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

COMUNICATO STAMPA

Osservatorio Information Security & Privacy

CRESCE IL MERCATO DELL'INFORMATION SECURITY: 1,19 MILIARDI DI EURO NEL 2018, +9%

GDPR: UN QUARTO DELLE IMPRESE E' PRONTO, L'88% HA UN BUDGET DEDICATO

Il 75% della spesa si concentra fra le grandi imprese, trainata dai progetti di adeguamento al GDPR e dalle componenti più tradizionali della cyber security. PMI ancora indietro: solo il 18% si trova a un livello maturo

Il 23% delle imprese si è già adeguata al GDPR, il 59% ha progetti in corso, l'88% ha un budget dedicato. Boom del Data Protection Officer, presente nel 71% delle imprese (+46%). Il 59% ha inserito un Chief Information Security Officer

Truffa, estorsione, spionaggio e interruzione di servizio le principali finalità dei cyber attacchi. I principali obiettivi sono account email e social, portali eCommerce e siti web

Milano, 5 febbraio 2019 – Il numero dei cyber attacchi cresce esponenzialmente con minacce sempre nuove e le imprese italiane aumentano gli investimenti sulla prevenzione dei rischi, ma faticano ad adattarsi alla rapida evoluzione delle modalità di aggressione. Il mercato italiano delle soluzioni di information security & privacy nel 2018 continua a crescere, raggiungendo il valore di 1,19 miliardi di euro, in crescita del 9% (dopo il +12% fatto registrare nel 2017). A trainare il mercato sono soprattutto le grandi imprese, con il 75% della spesa complessiva, concentrata su adeguamento al GDPR e componenti di sicurezza più tradizionali (come *Network Security*, *Business Continuity & Disaster Recovery*, *Endpoint Security*). Il 63% delle grandi imprese ha aumentato il budget per la cyber sicurezza e nel 52% è presente un piano di investimenti pluriennale, anche se ancora quasi una su cinque non prevede ancora investimenti dedicati o stanzia risorse solo in caso di necessità.

Per l'adeguamento alla normativa europea sulla protezione dei dati l'88% delle imprese ha dedicato uno specifico budget nel 2018 (era il 58% un anno fa). Quasi un'impresa su quattro ha già completato il processo di adeguamento al GDPR, mentre il 59% ha progetti strutturati ancora in corso. Con gli investimenti aumentano le figure professionali dedicate: il Data Protection Officer oggi è presente nel 71% delle imprese (+46%), il Chief Information Security Officer nel 59%, mentre sono sempre di più i profili emergenti come il Cyber Risk Manager, l'Ethical Hacker e il Machine Learning Specialist. Cresce l'attenzione per nuove tecnologie come l'Artificial Intelligence, considerata una minaccia da appena il 14% delle imprese, mentre il 40% già la impiega per prevenire potenziali minacce e frodi e gestire la risposta a incidenti di sicurezza. E nascono attori innovativi che propongono soluzioni di information security & privacy: sono 417 le startup a livello internazionale, per un totale di 4,75 miliardi di dollari di investimenti raccolti.

Le principali finalità dei cyber attacchi subiti dalle imprese nello scenario attuale sono truffe, come phishing e business email compromise (83%), e estorsioni (78%), poi intrusione a scopo di spionaggio (46%) e interruzione di servizio (36%). Ma nei prossimi tre anni le aziende temono soprattutto spionaggio (55%), truffe (51%), influenza e manipolazione dell'opinione pubblica (49%), acquisizione del controllo di sistemi come impianti di produzione (40%). I principali obiettivi degli attacchi sono oggi account email (91%) e social (68%), seguiti dai portali eCommerce (57%) e dai siti web (52%). Nel prossimo triennio, le imprese prevedono che gli hacker si concentreranno su device mobili (57%), infrastrutture critiche come reti elettriche, idriche e di telecomunicazioni (49%), smart home & building (49%) e veicoli connessi (48%). La principale vulnerabilità è costituita dal comportamento umano: per l'82% delle imprese la prima criticità è la distrazione e scarsa consapevolezza dei dipendenti, seguita da sistemi IT obsoleti o eterogenei (41%) e da aggiornamenti e patch non effettuati regolarmente (39%). Per minimizzare il rischio, l'80% delle imprese ha avviato piani di formazione del personale.

