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

COMUNICATO STAMPA

Osservatorio Information Security & Privacy

CRESCE IL MERCATO DELL'INFORMATION SECURITY: 972 MILIONI DI EURO

MA IMPRESE ITALIANE IN RITARDO NELLA GESTIONE DI SICUREZZA E PRIVACY

Cresce la consapevolezza sulla sicurezza informatica, ma le minacce su Cloud, Big Data, Internet of Things, Mobile e Social richiedono nuovi modelli di organizzazione: solo il 39% delle grandi imprese ha un piano di investimento pluriennale, solo il 46% ha in organico un Chief Information Security Officer.

Quasi tutte le grandi imprese hanno azioni di sensibilizzazione~~re~~ sul comportamento dei dipendenti. Ma appena il 15% ha attivato assicurazioni sul rischio Cyber.

Milano, 2 febbraio 2017 - In quello che sarà ricordato come "l'anno dell'Hack", con la scoperta delle violazioni di 500 milioni di account Yahoo, le presunte azioni di cyberspionaggio durante le elezioni presidenziali americane, la crescita dei ransomware, l'attacco a uno dei principali DNS provider, cresce l'attenzione delle imprese italiane per la sicurezza informatica. Il mercato delle soluzioni di information security in Italia nel 2016 raggiunge i 972 milioni di euro, in crescita del 5% rispetto 2015, con una spesa concentrata tra le grandi imprese (74% del totale) suddivisa tra tecnologia (28%), servizi di integrazione IT e consulenza (29%), software (28%) e managed service (15%). Sebbene cresca la consapevolezza, di fronte alle nuove sfide poste dallo sviluppo di tecnologie come Cloud, Big Data, Internet of Things, Mobile e Social, non è ancora diffuso un approccio di lungo periodo alla gestione della sicurezza e della privacy, con una chiara struttura di governo: solo il 39% delle grandi imprese ha un piano di investimento con orizzonte pluriennale e solo il 46% ha in organico in modo formalizzato la figura del Chief Information Security Officer, il profilo direzionale a capo della sicurezza. Sono alcuni dei risultati della ricerca dell'**Osservatorio Information Security & Privacy della School of Management del Politecnico di Milano***, presentata questa mattina al convegno *"Cyber Crime: La minaccia invisibile che cambia il mondo"*.

"Il Cyber Crime è una minaccia concreta anche se spesso invisibile, in grado di condizionare il mondo, come dimostrano i quotidiani fatti di cronaca, che richiede nuovi~~e~~ strumenti e modelli per farvi fronte – afferma **Gabriele Faggioli**, Responsabile scientifico dell'Osservatorio Information Security & Privacy -. I nuovi trend dell'innovazione digitale come Cloud, Big Data, Internet of Things, Mobile e Social richiedono nuove risposte non più rimandabili. Il nuovo Regolamento europeo sulla Protezione dei Dati Personali crea alcuni dei presupposti necessari per giungere a un quadro di riferimento, che richiede però di essere compreso ed attuato. Il percorso di gestione dell'Information Security & Privacy chiede alle aziende di mettere in campo adeguati modelli di governance, progettualità e soluzioni per affrontare la trasformazione".

"Il mercato dell'information security in Italia nel 2016 vale 972 Milioni di Euro, con un tasso di crescita del 5% sul 2015, un valore importante che tuttavia non può tranquillizzarci – spiega **Alessandro Piva**, Direttore dell'Osservatorio Information Security & Privacy –. Se analizziamo più in profondità i dati della ricerca, infatti, ci rendiamo conto di come le grandi organizzazioni italiane siano ancora indietro: oltre la metà non ha ancora una figura manageriale codificata per la gestione della sicurezza informatica, evidenziando un gap importante rispetto a quanto avviene in altri Paesi. Inoltre si denota un ritardo nella comprensione delle implicazioni dei trend dell'innovazione digitale quali Cloud, IoT, Big Data, Mobile, sulla gestione della sicurezza. Nel contesto attuale, servono modelli di governance più maturi e trasversali, assicurando il corretto mix di competenze per gestire tecnologie sempre più pervasive. Ed è necessario da una parte progettare sistemi in grado di predire i possibili attacchi, dall'altra sviluppare programmi di sensibilizzazione per gli utenti, al fine di promuovere comportamenti responsabili".

