*Comunicato stampa*

## Cybersecurity - i principali risultati secondo la Global State of Information Security® Survey 2015 curata da PwC, CIO e CSO:

- **Oltre 117.300 attacchi al giorno (+48% rispetto allo scorso anno)**
- **Danni per 2,7 milioni di dollari**
- **In calo del 4% i budget per la sicurezza informatica**
- **In crescita del 10% i crimini commessi da impiegati interni alle aziende**

**Milano, 30 settembre 2014** – Il numero di crimini connessi alla sicurezza informatica o cybersecurity ha subito un aumento a livello mondiale del 48% rispetto allo scorso anno, arrivando a 42,8 milioni, 117.339 attacchi al giorno (+66% dal 2009). E' quanto emerge dalla Global State of Information Security® Survey 2015 diffusa oggi da PwC insieme ai magazine CIO e CSO, condotta coinvolgendo 9.700 CEO, CFO, CIO, CISO, CSO, VP, manager IT e responsabili delle procedure di sicurezza di 154 Paesi.

"Non sorprende che i casi di violazione della cybersecurity crescano ogni anno, insieme all'impatto finanziario che ne deriva – sostiene Fabio Merello, Responsabile Cybersecurity in PwC Italia. Tuttavia, la rilevanza di tali violazioni diventa maggiore se consideriamo le modalità di individuazione e gestione di tali eventi".

Infatti con l'aumentare della frequenza di reati in materia di sicurezza informatica crescono anche i costi per gestire e attenuare i danni causati dalle violazioni. La perdita economica media per incidenti di cybersecurity in tutto il mondo è stata stimata in circa 2.7 milioni di dollari, il 34% in più rispetto allo scorso anno. Quest'anno abbiamo avuto inoltre un record di perdite: le società che hanno subito danni finanziari superiori ai 20 milioni di dollari sono quasi duplicate.

Tuttavia, nonostante le preoccupazioni crescenti, dalla ricerca emerge che le spese per la sicurezza informatica sono globalmente diminuite del 4% rispetto all'anno precedente. Negli ultimi cinque anni la percentuale di spesa all'interno dei budget IT è rimasta al 4% o diminuita.

"La spesa in sicurezza informatica implica che le imprese identifichino e investano nelle prassi di cybersecurity più efficaci per contrastare attacchi sempre più avanzati tecnologicamente" – spiega Fabio Merello. "E' fondamentale identificare procedure che integrino al massimo capacità predittive, preventive, di indagine e di risposta in caso di violazioni, per minimizzarne gli impatti negativi".

Le aziende sono consapevoli dei seri rischi riguardanti la cybersecurity: tuttavia sono le imprese più grandi a subire attacchi più frequenti. Grandi società con un fatturato annuo superiore al miliardo di dollari hanno registrato il 44% in più di incidenti rispetto allo scorso anno. Le società di medie dimensioni, con fatturati compresi tra i 100 milioni e il miliardo di dollari, il 64% in più. Tuttavia, mentre il rischio è globale, le perdite finanziarie variano sensibilmente a seconda delle dimensioni della società.

"Le grandi aziende sono i bersagli preferiti perché detengono informazioni di maggior valore", spiega Bob Bragdon, editore di Cso. "Tuttavia, con il migliorare delle misure di sicurezza adottate dalle grandi società, gli attacchi si concentrano su quelle di medie dimensioni, che spesso non hanno ancora adottato strategie efficaci".

"Nel contesto italiano, caratterizzato dalla presenza di un gran numero di piccole e medie imprese e da una contrazione della spesa più marcata rispetto ad altri paesi - aggiunge Fabio Merello - è ancora più importante per le aziende valutare correttamente i propri rischi, correlati alle possibili minacce, e ottimizzare gli investimenti".

Le persone che operano all'interno delle società sono spesso i principali indiziati, tuttavia in molti casi compromettono i dati involontariamente, per esempio smarrendo dispositivi mobili o quali vittime di phishing. Gli intervistati rivelano che i casi in cui sono coinvolti impiegati della società sono aumentati del 10%, mentre quelli attribuiti a service provider o consulenti esterni sono aumentati rispettivamente del 15% e 17%. "Molte società spesso gestiscono i casi di insider cyber crime senza coinvolgere le autorità, tuttavia con questo comportamento potrebbero danneggiare altre aziende, nel caso queste assumessero in futuro impiegati potenzialmente infedeli", aggiunge Bragdon.

Allo stesso tempo, benchè gli attacchi di alto profilo, cioè messi in atto da governi, organizzazioni criminali e concorrenti, siano quelli meno frequenti, rappresentano tuttavia il segmento in più rapida crescita. I cyberattack

effettuati a cura di governi sono cresciuti dell'86%, dato sicuramente sottostimato. La survey ha anche rilevato un incremento del 64% di incidenti attribuito all'iniziativa di competitors, alcuni dei quali sicuramente supportati dai rispettivi governi.