Sono alcuni dei risultati della ricerca dell'**Osservatorio Information Security & Privacy della School of Management del Politecnico di Milano***, presentata questa mattina al convegno *"Winter is coming: adapt to react"*. "Il mercato delle soluzioni per la sicurezza informatica e la privacy è dinamico, con consapevolezza e budget in crescita, anche se non con lo stesso ritmo del 2017 – afferma **Gabriele Faggioli**, Responsabile Scientifico dell'Osservatorio Information Security & Privacy -. Ma allo stesso tempo si registra un'accelerazione senza precedenti del numero e della varietà degli attacchi e le imprese non sembrano

adeguatamente preparate. Gli investimenti effettuati negli ultimi anni sono una buona base di partenza, che ha permesso di mettere in campo strutture organizzative, procedure e competenze, ma è necessaria una maggiore pervasività delle iniziative di sicurezza a tutti i livelli manageriali e organizzativi delle imprese e un maggiore coinvolgimento dei profili dedicati alla security nelle strategie di business".

"Oggi per le organizzazioni è necessario adattarsi al cambiamento per evitare di venirne travolte – dichiara **Alessandro Piva**, Direttore dell'Osservatorio Information Security & Privacy -. Siamo di fronte a un processo dirompente per quanto riguarda la gestione della sicurezza, che porrà nei prossimi mesi e anni sfide rilevanti. Le organizzazioni sono chiamate a internalizzare meccanismi di adattamento e a sviluppare regole istintive, da affiancare a strumenti, processi e competenze, per affrontare questa sfida e reagire in modo proattivo alle minacce che si troveranno ad affrontare".

I DATI DELLA RICERCA

Il mercato dell'Information Security – Il 75% della spesa in soluzioni di Information Security & Privacy riguarda le grandi imprese. Soltanto il 7% di queste dichiara di aver diminuito il budget dedicato nel corso dell'ultimo anno, il 63% lo ha aumentato (contro il 75% del 2017) e il restante 30% lo ha mantenuto stabile. Oltre metà delle grandi aziende (52%) dedica alla cyber security un piano di investimenti pluriennale, che nel 23% dei casi è anche inserito nel piano industriale, mentre il 30% pianifica gli investimenti su base annua. Nonostante il quadro positivo, però, quasi un'azienda su cinque è ancora indietro: il 13% non prevede un piano di investimenti specifico dedicato all'information security e privacy e il 6% stanzia finanziamenti solo in caso di necessità. Le principali voci di spesa riguardano l'adeguamento al GDPR, che per il secondo anno consecutivo incide in maniera netta sui budget delle aziende, e le componenti di sicurezza più tradizionali come la *Network Security*, strumenti di *Business Continuity & Disaster Recovery* e soluzioni di *Endpoint Security*, seguiti da *Application Security* e *Penetration Test*. Ma guardando al futuro, gli ambiti in cui le imprese dichiarano di voler aumentare i propri investimenti sono invece le componenti più innovative, come *Cloud Security* (sul quale il 71% delle organizzazioni dichiara di prevedere un aumento di budget), *Industrial Security* (52%), *Artificial Intelligence & Machine Learning* (50%), e protezione in ambiti *Mobile* (47%) e *IoT* (47%).

L'impatto di AI e IoT sulla sicurezza – L'Osservatorio ha approfondito le sfide di sicurezza poste dall'Internet of Things e dall'Artificial Intelligence. Le principali criticità legate all'IoT sono la mancanza di una logica di security by design (indicata dal 73% delle imprese), la scarsa consapevolezza da parte degli utenti sulle possibili problematiche legate a questi dispositivi (58%) e l'assenza di standard tecnologici e di sicurezza (53%). Se si restringe il campo all'ambito dell'Industrial Security, le principali sfide da superare sono la mancanza di consapevolezza delle problematiche di sicurezza da parte delle funzioni Operations (56%), l'interconnessione sempre maggiore tra gli impianti industriali e l'infrastruttura IT (55%), l'obsolescenza degli impianti industriali (40%) e la mancanza di figure con adeguate competenze (37%).