I progetti - I progetti di sicurezza delle aziende italiane nella sicurezza sono orientati principalmente all'identificazione dei rischi e alla protezione dagli attacchi, mentre sono ancora immaturi il supporto alla rilevazione degli eventi e poi la risposta e il ripristino. I progetti più diffusi tra le grandi imprese

infatti sono i penetration test e la data security (51%), network security (48%), application security (45%), endpoint security (43%), security information & event management (SIEM) (38%), messaging security (38%), web security (36%), identity governance & administration (IGA) (32%), threat intelligence (20%), transaction security (19%), social media security (16%).

Le policy maggiormente presenti invece riguardano il backup (89%), la gestione degli accessi logici (84%), la regolamentazione delle policy di sicurezza informatica (80%), la gestione e l'utilizzo dei device aziendali (72%), la gestione del ciclo di vita del dato (58%), l'utilizzo di social media e web (57%), le azioni da mettere in atto in risposta agli incidenti informatici (52%), le policy di classificazione dei dati (52%) e di criptazione degli stessi (39%).

Chief Information Security Officer e Data Protection Officer - Sono poche le aziende che hanno definito una struttura di governo chiara della security. Solo nel 46% delle grandi imprese è presente in modo formalizzatoa la figura del Chief Information Security Officer, nel 12% è presente ma non formalizzata, nel 9% è prevista l'introduzione nei prossimi 12 mesi. Nei restanti casi non esiste una figura ed il presidio dell'information security è demandato direttamente al Chief Information Officer (28%) o a figure esterne all' ICT (5%). Il "ritardo" italiano si conferma focalizzando le organizzazioni dove il CISO è presente: nel 65% dei casi fa parte della direzione ICT, riportando al CIO, solo in un 10% dei casi riporta direttamente al board aziendale, nel resto riporta ad una funzione security corporate, a Rirsk management, operations, o in casi marginali a compliance, finance o altre strutture.

"La bontà di un piano strategico di gestione della security e della privacy passa, necessariamente, dal disegno di una struttura di governo chiara, identificando un Chief Information Security Officer - spiega **Gabriele Faggioli** –. Un ruolo che sta evolvendo verso un profilo completo, che affianca alle competenze tecnologiche e organizzative soft skill relazionali, conoscenze del dominio di business e capacità di sviluppare e governare un team complesso. Identificare il corretto mix delle competenze appena citate non è semplice e non è univocamente valido per tutte le situazioni: il ruolo ricoperto dal CISO può essere anche manageriale, di controllo e supervisione dalla gestione del rischio alla compliance e la privacy".

Nel 18% delle imprese è formalizzata invece la figura del Data Protection Officer, nel 15% è una presenza di tipo informale. Il 31% vuole introdurre nei prossimi 12 mesi, mentre il restante 34% afferma che per il momento non saranno inserite figure di questo tipo. Nel 2% dei casi la responsabilità è delegata ad una figura esterna dell'azienda.

Mobile – La quasi totalità delle aziende italiane (il 97%) mette a disposizione dei propri dipendenti device mobili, tra notebook, smartphone e tablet e mobile business app, con rischi non solo per il possibile furto o smarrimento dei dispositivi mobili, ma anche per i possibili attacchi cyber mirati. Il 74% delle imprese italiane ha iniziative specifiche per mitigare il rischio connesso alla Mobile Security, che riguardano sia l'introduzione di piattaforme e strumenti tecnologici specifici come soluzioni di MDM (Mobile Device Management) per limitare l'utilizzo di device mobili (61%), sia la definizione standardizzata e convenzionale di regole a cui gli utilizzatori di dispositivi devono attenersi quando accedono ai sistemi e ai dati business. Il 27% delle organizzazioni ha fissato norme che limitano l'accesso a particolari applicazioni e servizi da reti esterne all'azienda e il 61% ha stabilito specifiche policy per l'utilizzo dei device mobili.

Cloud - I principali rischi per gli ambienti cloud dipendono dal rapporto col fornitore: la minaccia più importante per il 63% delle imprese è la mancanza di controllo sulle operations del service provider, per il 44% il rock in col fornitore e il data breach, per il 41% la scarsa trasparenza rispetto agli obblighi contrattuali con il fornitore. Risulta qQuindi evidente che non sono più le minacce tecnologiche a preoccupare le aziende ma un'attenzione sempre maggiore va riposta nella stesura del contratto e nella gestione del rapporto con i provider.

