**School of Management – Politecnico di Milano**
**www.osservatori.net**

COMUNICATO STAMPA

Osservatorio Information Security & Privacy

# CRESCE IL MERCATO DELL'INFORMATION SECURITY: 1,3 MLD DI EURO NEL 2019, +11%

*Il 51% delle aziende dichiara un aumento nei budget di security: il 52% della spesa è dedicata a soluzioni, ma sono i servizi a crescere di più (in crescita nel 45% delle organizzazioni). Il 45% delle grandi imprese impiega anche strumenti di Artificial Intelligence per gestire la sicurezza*

*Il 55% delle imprese è conforme al GDPR, il 45% ha aumentato il budget*

*Il 40% delle aziende ricerca nuovi profili, soprattutto Security Analyst, Security Architect e Security Engineer. Scarsa la maturità organizzativa: il 40% non ha una divisione Information Security*

*Milano, 5 febbraio 2020* – Per il terzo anno consecutivo cresce il mercato dell'information security in Italia, che nel 2019 raggiunge un valore di 1,317 miliardi di euro, in crescita di poco meno dell'11% rispetto all'anno precedente (dopo aver registrato un +9% nel 2018 e un +12% nel 2017). La spesa in sicurezza si concentra soprattutto in soluzioni di security, che raccolgono il 52% degli investimenti (in particolare per componenti di sicurezza più tradizionali), a fronte del 48% nei servizi che però crescono maggiormente (in crescita per il 45% delle aziende). La tecnologia al centro dell'attenzione è l'Artificial Intelligence, già impiegata per la gestione della sicurezza dal 45% delle grandi imprese.

A fine 2019, il 55% delle imprese ha completato l'adeguamento al GDPR (erano il 24% lo scorso anno), il 45% ha aumentato gli investimenti a questo scopo e il 61% oggi ha in forza all'interno della propria organizzazione un Data Protection Officer. Ora si guarda agli effetti del Cybersecurity Act, che ha definito un sistema di certificazione per la sicurezza informatica a livello europeo e che per il 76% degli Executive porterà più garanzie di sicurezza, uniformità normativa, vantaggi competitivi e calo dei costi.

La spinta normativa e la crescita degli investimenti trainano la domanda di competenze nell'information security. Il 71% delle grandi imprese italiane afferma che il team interno ha già le competenze necessarie, il 40% sta cercando nuovi profili. In particolare, il 51% attualmente è alla ricerca di Security Analyst, il 45% di Security Architect e il 31% Security Engineer, figure quindi in cima alle richieste dei recruiter. Appare ancora scarsa, però, la maturità organizzativa delle imprese: nel 40% delle organizzazioni non esiste una specifica funzione Information Security, che rimane all'interno dell'IT, e il responsabile della sicurezza è lo stesso CIO.

Sono alcuni dei risultati della ricerca dell'**Osservatorio Information Security & Privacy della School of Management del Politecnico di Milano***, presentata questa mattina al convegno "*Security-enabled transformation: la resa dei conti*".

"Il mercato italiano dell'Information Security si conferma dinamico e in crescita anche nel 2019. La sicurezza informatica non è più percepita come un ostacolo all'adozione di nuove tecnologie e servizi, ma come un fattore fondamentale per il successo del business – afferma **Alessandro Piva**, Direttore dell'Osservatorio Information Security & Privacy - ma c'è ancora molta strada da fare nella maturità organizzativa. Ben il 40% delle imprese non ha una funzione specifica che si occupi di sicurezza informatica: questo genera incertezza e oltre un'impresa su due è insoddisfatta di come viene gestita. Emerge la necessità di adottare un modello integrato di governance della security che permetta di definire modalità di intervento uniformi e monitorare in maniera completa e affidabile le potenziali minacce".

"Anche dal punto di vista della privacy ci sono evidenti miglioramenti in relazione all'adeguamento al GDPR, dove però esiste ancora un certo numero di aziende non conformi, con e un diffuso ottimismo anche nei confronti del Cybersecurity Act. - afferma **Gabriele Faggioli**, Responsabile Scientifico dell'Osservatorio Information Security & Privacy -. Allo stesso tempo, però, le minacce alla sicurezza diventano sempre più numerose e pericolose: per difendersi le imprese sono chiamate ad attivare logiche di security-by-design e strumenti di protezione in tempo reale".