L'Artificial Intelligence è vista invece più come un'opportunità che una sfida. Soltanto il 14% del campione ritiene possa costituire una minaccia, soprattutto a causa dell'inaffidabilità delle macchine nel lungo periodo e della possibilità di utilizzarla per condurre attacchi mirati, mentre il 64% crede che sia utile per automatizzare il processo di raccolta e analisi dei dati per identificare in ottica preventiva eventuali minacce e vulnerabilità e il 17% per prendere decisioni in supporto o al posto dell'uomo. Un interesse che si traduce in progetti concreti, con il 40% delle imprese che già oggi sta utilizzando tecniche di AI o Machine Learning per prevenire potenziali minacce e identificare gli attacchi ancora prima che si verifichino (17%), per ottimizzare la gestione di eventuali incidenti di sicurezza automatizzando il processo decisionale e il tempo di risposta (15%) e per intercettare possibili frodi (8%). Il 36% del campione sta pianificando di adottare soluzioni di intelligenza artificiale nel prossimo futuro.

L'adeguamento al GDPR – Il 23% delle imprese è già conforme ai requisiti del GDPR, mentre il 59% ha ancora in corso progetti strutturati di adeguamento. Le imprese che dichiarano una scarsa conoscenza della normativa sono scese al 10% (dal 16% del 2017) e quelle che si trovano ancora in fase di analisi dei requisiti e delle attività da mettere in campo sono calate all'8% (dal 34%). Insieme alla consapevolezza e alle iniziative sono cresciute anche le risorse stanziate dalle imprese in misure di adeguamento al GDPR: un budget dedicato è presente nell'88%, trenta punti in più rispetto al 2017. Due aziende su tre (67%) prevedono un budget anche per le attività di mantenimento dei progetti di adeguamento normativo, come gli audit periodici, la revisione del registro dei trattamenti e l'aggiornamento delle procedure e delle tecnologie di sicurezza e protezione dei dati; nel 25% del campione tale budget verrà predisposto nei prossimi dodici mesi. Poco più della metà (51%) delle imprese ha inoltre risorse dedicate alla gestione di eventuali incidenti di

sicurezza, che comprendono i costi di notifica del data breach all'Autorità e agli interessati, come previsto dal Regolamento.

Le difficoltà riscontrate con più frequenza dalle imprese nell'adeguamento al GDPR riguardano la raccolta e mappatura dei dati personali (52%), la mancanza di sensibilizzazione sul tema da parte dei dipendenti aziendali (38%), la scarsa sponsorizzazione da parte del Top Management (37%), le difficoltà di comprensione della normativa (27%), la mancanza di figure professionali competenti sull'argomento (23%), la mancanza o la non adeguatezza del budget stanziato (20%) e l'inefficacia delle soluzioni tecnologiche di protezione e delle iniziative organizzative (20%).

"Il quadro dell'adeguamento delle imprese al GDPR è sostanzialmente positivo, con sensibilità, budget e acquisizione di competenze in deciso aumento – commenta **Gabriele Faggioli** -: nel 63% delle organizzazioni è aumentata la sensibilità dei Top Manager sul tema della protezione dei dati; più della metà ha introdotto corsi di formazione su sicurezza e privacy per i dipendenti, il 47% delle imprese ha effettuato investimenti in tecnologie, mentre il 34% ha inserito in organico nuove figure professionali specializzate".

Il CISO, il DPO e i nuovi ruoli emergenti – Le aziende stanno cercando di acquisire e potenziare le competenze specializzate in sicurezza e privacy. Il 41% delle grandi imprese analizzate prevede un aumento dell'organico dedicato alla gestione della security, il 2% una diminuzione, il resto lo manterrà invariato. Sul fronte privacy, invece, il 38% inserirà nuovi profili e soltanto l'1% li ridurrà. Il 2018 ha registrato un boom del Data Protection Officer (DPO): questo profilo è stato formalizzato nel 65% delle imprese ed è stato inserito informalmente nel 6%, con una crescita del 46% rispetto al 2017, mentre è calata di conseguenza la percentuale di aziende che ha intenzione di introdurlo in futuro (dal 57% al 5%) e delle imprese che non ne prevedono l'introduzione (dal 15% a 6%); il 18% delega queste mansioni a una figura esterna.

