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

COMUNICATO STAMPA

Osservatorio Information Security & Privacy

CRESCE L'ATTENZIONE PER LA SICUREZZA, MA LE MINACCE DIGITALI VIAGGIANO TROPPO VELOCI

Mentre esplodono le minacce di Cybercrime, solo un quinto delle grandi imprese ha definito strategia e piani concreti sull'information security. Aumenta la consapevolezza sulla gestione la sicurezza e cresce del 7% il budget medio delle aziende, ma le scelte di spesa sono influenzate soprattutto da obblighi normativi. Ancora limitati gli investimenti di security in ambiti emergenti del digitale come cloud e mobile.

Un terzo delle aziende ha subito perdita o furto di dati negli ultimi 12 mesi. Le principali fonti di attacco sono esterne come le associazioni criminali, seguite da quelle interne degli stessi lavoratori. Malware, phishing, spam, attacchi ransomware e frodi le minacce più diffuse.

È necessario definire ruoli manageriali per le strategie di sicurezza, ma solo il 42% delle grandi aziende si è già dotato di un Chief Information Security Officer. Solo il 21% ha formalizzato un Data Protection Officer per la gestione della privacy.

Milano, 29 gennaio 2016 - Cresce l'attenzione delle aziende sull'information security e la privacy, testimoniata da un aumento del 7% della spesa media dedicata negli ultimi mesi, con punte nei settori Media-Telco e Finance, seguiti da PA-Sanità, Utility e Servizi. Ma ad oggi solo il 19% delle grandi imprese dispone sia di consapevolezza e visione di lungo periodo sulla sicurezza, che di azioni e piani concreti con approcci tecnologici e ruoli organizzativi definiti, mentre il 48% è ad uno stadio iniziale di questo percorso. E così, mentre le minacce aumentano al ritmo del +30% nei primi 6 mesi del 2015 (dati Clusit), le strategie di information security faticano a tenere il passo dell'evoluzione delle tecnologie digitali e dei pericoli che ne possono derivare. Lo dimostrano le tipologie investimento delle aziende, che oggi si concentrano in particolare su ambiti come *network security* o *business continuity/disaster recovery* e ancora poco su trend emergenti del digitale come il mobile (priorità di investimento attuale nel 30% dei casi) e il cloud (7%), seppure riconosciuti di grande interesse in prospettiva.

Nell'86% delle imprese la consapevolezza dell'importanza di una gestione dell'information security & privacy è cresciuta negli ultimi 3 anni. E la conferma viene dalla pianificazione del budget, che prevede nel 74% dei casi un'allocazione formale con orizzonte annuale o pluriennale, solo nel 26% un'allocazione non definita in cui le risorse sono stanziate all'occorrenza. In ogni caso, nel 58% delle organizzazioni le scelte di allocazione del budget sono fortemente influenzate dalle normative vigenti negli specifici settori.

Le principali fonti di attacco riscontrate provengono da fonti esterne come le associazioni criminali (nel 58% dei casi) o gli hacktivist (46%), ma va riposta attenzione anche a quelle interne, come gli stessi lavoratori (49%) ed i consulenti aziendali (30%). Le minacce più diffuse negli ultimi due anni sono malware (80%), phishing (70%), spam (58%), attacchi ransomware (37%) e frodi (37%). Le principali vulnerabilità sono la consapevolezza dei collaboratori su policy e buone pratiche di comportamento (79%), la distrazione (56%), l'accesso in mobilità alle informazioni aziendali (45%), la presenza di dispositivi mobili personali (33%): per queste ragioni circa un terzo delle grandi aziende ha subito una perdita o un furto di dati negli ultimi 12 mesi, trafugando per lo più informazioni operative interne, price sensitive, informazioni sui clienti o sui pagamenti. In questo quadro emerge la necessità di ruoli di responsabilità manageriale per le strategie di information security: le organizzazioni si stanno attrezzando, ma oggi solo il 42% delle grandi aziende può dire di aver formalizzato al proprio interno una figura di Chief Information Security Officer (CISO).