**Il mercato dell'Information Security** – Il 52% delle risorse è dedicato a soluzioni di sicurezza (in aumento del 26%rispetto al 2018), il restante 48% ai servizi (in crescita per il 45% delle aziende). Tra le soluzioni, la categoria che raccoglie la quota principale della spesa è la "Network & Wireless Security", intesa come protezione della rete fisica e logica (36%), seguita dalla "Endpoint Security" (20%), che comprende postazioni fisse e dispositivi mobili, e dalla "Application Security" (19%). La protezione degli ambienti Cloud attrae il 13% della spesa e rappresenta la categoria con la crescita più elevata (in crescita per il 55% delle aziende). Vengono poi i dispositivi connessi dell'Internet of Things, col 5%, e un'ulteriore voce marginale in cui rientrano diversi aspetti di governance, che complessivamente coprono il 7% del budget. I servizi più finanziati sono quelli offerti da fornitori esterni all'azienda per progetti specifici (professional services, 54%), ma quelli più in crescita sono i servizi offerti in maniera continuativa da provider esterni all'organizzazione per garantire il supporto e la manutenzione dei sistemi informativi aziendali (in aumento nel 45% delle organizzazioni).

I trend dell'innovazione digitale considerati priorità di investimento nell'information security e data protection indicati dalle imprese nell'anno appena trascorso sono Cloud (67%), Mobile (43%) e Big Data (41%). Seguono Industria 4.0 (39%), eCommerce & Payment (37%), Internet of Things (31%), Artificial Intelligence (27%), Blockchain (13%), 5G (10%) e Realtà Aumentata e Virtuale (7%).

**I modelli organizzativi per la gestione della security** – Dalla ricerca emerge un diffuso ritardo nei modelli organizzativi e di gestione della sicurezza informatica: nel 40% delle imprese è assente una specifica funzione e una figura direzionale dedicata all'Information Security, la cui gestione è affidata ancora al CIO e all'IT. In più di un quarto del campione, inoltre, esiste una funzione esterna ai Sistemi Informativi, ma la figura responsabile della sicurezza (CISO o ruolo equivalente) riporta all'IT (27%). Sono poche le imprese in cui la funzione Security riporta a una funzione aziendale diversa dall'IT (17%) o direttamente al Board (16%).

La scarsa maturità organizzativa si riflette nella mancanza di soddisfazione, con oltre metà delle realtà che boccia il modello di gestione della sicurezza impiegato. L'insoddisfazione è più elevata dove la funzione Security riporta alla divisione IT (65%), mentre è minima nelle realtà in cui il CISO riferisce direttamente al Board (il 90% è contento della struttura organizzativa utilizzata). Più strutturata la gestione del fattore umano: nel 55% del campione è attivo un piano formativo pluriennale che coinvolge l'intero personale, nel 25% la formazione è rivolta alle sole divisioni più sensibili al tema (come IT, Risk Management e Compliance), mentre il 20% non ha un progetto formativo strutturato.

**L'information security in ambito industriale** – L'interconnessione di sistemi industriali e la sempre maggiore diffusione di dispositivi IoT pongono il problema della protezione degli ambienti OT (Operational Technologies). Il principale rischio di OT Security individuato dalle aziende è il fermo della produzione (54%), seguito dalla "safety" (20%), minacciata dall'interazione sempre più diretta fra operatori e macchine (ad esempio la robotica collaborativa), dall'alterazione o modifica della produzione (16%) e dal furto o perdita di dati confidenziali (10%). Per fronteggiare questi rischi, il 68% delle aziende effettua security assessment e/o audit su sistemi e reti OT e il 60% ha introdotto strumenti di sicurezza specifici per l'ambito industriale.

La gestione dell'OT Security all'interno delle grandi aziende viene affidata nella maggioranza dei casi alla funzione IT (47%), mentre è più marginale il ruolo delle divisioni Information Security (11%) e Operations (4%). Nel 23% dei casi se ne occupano più funzioni aziendali, nel 15% la gestione non è affidata a nessuna funzione, profilo o fornitore. In quasi una realtà su due (48%) sono presenti figure interne con competenze di OT Security sparse fra le diverse funzioni aziendali, prevalentemente IT (25%), poi Information Security (15%), Operations (6%) o in altre funzioni (2%). Il 22% non ha ancora inserito figure specializzate ma intende farlo nel corso del 2020, il 30% non ha intenzione di introdurle in futuro.

