COMUNICATO STAMPA

Osservatorio Cybersecurity & Data Protection

IL MERCATO DELLA CYBERSECURITY VALE 1,37 MILIARDI DI EURO, +4%

CRESCONO GLI ATTACCHI CYBER PER IL 40% DELLE IMPRESE

Nell'anno dell'emergenza sanitaria il mercato ha retto: il 40% delle grandi imprese ha aumentato il budget in cybersecurity (51% nel 2019), il 19% lo ha ridotto (2% l'anno prima)

Il 52% della spesa dedicato a soluzioni di security, il 48% ai servizi. Network & Wireless Security, Endpoint Security e Data Security sono le tipologie di sicurezza che attirano più risorse

Gestione della cybersecurity ancora poco matura: solo nel 41% c'è un CISO. Il Data Protection Officer presente nel 69% delle realtà, il resto si affida a figure esterne

Milano, 3 febbraio 2021 – Il 2020 è stato un anno di emergenza anche sul fronte della cybersecurity. Per il 40% delle grandi imprese sono aumentati gli attacchi informatici rispetto all'anno precedente. La diffusione improvvisa e capillare del remote working e del lavoro agile, l'uso di dispositivi personali e reti domestiche e il boom delle piattaforme di collaborazione hanno infatti aumentato le opzioni di attacco a disposizione degli attaccanti. L'impatto economico della pandemia ha costretto le imprese italiane a fronteggiare le aumentate sfide di sicurezza con budget ridotti: il 19% ha diminuito gli investimenti in cybersecurity (contro il 2% del 2019) e solo il 40% li ha aumentati (era il 51% l'anno precedente). Ma per oltre un'impresa su due (54%) l'emergenza è stata un'occasione positiva per investire in tecnologie e aumentare la sensibilità dei dipendenti riguardo alla sicurezza e alla protezione dei dati.

Nel complesso, la crisi legata al Covid19 ha rallentato la crescita del mercato della cybersecurity ma non l'ha fermata. Nel 2020 la spesa in soluzioni di cybersecurity ha raggiunto un valore di 1,37 miliardi di euro, in crescita del 4% rispetto all'anno precedente (nel 2019 il mercato aveva segnato un +11% rispetto al 2018), di cui il 52% è rappresentato dalle soluzioni di security e il 48% dai servizi. Gli investimenti in cybersecurity sono legati principalmente alla gestione dell'emergenza, come testimonia la crescita della spesa in Endpoint Security. Cloud, Smart Working e Big Data sono i trend del digitale che hanno maggiormente influenzato la gestione della sicurezza negli ultimi dodici mesi. Degni di nota anche Operational Technology (OT) Security, che riscontra un'accelerazione degli investimenti, e Artificial Intelligence, utilizzata in ambito cybersecurity dal 47% delle aziende.

Nonostante un mercato in crescita e il ruolo sempre più strategico della cybersecurity, le imprese presentano ancora una scarsa maturità organizzativa. Solo nel 41% la responsabilità della sicurezza informatica è affidata a un CISO e ancora nel 38% dei casi non è prevista nessuna comunicazione al Board sull'argomento. La gestione della data protection è più evoluta, anche per effetto della spinta normativa, con il 69% delle imprese che ha inserito un Data Protection Officer (DPO) in organico e il resto che si avvale di figure esterne.

Sono i risultati della ricerca **dell'Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano***, presentata oggi durante il convegno online "*Cybersecurity Odyssey: la chiave per evolvere*".

"Il 2020 è stata una vera e propria odissea, con un aumento senza precedenti degli attacchi informatici, la necessità di riorganizzarsi per gestire l'improvviso boom dello smart working e la razionalizzazione del budget a disposizione per affrontare le sfide di sicurezza a causa del grave impatto economico della pandemia – afferma **Alessandro Piva**, Direttore dell'Osservatorio Cybersecurity & Data Protection -. Nonostante il contesto negativo, il mercato non ha smesso di crescere e la maggior parte delle imprese ha colto l'occasione per investire, rinnovarsi e aumentare la sensibilità dei dipendenti sul tema. La cybersecurity può essere la chiave per evolvere e gestire i cambiamenti in atto, ma deve essere gestita in modo più maturo e strategico".

