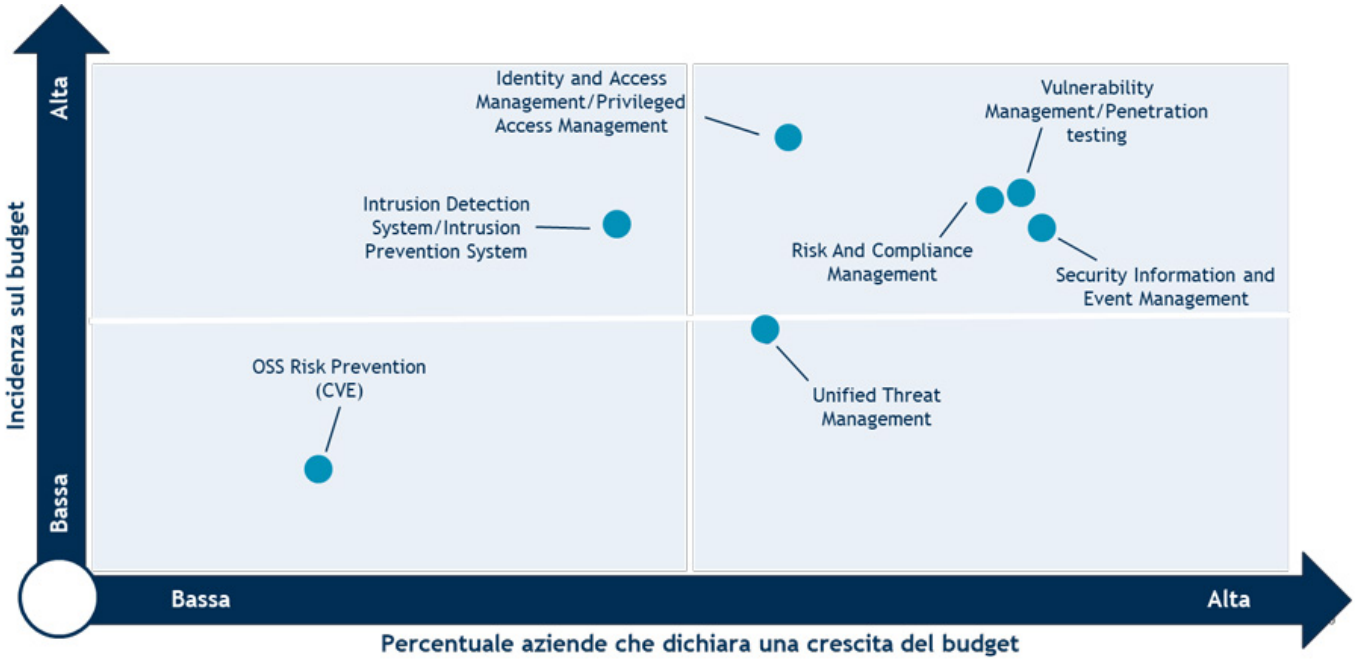

Figura 3: La scomposizione della spesa in soluzioni di information security – Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano

Anche la componente di spesa relativa ai servizi è stata ulteriormente suddivisa: la quota relativa ai ***professional services***, ossia i servizi offerti da *provider* esterni all'organizzazione per il compimento di uno specifico progetto, vale il 54% del totale, mentre la quota relativa ai ***managed services***, voce con cui si intendono i servizi offerti in maniera continuativa da *provider* esterni all'organizzazione per garantire il supporto e la manutenzione dei sistemi informativi aziendali, vale il restante 46%.

In conclusione, la dinamica del mercato pare confermare la maggiore attenzione da parte delle organizzazioni al tema della *security*, con un bilanciamento della spesa che interessa in misura crescente componenti innovative, legate alla gestione degli *endpoint*, al design delle applicazioni, al Cloud e ai dispositivi connessi.
In tale contesto di diffusa crescita, si evidenzia inoltre la tendenza a ricorrere sempre di più a

servizi professionali e servizi gestiti, in grado di fornire il supporto necessario per garantire un’adeguata ed efficace tutela delle informazioni aziendali.

Bibliografia

Security-enabled transformation: la resa dei conti – Osservatorio Information Security & Privacy, School of Management Politecnico di Milano

Articolo a cura di **Alessandro Piva**