IoT – Con lo sviluppo dell'Internet of Things aumenta il numero di dispositivi connessi alla rete e i possibili punti di accesso per un attacco al sistema informativo aziendale. Il 47% delle organizzazioni

non ha ancora messo in atto nessuna azione per tutelarsi in questo ambito, il 41% sta valutando possibili azioni, il 13% ha Policy di security by design nella progettazione di prodotti (la messa in sicurezza con misure come il monitoraggio continuo, l'utilizzo di credenziali e pratiche di programmazione migliori), il 10% utilizza soluzioni tecnologiche specifiche, il 9% ha Policy sulla rilevazione di dati nel perimetro aziendale e il 5% per la gestione di dati raccolti da oggetti smart.

Cyber intelligence – Le minacce informatiche diventano sempre più parte integrante del tessuto digitale aziendale e non è possibile evitare al 100% una violazione della sicurezza, così accanto all'approccio tradizionale basato sulla protezione dei sistemi, le aziende stanno cominciando ad adottare una logica di anticipazione delle minacce. L'analisi dei dati legati al mondo dell'information security è presidiata dal 57% delle organizzazioni tramite un presidio formale o informale, per l'8% c'è un presidio fuori delle attività core dell'information security, nel 35% il tema non è presidiato.

Il 32% delle imprese non utilizza dati per interpretare o anticipare criticità, mentre il restante 68% ha avviato azioni in questo ambito. L'integrazione di dati provenienti da varie fonti (dati sugli incidenti avvenuti a livello mondiale, indirizzi IP, log, URL sospette provenienti dalle segnalazioni degli utenti, ecc.) permette di sviluppare modelli di monitoraggio delle minacce, in grado di intercettare possibili anomalie e gestirle prima che la situazione diventi effettivamente critica. In alcune aziende esistono apposite strutture all'interno dei Security Operation Center, che analizzano e correlano i dati in ottica di Cyber Intelligence.

Le assicurazioni - Il mercato dell'assicurazione del rischio cyber è ancora immaturo in Italia. La copertura del rischio cyber è orientata~~re~~ a coprire i dannn~~tt~~i causati direttamente al sottoscrittore o a terze parti, dall'investigazione e gestione degli eventi, alla gestione delle istruttorie, alla copertura danni. Solo il 15% delle imprese ha già attive coperture assicurative, sebbene solo in poco più della metà dei casi (8%) si tratti di polizze espressamente orientate al rischio Cyber, mentre nei restanti casi si tratta di coperture generalistiche che la offrono tra le condizioni. Il 29% è in valutazione di coperture assicurative, mentre il 32% non ritiene sufficientemente maturo il mercato cyber insurance o non ritiene il problema rilevante.

Il fattore X - Nella sicurezza è fondamentale il *fattore X*, l'elemento di incertezza legato al comportamento umano, come la distrazione o la mancanza di consapevolezza, utilizzato spesso dai cybercriminali per fare breccia nei sistemi aziendali. Il 95% delle organizzazioni italiane ha già avviato azioni specifiche per sensibilizzare gli utenti aziendali. Le iniziative più diffuse riguardano comunicazioni periodiche inviate ai dipendenti tramite mail (77%) e corsi di formazione attraverso sessioni d'aula o e-learning (66%). Nel 28% dei casi la formazione viene inoltre supportata dalla distribuzione spot di materiale informativo (voucher, booklet, cartellonistica). Per il 28% delle organizzazioni si tratta di veri e propri progetti strutturati di sensibilizzazione tramite diversi strumenti e coprono spesso un orizzonte pluriennale. Vengono inoltre effettuate attività di vulnerabilityà assessment sui dipendenti aziendali (28%), per esempio tramite l'invio di finte mail di phishing o simulazioni di attacchi informatici, che servono da un lato a misurare il livello di consapevolezza dei dipendenti, dall'altro a testare l'efficacia delle iniziative già portate avanti.