Meno rapida la diffusione del Chief Information Security Officer (CISO), presente formalmente nel 47% delle aziende, informalmente nel 12% e di prossima introduzione nel 2% del campione. Nel 37% delle aziende non esiste una figura dedicata e sono il Chief Information Officer (30%) o funzioni diverse dall'ICT (7%) a occuparsi del presidio della cyber security, mentre l'8% si affida a una figura che si occupa sia di sicurezza fisica sia di sicurezza logica. Anche nelle aziende che hanno inserito il CISO, però, la situazione non è rosea: solo nell'8% dei casi il CISO riporta direttamente al Board aziendale, nel 60% fa parte della direzione ICT e riporta al CIO, nel 10% il CISO riporta ad una funzione Security Corporate (che si occupa di sicurezza sia fisica sia logica), nel 3% alla funzione Compliance e Legal, nel 2% Risk Management oppure Operations.

Le altre figure professionali specializzate in security più diffuse in azienda sono il S*ecurity Administrator (*a cui ricorre, con figure interne o consulenti esterni, l'86% del campione) che si occupa di rendere operative le soluzioni tecnologiche di security, il *Cyber Risk Manager* (79%), che identifica gli scenari di rischio e le minacce informatiche, e il *Security Analyst* (78%), che valuta le vulnerabilità di reti e servizi aziendali. Seguono l'*Ethical Hacker* (76%), la cui mansione è simulare incidenti di sicurezza per testare le vulnerabilità di cui soffre l'azienda, il *Security Architect* (65%), che verifica le soluzioni e le policy di security presenti in azienda, e il *Security Engineer* (61%), che monitora i sistemi e risponde agli incidenti. Ci sono poi il *Security Developer* (51%), impegnato nello sviluppo di soluzioni di security specifiche, e il *Machine Learning Specialist* (32%), che sviluppa sistemi di risposta in tempo reale per trattare possibili minacce in modo automatico e cognitivo.

L'assicurazione del rischio cyber – Il mercato dell'assicurazione del rischio cyber prevede oggi svariate possibilità di copertura riguardanti la perdita o la divulgazione di dati personali e sensibili, la compromissione del sistema informativo e la sua interruzione di servizio. "A livello internazionale è un settore già molto radicato, mentre in Italia si trova ancora in una fase di sviluppo, seppure in crescita rispetto alla precedente rilevazione – commenta **Alessandro Piva** -. Il 33% delle imprese ha sottoscritto coperture assicurative di trasferimento del rischio cyber (+6%), di cui il 18% che ha scelto polizze completamente dedicate al cyber risk e il 15% che ha optato per assicurazioni generaliste che lo coprono parzialmente. Il 25% sta valutando se attivarle, il 30% è informato della possibilità ma non ha intenzione di farne uso, mentre il 12% non ne è a conoscenza". Gli ostacoli che rallentano la crescita del mercato assicurativo sono in primo luogo la difficoltà a misurare l'impatto finanziario di un eventuale incidente di sicurezza (64%) e l'incapacità delle aziende di valutare la propria esposizione ai rischi cyber (58%). Seguono lo scarso coinvolgimento dei Top Manager (30%) e la poca predisposizione delle imprese a sostenere un assessment del rischio cyber (19%). Ci sono infine lacune nell'offerta assicurativa, come la mancanza di trasparenza nella definizione dei danni coperti dalle polizze (19%) e la ancora scarsa competenza tecnica degli assicuratori (19%).

Le PMI – Le piccole e medie imprese coprono soltanto il 25% della spesa in soluzioni di information security. Il 43% investe in sistemi di information security & privacy, con i progetti di adeguamento al GDPR come principale motivazione di spesa (70%). Circa nove su dieci hanno adottato soluzioni di sicurezza informatica di base, mentre le tecnologie più sofisticate (quali ad esempio Intrusion Detection e Identity & Access Management) sono adottate dal 64% delle medie imprese (+20%) e dal 39% delle piccole. Il CISO è una figura ancora scarsamente diffusa nelle PMI, presente solo nel 15% del campione (nel 25% se ci si focalizza sulle medie imprese, +15%).