"Anche nel 2020, nonostante l'emergenza sanitaria, sono stati fatti importanti passi avanti nell'ambito cybersecurity – afferma **Gabriele Faggioli**, Responsabile scientifico dell'Osservatorio Cybersecurity & Data Protection -. Il mercato italiano della cybersecurity, però, è ancora limitato in rapporto al PIL, con un'incidenza di appena lo 0,07% nel 2019, circa 4-5 volte in meno rispetto ai paesi più avanzati. E dalla ricerca emerge anche la necessità di rafforzare il presidio delle normative, anche considerando le sanzioni comminate dalle Autorità competenti e gli importanti data breach di cui si ha avuto notizia nel corso dell'anno".

Il mercato della cybersecurity – La tipologia di sicurezza che attira la maggior parte degli investimenti è la

Network & Wireless Security (33%), le strategie e le soluzioni che proteggono l'infrastruttura da danni e accessi impropri. Seguono la Endpoint Security (23%), ovvero la protezione di ciascun dispositivo connesso alla rete, e la Data Security (14%), i sistemi per la protezione dei dati dell'azienda e dei singoli utenti. La sicurezza degli ambienti Cloud vale il 13% della spesa, la Application Security il 12%, mentre è ancora marginale la IoT security (3%). Infine, vi è un'ulteriore categoria residuale che occupa il restante 2%, in cui rientrano principalmente le iniziative di cybersecurity awareness e training.

La spesa si divide quasi a metà fra le soluzioni di security, col 52% del mercato, e i servizi professionali e gestiti, col 48%. Le soluzioni su cui le aziende investono maggiormente sono sistemi per il monitoraggio degli eventi di sicurezza (16%), per gestire e monitorare l'accesso degli utenti a dati e applicazioni (14%), per valutare la vulnerabilità e la sicurezza di sistemi, applicazioni o reti (14%), per analizzare l'esposizione al rischio cyber dei sistemi aziendali e valutarne la conformità agli standard di sicurezza (12%) e soluzioni che monitorano il traffico di rete per identificare e bloccare accessi non autorizzati (11%). Fra i servizi, il 51% della spesa è dedicato ai Professional Services, i servizi offerti da fornitori esterni all'azienda per un progetto specifico, mentre il 49% riguarda i Managed Services, i servizi offerti in modo continuativo da fornitori esterni per la manutenzione dei sistemi informativi aziendali.

I trend in ambito cybersecurity e data protection – Il Cloud è il trend che più ha influenzato la gestione della cybersecurity nelle imprese, insieme allo Smart Working e ai Big Data. Nell'ultimo anno sono emersi servizi Cloud di tipo edge, che estendono i confini della nuvola, ma le aziende lamentano ancora scarsa consapevolezza delle minacce da parte del top management (74%), un aumento degli attacchi più evidente rispetto ad altri ambiti (64%) e difficoltà a relazionarsi con i cloud service provider perché hanno poco potere negoziale (74%) o faticano a fare security assessment (66%).

Fra le altre tendenze più rilevanti, l'accelerazione degli investimenti in OT security, a cui però non si accompagna un'adeguata maturità: solo un'impresa su due ha introdotto policy di OT security e meno di un terzo prevede attività di formazione specifiche sulla materia. L'Artificial Intelligence si conferma un tema di interesse per le aziende, che la impiegano in ambito cybersecurity nel 47% dei casi (ma solo nel 14% in modo significativo) soprattutto per identificare nuove minacce (68%) e per il monitoraggio del comportamento di sistemi e utenti al fine di rilevare anomalie (66%). Cresce anche l'importanza della Supply Chain security, le attività di protezione dei sistemi e delle reti di terze parti, ma finora solo il 13% del campione ha messo in campo strumenti tecnici e predisposto un presidio organizzativo formale.

Le competenze di security e data protection – La gestione della cybersecurity e della data protection richiede profili e competenze specifiche. Per quanto riguarda l'area della sicurezza informatica, la situazione non ha registrato cambiamenti evidenti nell'ultimo anno: solo nel 41% delle imprese la responsabilità è affidata ad un CISO formalizzato, nel 25% è in capo al CIO, nel 13% ad un CSO o security manager, mentre nei restanti casi è in mano ad un'altra figura aziendale (19%) o non esiste una figura dedicata (2%). Nel 38% delle organizzazioni analizzate non è prevista una relazione periodica al CdA da parte della figura responsabile della sicurezza sulle azioni messe in campo.

La data protection è gestita in modo più avanzato, con il DPO presente nell'organico del 69% delle imprese e come figura esterna nel resto del campione. Nel 51% dei casi tale figura riporta direttamente al board e nel 52% dispone di un budget dedicato (+9% sul 2019).