Le PMI - L'analisi sulla diffusione delle soluzioni di information security tra circa 800 piccole e medie imprese italiane rivela che il 93% delle PMI ha dedicato un budget nel 2016, sebbene questo non corrisponda necessariamente ad un utilizzo maturo e consapevole. Le principali motivazioni agli investimenti infatti sono l'adeguamento normativo (48%) e gli attacchi subiti in passato (35%), ma a volte seguono la necessità di rispondere a nuove esigenze tecnologiche (22%) o di business (31%). La maggior parte delle PMI ha soluzioni di sicurezza di base (76%) come antivirus ed antispam ed il 62% dichiara di disporre anche di soluzioni sofisticate, come ad esempio firewall o sistemi di intrusion detection. Un'organizzazione su quattro (25%) però si fa guidare dal buon senso, senza un approccio tecnologico definito. Il 46% ha policy aziendali ben definite, mentre solo il 10% ha programmi di formazione orientati ad aumentare la consapevolezza. L'approccio alla sicurezza nelle PMI è orientato prevalentemente all'identificazione (66%) e alla protezione (66%), molto meno alla rilevazione (12%) e

alla risposta (15%). L'attenzione alla rilevazione cresce all'aumentare della dimensione di impresa, passando dall'11% delle piccole imprese al 20% delle medie.

"Le PMI sembrano sottovalutare la crescita della consapevolezza dei rischi tra i propri dipendenti – rileva **Alessandro Piva** -. Solo il 9% delle piccole aziende (tra i 10 e i 49 addetti) ha specifici programmi di formazione per aumentare la consapevolezza delle risorse rispetto~~i~~ ai rischi informatici, mentre la rilevanza delle azioni di sensibilizzazione cresce con l'aumentare della dimensione aziendale, attestandosi al 20% per le aziende medio-piccole (tra i 50 e i 99 addetti) e al 24% per le imprese più grandi (tra i 100 e i 249 addetti).".

*L'edizione 2016 dell'Osservatorio Information Security & Privacy è realizzata con il supporto di AlmavivA, BT Italia, Kaspersky Lab, Poste Italiane, Spike Reply, Symantec, TESISQUARE©, Trend Micro; Hitachi Systems CBT, Sinergy; Horizon Security; in collaborazione con Cefriel, 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@osservatori.net
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, 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. 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 per i programmi MBA e Executive MBA. Dal 2014, la Scuola è membro di UniCON, PRME e Cladea. La Scuola può contare su un corpo docente di più di duecento tra professori, ricercatori, tutor e staff e ogni anno vede oltre seicento matricole entrare nel programma undergraduate. Fanno parte della Scuola: il Dipartimento di Ingegneria Gestionale e MIP Graduate School of Business che, in particolare, si focalizza sulla formazione executive e sui programmi Master. Gli Osservatori Digital Innovation della School of Management del Politecnico di Milano (www.osservatori.net) nascono nel 1999 con l'obiettivo di fare cultura in tutti i principali ambiti di Innovazione Digitale per favorire lo sviluppo del Paese. La Vision che guida gli Osservatori è che l'Innovazione Digitale sia un fattore essenziale per lo sviluppo del Paese. La Mission degli Osservatori 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. Gli Osservatori sono oggi un punto di riferimento qualificato sull'innovazione digitale in Italia che integra attività di Ricerca, Comunicazione, Formazione e una Community sempre più ampia di professionisti. Gli Osservatori sono ormai molteplici e affrontano in particolare tutte le tematiche più innovative: Agenda Digitale, Big Data Analytics & Business Intelligence, Cloud & ICT as a Service, Cloud nella PA, Contract Logistics, Digital Finance, Digital Transformation Academy, Digital Insurance, eCommerce B2c, eGovernment, Enterprise Application Governance, Export, Fatturazione Elettronica e Dematerializzazione, Gestione Progettazione e PLM (GeCo), Gioco Online, HR Innovation Practice, Hubility/Multicanalità, Industria 4.0, Information Security & Privacy, Innovazione Digitale in Sanità, Innovazione Digitale nel Retail, Innovazione Digitale nei Beni e Attività Culturali, Innovazione Digitale nel Turismo, Internet Media, Internet of Things, Mobile B2c Strategy, Mobile Banking, Mobile Payment & Commerce, Professionisti e Innovazione Digitale, Smart Agrifood, Smart Working, Startup Hi-tech, Startup Intelligence, Supply Chain Finance.