Oltre la metà del campione (il 52%) non si sta ancora muovendo sul fronte della cyber sicurezza, adotta al massimo soluzioni di base e non ha inserito profili specializzati su questi temi. Una piccola parte, l'8%, è consapevole dei rischi legati al cyber crimine e affida la sicurezza a figure della funzione IT, ma non adotta sistemi sofisticati per mancanza di budget. Più di una su cinque (22%) ha adottato soluzioni tecnologiche avanzate, ma non è ancora strutturata a livello di ruoli e competenze. Chiude un 18% di imprese mature sia dal punto di vista organizzativo (una su quattro ha un CISO) sia per strumenti adottati (una su tre ha attivato una polizza di trasferimento del rischio cyber).

Le startup – Sono 417 le startup a livello internazionale censite dall'Osservatorio, fondate dal 2013 e che hanno ricevuto almeno un finanziamento nell'ultimo biennio. Fra queste sono 357 le nuove imprese di cui è stato tracciata l'entità dei finanziamenti ricevuti, pari a 4,75 miliardi di dollari, circa 13,3 milioni a startup. Il Nord America è l'area con più nuove imprese (60%), seguito da Europa (22%) e Asia (15%). Il primo paese per numero di startup sono gli Stati Uniti (244), seguiti da Israele (48) e Regno Unito (38). Quasi metà delle startup censite rientra nella categoria "Enterprise Solution Security" (48%) e offre soluzioni di Identity & Access Management, applicazioni security-by-design e protezione dei dati aziendali o dell'utenza. Segue "Security Foundation", col 40% delle nuove imprese, attive nell'offerta di sistemi di protezione della rete e degli endpoint, di rilevamento delle minacce e risposta a incidenti. Il 12% delle startup, infine, appartiene alla categoria "Security Governance" e propone strumenti di tutela della privacy, polizze assicurative e formazione sulla cyber security. Le startup più finanziate sono quelle di "Security Foundation", con investimenti pari in media a 14,3 milioni di euro, seguite dal gruppo "Enterprise Solution Security", con 13,7 milioni a startup, e dalla categoria "Security Governance", con in media 13,6 milioni.

*L'edizione 2018 dell'Osservatorio Information Security & Privacy è realizzata con il supporto di Assolombarda, CAST, Enel, Fastweb, Leonardo, Lutech, Marsh, Poste Italiane, Spike Reply, TESISQUARE©; ABB, Informatica, Microsoft, Nodes; Aizoon, Axa XL, Generali, Nido Group, RSM; con il supporto di Cefriel e DEIB; e con il patrocinio di Clusit e ANRA.

Ufficio stampa Osservatori Digital Innovation del Politecnico di Milano

Barbara Balabio
Tel.: 02 2399 9578
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 attivita della School of Management legate all'Innovazione Digitale si articolano in Osservatori Digital Innovation, che fanno capo per le attivita 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 è 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 30 differenti Osservatori che affrontano i temi chiave dell'Innovazione Digitale nelle Imprese (anche PMI) e nella Pubblica Amministrazione: Agenda Digitale, Artificial Intelligence, Big Data

Analytics & Business Intelligence, Blockchain & Distributed Ledger, Cloud Transformation, Cloud nella PA, Contract Logistics, Digital Thinking for Business, Digital Transformation Academy, eCommerce B2c, eGovernment, Export, Fatturazione Elettronica & eCommerce B2b, Fintech & Insurtech, Food Sustainability, Gestione Progettazione e PLM (GeCo), Gioco Online, HR Innovation Practice, Industria 4.0, Information Security & Privacy, Innovazione Digitale in Sanità, Innovazione Digitale nei Beni e Attività Culturali, Innovazione Digitale nel Retail, Innovazione Digitale nel Turismo, Innovazione Digitale nell'Industria dello Sport, Internet Media, Internet of Things, Kids & Toys, Mobile B2c Strategy, Mobile Banking, Mobile Payment & Commerce, Multicanalità, Omnichannel Customer Experience, Professionisti e Innovazione Digitale, Smart Agrifood, Smart Working, Startup Hi-tech, Startup Intelligence, Supply Chain Finance, Tech Company - Innovazione nel Canale ICT.