**L'impatto di AI e IoT** – L'Osservatorio ha analizzato l'impatto dell'Artificial Intelligence e della Blockchain sull'information security. Solo il 44% dei CISO ha una conoscenza almeno discreta dell'AI, percentuale che scende al 28% quando si parla di Blockchain. Quattro imprese su dieci giudicano positivamente l'impiego della Blockchain per applicazioni di security, ma soltanto l'1% ha attivato un progetto e appena il 16% lo sta valutando per il futuro, soprattutto per garantire che il dato non venga

modificato, per gestire la privacy e i diritti di accesso ai dati e per l'identificazione di dispositivi fisici connessi.

Più diffuso il consenso sulle capacità dell'AI di garantire più sicurezza rispetto ai sistemi tradizionali e agli operatori umani (rispettivamente 86% e 85%) e rendere il personale addetto più efficiente (82%), anche se la maggior parte del campione ritiene che l'AI non possa sostituire completamente il giudizio umano nel contesto della security (89%) e il 77% pensa che sia necessario dotarsi di profili esperti di questa tecnologia. L'impiego di algoritmi di AI e Machine Learning per la gestione della sicurezza informatica è cresciuto significativamente nel 2019, passando dal 22% al 45% di imprese che ne fanno uso, soprattutto nel monitoraggio dei comportamenti di sistemi e persone per rilevare potenziali minacce (71%), nell'identificazione di tentativi di phishing (41%) e nella prevenzione di possibili frodi (25%). Seguono l'analisi e la gestione degli incidenti (24%) e la ricerca di vulnerabilità in fase di sviluppo software (16%).

**GDPR, NIS e Cybersecurity Act** – Il 55% delle imprese ha completato i progetti di adeguamento al GDPR (+31% sul 2018), nel 30% queste iniziative sono ancora in corso (erano il 58% un anno fa), il 5% si trova ancora nella fase di analisi dei requisiti, mentre nel 10% il tema non è ancora all'attenzione del Board. Con l'aumento delle imprese conformi crescono gli investimenti: il 45% ha aumentato il budget dedicato, nel 53% delle realtà è rimasto invariato, solo il 2% lo ha ridotto. L'aumento della mole di lavoro a cui è stata sottoposta l'Autorità Garante nell'ultimo anno e l'iniziale indulgenza prevista dalla normativa hanno limitato il numero di controlli al GDPR: solo il 2% ha dichiarato di aver subito ispezioni formali, l'89% non ha ricevuto controlli, mentre il 9% ha preferito non rispondere. Ma con la messa a regime del meccanismo sanzionatorio, il 45% di imprese che ancora non ha completato i progetti di adeguamento è chiamato ad accelerare il processo per non incorrere in sanzioni.

Più indietro le iniziative per la conformità alla Direttiva NIS, recepita in Italia il 24 Giugno 2018, che promuove una cultura di gestione del rischio e di segnalazione degli incidenti fra i principali operatori economici. Solo il 6% ha completato le attività richieste, il 12% si sta adeguando ai requisiti, il 16% sta valutando cosa fare, il 24% non si è ancora attivato mentre il restante 42% dichiara di non essere coinvolto dalla normativa.

Il Cybersecurity Act, entrato in vigore il 27 giugno 2019 con l'obiettivo di creare un quadro europeo sulla certificazione della sicurezza informatica di prodotti ICT e servizi digitali, produrrà i primi effetti nei prossimi anni. Finora la percezione degli Executive è positiva: per il 67% consentirà alle aziende di scegliere i prodotti e servizi tecnologici con maggiori garanzie di sicurezza. Il 14% del campione teme però che gli Stati membri creeranno diversi meccanismi di rilascio delle certificazioni annullando lo sforzo di elaborare un quadro comune, mentre il 10% crede che le imprese si concentreranno più sulla vendita del prodotto che sulla garanzia di maggiore sicurezza. Il restante 9% ritiene che le aziende avranno vantaggi competitivi e di risparmio dei costi, in quanto non sarà più necessario seguire processi di certificazione nazionali.