Un'efficace sensibilizzazione al tema della Cybersecurity richiede un coinvolgimento a livello apicale e un livello di comunicazione all'interno delle aziende che secondo la ricerca spesso manca. Solo il 49% degli intervistati afferma che la propria azienda utilizza un team multidisciplinare e trasversale che periodicamente si riunisce per discutere, coordinare e comunicare informazioni che riguardano la sicurezza informatica.

Come fa notare PwC è fondamentale per le società concentrarsi su una rapida individuazione dei casi di intrusione per avere una risposta efficace e tempestiva. Visto l'attuale livello di interconnessione nel business, è importante stabilire specifiche politiche e processi nell'ambito dei rapporti economici con terze parti.

"I rischi legati alla sicurezza informatica non verranno mai completamente eliminati, e con la crescita del cybercrime le società devono essere preparate e vigili nell'ambito di uno scenario in costante evoluzione", conclude Merello. "Le società devono passare da un modello di sicurezza concentrato su prevenzione e controllo, a un approccio basato sulla gestione del rischio che sia in grado di dare priorità agli asset di maggior valore e valuti le minacce incombenti. Investire in una solida politica di sensibilizzazione sul tema della Cybersecurity sarà fondamentale per il successo futuro delle imprese".

Per scaricare *The Global State of Information Security Survey 2015*: http://pwc.to/GSISS15.

**NOTE:** La dicitura corretta dell'indagine è "The Global State of Information Security® Survey 2015, a worldwide survey by *CIO, CSO* and PwC". Le fonti devono menzionare CIO, CSO e PwC. I risultati della ricerca saranno analizzati in profondità anche su *CIO.com* e *CSO*online.com nel mese di ottobre.

**IL METODO DI RICERCA:** *The Global State of Information Security® Survey 2015* è uno studio realizzato su scala mondiale da PwC, CIO e CSO. E' stato condotto online dal 27 marzo 2014 al 25 maggio 2014. Clienti di PwC e lettori di CIO e CSO sono stati invitati via e-mail a partecipare all'indagine. I risultati esposti in questo report sono fondati sulle risposte di oltre 9.700 CEO, CFO, CIO, CISO, CSO, VP, manager IT e responsabili delle procedure di sicurezza di 154 Paesi. Il 35% degli intervistati sono del Nord America, il 34 % dell'Europa, il 14% dell'Asia, il 13% del Sud America e il 4% di Africa e Medio Oriente.

**PwC** fornisce servizi professionali di revisione, di advisory, di consulenza legale e fiscale alle imprese con l'obiettivo di creare valore. PwC è un network distribuito in 157 Paesi con oltre 184.000 professionisti, di cui 3.400 in PwC Italia. Maggiori informazioni sul sito www.pwc.com.

***CIO* E *CSO:*** CIO è una primaria risorsa di contenuti e di community per i dirigenti e i leader in campo IT che prosperano e crescono in quest'era di rapida trasformazione informatica delle aziende. Il premiato portfolio di CIO, che comprende CIO.com, la rivista CIO (lanciata nel 1987), i programmi executive, i servizi marketing, i forum su LinkedIn e le ricerche CIO, rappresenta per i leader della business technology una fonte di analisi e approfondimento sulle tendenze informatiche e offre una profonda comprensione del ruolo che riveste l'informatica nel raggiungimento degli obiettivi aziendali. CIO fornisce anche un'opportunità per i fornitori di soluzioni IT di raggiungere questa tipologia di pubblico. CIO è pubblicata da IDG Enterprise, controllata di International Data Group (IDG), società leader a livello mondiale nell'ambito media, eventi e ricerca. Per maggiori informazioni sull'azienda, visitare www.idgenterprise.com.

CSO è una primaria risorsa di contenuti e community per i decision maker in campo di sicurezza a capo delle strategie di "gestione del rischio d'impresa" della propria azienda. Sono oltre dieci anni che i responsabili della sicurezza attingono al premiato sito (CSOonline.com), alle conferenze executive, ai servizi marketing e di ricerca di CSO per trovare gli strumenti per contenere il rischio di tipo IT e corporate/fisico delle proprie imprese; mentre i vendor in campo di sicurezza hanno la possibilità di entrare in contatto con questa categoria di pubblico. Per aiutare i CSO a formare i propri dipendenti in tema di pratiche di sicurezza aziendale e personale, CSO pubblica anche una newsletter trimestrale, Security Smart. CSO è pubblicata da IDG Enterprise, controllata di International Data Group (IDG), società leader a livello mondiale nell'ambito media, eventi e ricerca. Per maggiori informazioni sull'azienda, visitare www.idgenterprise.com.

The Global State of Information Security® è un marchio registrato International Data Group, Inc.

**Barabino & Partners**
Raffaella Nani
r.nani@barabino.it
Alice Brambilla
a.brambilla@barabino.it
Tel. + 39.02/72.02.35.35
Cell. +39.328/266.81.96

Milano, 30 settembre 2014