Sono alcuni dei risultati della ricerca dell'**Osservatorio Information Security & Privacy** della School of Management del Politecnico di Milano (www.osservatori.net)* presentata questa mattina a Milano al convegno *"Digital Transformation: siamo al Sicuro?"*. La ricerca dell'Osservatorio, al suo primo anno di attività, ha coinvolto oltre 150 Chief Information Security Officer, Chief Security Officecer e Chief Information Officer di grandi aziende italiane per indagare il contesto di riferimento, il budget dedicato, le principali aree di investimento ed interesse, le minacce e le principali fonti di attacco ed i ruoli e

meccanismi di governance.

“Dalla ricerca emerge la consapevolezza della rilevanza di security e privacy tra le imprese italiane, ma anche la tendenza ad affrontare la tematica in modo ancora poco sistemico, mettendo a disposizione i budget necessari soprattutto sotto la spinta degli obblighi normativi – afferma **Gabriele Faggioli**, Responsabile scientifico dell'Osservatorio Information Security & Privacy –. Tra le aziende, risulta evidente il timore di attacchi che provengono anche dall’interno dell’azienda e dei rischi che discendono dalla scarsa cultura informatica del personale. Si nota sempre più anche il 'peso' delle tecnologie mobili che, sempre più diffuse, sono diventate un fattore rilevante di rischio. La trasformazione digitale delle imprese richiede oggi nuove tecnologie, modelli organizzativi, competenze e regole per garantire, insieme all’innovazione, la necessaria protezione degli asset informativi aziendali”.

“Nonostante il crescente interesse per l’information security, testimoniato dall'aumento pari al 7% del budget nelle grandi imprese, non è semplice maturare modelli in grado di rispondere all’innovazione digitale sempre più dirompente – dice **Alessandro Piva**, Direttore dell' Osservatorio Information Security & Privacy - significa sviluppare consapevolezza strategici e definire meccanismi organizzativi ed approcci tecnologici: ad oggi solo il 19% delle grandi aziende si può definire matura su entrambe queste linee di azione. Vi è poi la necessità di definire ruoli di responsabilità manageriale per pianificare e mettere atto la strategia di information security. Di fronte a queste sfide, per tenere il passo con l’evoluzione delle tecnologie digitali, la velocità con cui mettere in atto strategie e progetti diventa sempre più fondamentale”.

Chief Information Security Officer e Data Protection Officer

I modelli di governance dell’information security sono variegati e prevedono la presenza, spesso anche la coesistenza, di diversi meccanismi di coordinamento. Sono nel 42% delle grandi imprese è presente in modo formalizzato la figura del *Chief Information Security Officer* (CISO), il professionista incaricato di definire la visione strategica, implementare programmi a protezione degli asset informativi e mitigare i rischi, mentre nel 10% è prevista l’introduzione nei prossimi 12 mesi. Nel 36% dei casi il presidio dell’information security è demandato ad altri ruoli in azienda, come un responsabile della sicurezza (CSO). Nel restante 12% non esiste una figura dedicata e non ne è prevista l’introduzione nel prossimo anno.

L’aumento dei dati e l’eterogeneità delle fonti informative rendono necessarie anche figure professionali per la gestione dei problemi della privacy. Il nuovo regolamento europeo sulla protezione dei dati che sta vedendo la luce prevede la possibile introduzione del *Data Protection Officer* (DPO). Già presente in alcune legislazioni europee, è il professionista con competenze giuridiche, informatiche, di gestione del rischio e di analisi dei processi aziendali che mette in atto la politica di gestione del trattamento dei dati personali per adempiere alle normative di riferimento. La figura è già formalizzata solo nel 21% delle grandi imprese, mentre in un 33%, pur non esistendo il ruolo, la responsabilità è demandata ad altre funzioni, nel 16% sarà introdotta nei prossimi 12 mesi, nel restante 30% per il momento non sarà inserita.

Le policy

Le policy di gestione dell’information security & privacy più diffuse sono quelle relative al backup dei dati (86%) e degli accessi logici (83%), alla regolamentazione scritta delle policy di sicurezza informatica aziendali (80%), alla regolamentazione sull’utilizzo degli asset informativi aziendali (79%). Sono meno comuni invece quelle sulla gestione dei device mobili ed in materia di “bring your own device” (48%), di gestione del ciclo di vita del dato (47%), di criptazione dei dati (36%) e di gestione degli ambiti social e web (31%).