**Le competenze** – Dall'indagine dell'Osservatorio emerge un quadro positivo anche per quanto riguarda la presenza di competenze di security e data protection nelle imprese. Il 71% afferma che il team interno ha le competenze necessarie, ma fra queste il 30% sta cercando altre figure specializzate da introdurre in organico; resta tuttavia ancora elevata la percentuale di aziende sprovviste dei profili necessari per gestire la sicurezza (29%, di cui solo il 9% sta selezionando nuovi ruoli e il 20% si affida a consulenti esterni).

Circa il 40% delle aziende è quindi alla ricerca di nuove risorse e il 77% di queste incontra difficoltà a reperire sul mercato profili specializzati. La figura più ricercata è il Security Analyst (dal 51% di queste aziende), che valuta le vulnerabilità di reti, applicazioni e servizi proponendo soluzioni e accorgimenti pratici, seguita dal Security Architect (45%), che cura il disegno armonico e coerente delle misure di security presenti in azienda, e dal Security Engineer (31%), che monitora i sistemi e propone soluzioni per rispondere agli incidenti. Seguono l'Ethical Hacker (24%), che simula gli attacchi informatici per individuarne le vulnerabilità, il Security Administrator (22%), che rende operative le soluzioni tecnologiche di security, l'OT Security Specialist (20%), che sviluppa e introduce soluzioni per ridurre i rischi di sicurezza in ambito industriale, il Machine Learning Specialist (14%), che sviluppa e monitora

sistemi per gestire possibili minacce in tempo reale e in modo automatico, e il Security Developer (12%), che lavora a soluzioni di sicurezza e all'integrazione dei servizi di terze parti.

Nell'ambito privacy, nel 2019 è leggermente diminuita la presenza di Data Protection Officer (DPO), inserito formalmente nel 57% delle imprese e informalmente nel 4% (erano il 71% complessivamente nel 2018), ma è cresciuto del 9% il numero di imprese che delega questa responsabilità a un consulente esterno (dal 18% al 27%). Il 2% dichiara la volontà di introdurre questo ruolo in futuro, nel 10% invece l'introduzione della figura non è prevista.

**L'assicurazione del rischio cyber** – Il mercato della cyber insurance in Italia è ancora in fase di sviluppo ma crescono le aziende che stanno valutando polizze assicurative. Circa un terzo del campione ha attivato coperture assicurative di trasferimento del rischio cyber (in linea col 2018), suddivise fra imprese che hanno scelto polizze completamente dedicate al cyber risk (19%) e altre che hanno preferito assicurazioni generaliste che coprono in parte questo rischio (11%). Il 37% sta valutando (+12% sul 2018), il 23% non è al momento interessato, il 10% non le conosce. Solo metà del campione gestisce il rischio cyber con un processo di Risk Management che coinvolge l'intera azienda, il 40% affida questa attività alla funzione IT o a un'altra singola divisione, mentre nel 10% dei casi il cyber risk non viene nemmeno monitorato costantemente.

**Le PMI** – Pur se in ritardo rispetto alle grandi imprese, le PMI mostrano un leggero miglioramento nella gestione dell'information security. Il 90% dispone di soluzioni di sicurezza di base come sistemi antivirus e antispam e una su due sta investendo per migliorare la propria dotazione di security. Nel 43% è presente un ruolo che si occupa di sicurezza informatica, anche se nella maggior parte dei casi non si tratta di un vero e proprio CISO, ma di una figura interna che gestisce gli strumenti aziendali e si occupa della relazione con i fornitori.

Cresce l'attenzione alla formazione: il 54% delle PMI ha attivato corsi di formazione sulla sicurezza informatica, contro il 33% nel 2018. Si intravedono progressi anche nella gestione della privacy e della protezione dei dati. Solo il 9% delle PMI non conosce il GDPR (il 2% fra le medie imprese) e il 67% ha attivato progetti di adeguamento alle normative, seppur spesso limitati ad attività che richiedono investimenti contenuti. Il 44% ha definito un ruolo dedicato alla privacy, percentuale che sale al 53% fra le medie imprese. Nel complesso, tuttavia, le PMI faticano a prendere consapevolezza sugli impatti e sui rischi di una cattiva gestione della sicurezza informatica.