Le PMI – Le realtà più piccole hanno faticato ad adeguarsi ai nuovi modelli di organizzazione del lavoro imposti dall'emergenza. Secondo il 59% delle PMI intervistate dall'Osservatorio, l'uso di device personali e reti domestiche ha esposto le aziende a maggiori rischi di sicurezza, e per il 49% sono aumentati gli attacchi informatici. Sebbene la cybersecurity inizi a farsi strada tra le priorità, le PMI faticano ancora a tradurre la percezione in concretezza: solo il 22% ha previsto investimenti in sicurezza per il 2021, il 20% li aveva previsti ma ha dovuto ridurre il budget in seguito all'emergenza, un terzo non ha un budget da dedicare (32%) e oltre un quarto non è interessato all'argomento.

Chi investe si concentra soprattutto sulla componente tecnologica: il 41% intende investire in soluzioni di sicurezza di base, come antivirus o firewall, il 37% guarda a soluzioni più sofisticate, come sistemi di Intrusion Detection o Identity & Access Management. Per quanto riguarda la gestione della cybersecurity, il 32% del campione ha investito in formazione su sicurezza e data protection ai dipendenti, il 28% si è rivolto a consulenti per migliorare la gestione della cybersecurity in azienda, il 18% ha introdotto competenze dedicate come Security Analyst o Security Administrator e il 15% ha stipulato polizze assicurative per il trasferimento del

rischio cyber.

Il quadro normativo e la sfida della compliance – Il quadro normativo europeo in materia di data protection e cybersecurity si è evoluto negli ultimi anni, con l'entrata in vigore, in particolare, del GDPR, della direttiva NIS e del Cybersecurity Act. Alla fine del 2020 la Commissione europea ha pubblicato un nuovo pacchetto di misure per realizzare un piano strategico sulla cybersecurity per i prossimi cinque anni, aumentare la resilienza di reti e infrastrutture e contrastare il cybercrime. In Italia è stato adottato il "Perimetro di sicurezza nazionale cibernetica".

Ci sono però ancora molte sfide da affrontare per imprese e istituzioni, a partire dal rafforzamento della compliance. Un'altra sfida "cruciale" è quella che riguarda il difficile rapporto tra innovazione tecnologica e data protection. In un'era volta alla digitalizzazione e al progresso tecnologico è necessario bilanciare saggiamente le opportunità offerte dalle nuove tecnologie con gli strumenti di tutela messi a disposizione dal framework normativo in materia di protezione dei dati: la trasformazione digitale e l'innovazione tecnologica, in assenza di adeguate misure di intervento, produrrebbero effetti negativi senza apportare alcun beneficio.

*L'edizione 2020/21 dell'Osservatorio Cybersecurity & Data Protection è realizzata con il supporto di Accenture, Assolombarda, BlackBerry, CAST Italia, Forcepoint – Project Informatica, Lutech Group, Microsoft, Poste Italiane, RAI, Spike Reply, Vodafone Business; CyberArk, Huawei, Konica Minolta, Splunk, Var Group, Yarix; Aditinet Consulting, AXA XL, CrowdStrike, CryptoNet Labs, F-Secure, Orange Business Services; con la collaborazione di Cefriel e Politecnico di Milano Dipartimento di Elettronica, Informazione e Bioingegneria; e con il patrocinio di ANRA, Assintel 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

*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 oltre 100 tra professori, ricercatori e analisti impegnati su più di 40 differenti Osservatori che affrontano i temi chiave dell'Innovazione Digitale nelle Imprese (anche PMI) e nella Pubblica Amministrazione: 5G & Beyond, Agenda Digitale, Artificial Intelligence, Big Data & Business Analytics, Blockchain & Distributed Ledger, Business Travel, Climate Finance, Cloud Transformation, Cloud nella PA, Connected Car & Mobility, Contract Logistics "Gino Marchet", Cybersecurity & Data Protection, Design Thinking for Business, Digital B2b, Digital Content, Digital Identity, Digital Transformation Academy, Droni, eCommerce B2c, eGovernment, Export Digitale, Fintech & Insurtech, Food Sustainability, HR Innovation Practice, 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, Mobile B2c Strategy, Multicanalità, Omnichannel Customer Experience, Professionisti e Innovazione Digitale, Smart AgriFood, Smart Working, Space Economy, Startup Hi-tech, Startup Intelligence, Supply Chain Finance, Sustainable & Digital Beauty, Tech Company - Innovazione del Canale ICT, Transizione Industria 4.0.*