Nel 39% delle imprese non esiste un piano strutturato di formazione e comunicazione delle policy, negli altri casi la comunicazione delle policy viene inserita nel piano di formazione annuale obbligatorio (17%) o si prevede la formazione con specifici corsi interni (39%) o con l’ausilio di esperti esterni (5%).

I freni alla strategia di information security

L’elemento di maggior freno alla creazione di una strategia di information security evidenziato dalle aziende è di gran lunga la difficoltà di identificare costi e benedici derivanti dall’utilizzo di determinati approcci e tecnologie (60%), seguito dallo scarso committment del top management (38%) e dalla difficoltà a definire i confini d’azione (32%).

“Le barriere che impediscono oggi di creare una strategia di information security nelle imprese italiane sono

molto eterogenee, a testimonianza di situazioni molto differenti, ma si possono identificare alcune linee comuni di intervento – spiega **Mariano Corso**, Responsabile scientifico dell'Osservatorio Information Security & Privacy -. Da una parte è necessaria un'evoluzione dell'organizzazione per favorire la creazione di nuovi ruoli, meccanismi di coordinamento e competenze. Dall'altra si chiede un ripensamento delle metodologie di indagine dei confini della sicurezza, affiancando a logiche tradizionali nuove modalità di analisi per processi, per rispondere meglio ai trend emergenti del digitale che cambiano il normale perimetro di difesa. Infine, occorre sviluppare sensibilità alla gestione del rischio, pianificando interventi ed investimenti sulla base di scenari di priorità".

*L'edizione 2015 dell'Osservatorio Information Security & Privacy è realizzata con il supporto di AlmavivA, Poste Italiane, Symantec, Trend micro; Data Storage Security, Spike Reply & Communication Valley. In collaborazione con Cefriel e DEIB (Dipartimento di Elettronica, Informazione e Bioingegneria). Con il patrocinio di Clusit.

Ufficio stampa School of Management del Politecnico di Milano

Barbara Balabio
Tel.: 02 2399 9578
email barbara.balabio@polimi.it_
Skype barbara.balabio
www.osservatori.net

d'I Comunicazione:

Stefania Vicentini
sv@dicomunicazione.it
Mob.: 335 5613180

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

La School of Management del Politecnico di Milano, con oltre 240 docenti, e circa 80 fra dottorandi e collaboratori alla ricerca, dal 2003 accoglie le attività di ricerca, formazione e alta consulenza, nei campi management, economia e industrial engineering. Fanno parte della Scuola il Dipartimento di Ingegneria Gestionale, le Lauree e il PhD Program di Ingegneria Gestionale e il MIP, la business school del Politecnico di Milano. Nel 2007 ha ricevuto l'accreditamento EQUIS e dal 2009 è nella classifica del Financial Times delle migliori Business School d'Europa; nel Marzo 2013 ha ottenuto il prestigioso accreditamento internazionale da AMBA (Association of MBAs).
Gli Osservatori Digital Innovation della School of Management del Politecnico di Milano (www.osservatori.net) vogliono offrire una fotografia accurata e continuamente aggiornata sugli impatti che le tecnologie dell'informazione e della comunicazione (ICT) hanno in Italia su imprese, pubbliche amministrazioni, filiere, mercati ecc. Gli Osservatori sono ormai molteplici e affrontano in particolare tutte le tematiche più innovative: Agenda Digitale, Big Data Analytics & Business Intelligence, Canale ICT, Cloud & ICT as a Service, Cloud per la Pubblica Amministrazione, Digital & M&A, Digital Innovation Academy, eCommerce B2c, eGovernment, Enterprise Application Evolution, eProcurement nella PA, Export, Fatturazione Elettronica e Dematerializzazione, Gestione Progettazione e PLM, Gioco Online, HR Innovation Practice, ICT & PMI, ICT Accessibile e Disabilità, ICT nel Real Estate, Information Security & Privacy, Innovazione Digitale in Sanità, Innovazione Digitale nel Retail, Innovazione Digitale nel Turismo, Innovazione Digitale nelle Utility, Internet of Things, Intranet Banche, Mobile B2c Strategy, Mobile Banking, Mobile Economy, Mobile Enterprise, Mobile Payment & Commerce, Multicanalità, New Media & New Internet, Professionisti e Innovazione Digitale, Smart Manufacturing, Smart Working, Startup, Supply Chain Finance.