**L'edizione 2019-2020 dell'Osservatorio Information Security & Privacy è realizzata con il supporto di Assolombarda, CAST Italia, Microsoft, Fastweb, Lutech, Poste Italiane, Spike Reply, TESISQUARE©; Axians – Check Point, CyberArk, Informatica, Moviri, Nodes; AXA XL, CryptoNet Labs, Generali Global Corporate & Commercial, Nido Group; in collaborazione con Cefriel e DEIB e con il patrocinio di ANRA – Associazione Nazionale Risk Manager e Responsabili Assicurazioni Aziendali e Clusit.*

**Ufficio stampa School of Management del Politecnico di Milano**

Barbara Balabio
Tel.: 02 2399 9545
email barbara.balabio@osservatori.net
Skype barbara.balabio
www.osservatori.net

**d'I Comunicazione**:

Piero Orlando
po@dicomunicazione.it
Mob.: 335 1753472

Marco Puelli
mp@dicomunicazione.it
Mob.: 320 1144691

***La School of Management del Politecnico di Milano**, costituita nel 2003, accoglie le molteplici attività di ricerca, formazione e alta consulenza, nel campo dell'economia, del management e dell'industrial engineering che il Politecnico porta avanti attraverso le sue diverse strutture interne e consortili. La Scuola ha ricevuto, nel 2007, il prestigioso accreditamento EQUIS. Nel 2009 è entrata per la prima volta nel ranking del Financial Times delle migliori Business School europee. Nel 2013 ha ottenuto il prestigioso accreditamento internazionale da AMBA. Dal 2015, la Scuola è membro di AACSB International. La Scuola è presente inoltre nei QS World University Rankings. Nel 2017, la School of Management è la prima business school italiana a vedere riconosciuta la qualità dei propri corsi erogati in digital learning nei master Executive MBA attraverso la certificazione EOCCS. La Scuola è membro PRME, Cladea e QTEM. Fanno parte della Scuola: il Dipartimento di Ingegneria Gestionale e il MIP Graduate School of Business che, in particolare, si focalizza sulla formazione executive e sui programmi Master. Le attività della School of Management legate all'Innovazione Digitale si articolano in*

*Osservatori Digital Innovation, che fanno capo per le attività di ricerca al Dipartimento di Ingegneria Gestionale, e Formazione executive e programmi Master, erogati dal MIP.* ***Gli Osservatori Digital Innovation*** *della School of Management del Politecnico di Milano nascono nel 1999 con l'obiettivo di fare cultura in tutti i principali ambiti di Innovazione Digitale. Oggi sono un punto di riferimento qualificato sull'Innovazione Digitale in Italia che integra attività di Ricerca, Comunicazione e Aggiornamento continuo. La Vision che guida gli Osservatori eÌ che l'Innovazione Digitale sia un fattore essenziale per lo sviluppo del Paese. La mission è produrre e diffondere conoscenza sulle opportunità e gli impatti che le tecnologie digitali hanno su imprese, pubbliche amministrazioni e cittadini, tramite modelli interpretativi basati su solide evidenze empiriche e spazi di confronto indipendenti, pre-competitivi e duraturi nel tempo, che aggregano la domanda e l'offerta di Innovazione Digitale in Italia. Le attività sono svolte da un team di quasi 100 tra professori, ricercatori e analisti impegnati su oltre 40 differenti Osservatori che affrontano i temi chiave dell'Innovazione Digitale nelle Imprese (anche PMI) e nella Pubblica Amministrazione: Agenda Digitale, Artificial Intelligence, Big Data & Business Analytics, Blockchain & Distributed Ledger, Business Travel, Cloud Transformation, Cloud nella PA, Contract Logistics, Digital B2b, Digital Content, Digital Identity, Digital Thinking for Business, Digital Transformation Academy, Droni, eCommerce B2c, eGovernment, Export Digitale, Fintech & Insurtech, Food Sustainability, Gioco Online, HR Innovation Practice, Industria 4.0, Information Security & Privacy, Innovative Payments, Innovazione Digitale in Sanità, Innovazione Digitale nei Beni e Attività Culturali, Innovazione Digitale nel Retail, Innovazione Digitale nel Turismo, Innovazione Digitale nelle PMI, Internet Media, Internet of Things, Kids & Toys, Mobile B2c Strategy, Multicanalità, Omnichannel Customer Experience, Professionisti e Innovazione Digitale, Smart & Connected Car, Smart Agrifood, Smart Working, Startup Hi-tech, Startup Intelligence, Supply Chain Finance, Tech Company - Innovazione del Canale ICT.*