
Comunicato stampa

Cybersecurity - i principali risultati secondo la Global State of Information Security® Survey 2016 curata da PwC, in collaborazione con CIO e CSO:

- **A livello mondiale cresce del 38% il numero di attacchi informatici rilevati (42,8 milioni lo scorso anno)**
- **Aumentano i budget in sicurezza informatica: +24% nel mondo, +66% in Italia**
- **E' pari a 2,5 milioni di dollari il danno medio per attacco (2,7 milioni di dollari lo scorso anno)**
- **Autori dei crimini informatici sono nel 34% dei casi gli impiegati interni alle aziende, nel 22% dei casi i business partner**
- **Aumentano i furti di proprietà intellettuale, +56% a livello mondiale e +108% in Italia.**

Milano, 7 Ottobre 2015 – Anno dopo anno, gli attacchi informatici continuano a crescere per frequenza, gravità e impatto. Sono continue le innovazioni in ambito Cybersecurity, migliorano costantemente i metodi di prevenzione e rilevazione, così come i Business Leader più attenti si concentrano su soluzioni finalizzate alla riduzione dei rischi e al miglioramento delle performance di business.

E' quanto emerge dalla Global State of Information Security® Survey 2016 diffusa oggi da PwC in collaborazione con i magazine CIO e CSO, condotta coinvolgendo 10.000 CEO, CFO, CIO, CISO, CSO, VP, manager IT e responsabili delle procedure di sicurezza, di cui circa 500 italiani, in 127 Paesi.

I dati dimostrano un significativo trend di crescita del Cybercrime con un incremento del 38% del numero di attacchi rilevati a livello mondiale (42,8 milioni lo scorso anno), cui corrisponde un incremento degli investimenti pari al 24%. Spicca il dato italiano, con un incremento degli investimenti pari al 66%, dovuto in parte al significativo rallentamento complessivo degli investimenti negli anni passati e quindi all'esigenza di rimettersi al passo in un settore che si sta rivelando molto critico per il business delle imprese.

“Il danno medio per evento – spiega Fabio Merello, Responsabile Cybersecurity in PwC Italia – rimane sostanzialmente immutato assestandosi a 2,5 milioni di dollari (2,7 milioni di dollari lo scorso anno), mentre appare preoccupante il trend di crescita relativo alla rilevazione di furti di proprietà intellettuale, pari al 56% a livello mondiale e al 108% in Italia. Questo dato potrebbe in realtà nascondere una nota positiva, in quanto indice di una migliorata capacità di rilevazione”.

Altri trend rilevati:

Evoluzione dei ruoli: il 54% di chi ha risposto (il 58% in Italia) ha istituito la carica di CISO (Chief Information Security Officer). La struttura di riporto lo vede dipendere, in ordine di probabilità, da CEO, CIO, Consiglio di Amministrazione e CTO (per l'Italia CEO, CdA, CIO, CSO).

Cresce il coinvolgimento del CdA: nel 45% dei casi (55% in Italia) il CdA è coinvolto nella strategia di sicurezza complessiva. Questo maggiore coinvolgimento ha aiutato molto spesso il miglioramento delle prassi di sicurezza.

Crescono i pagamenti via mobile e la necessità di presidio del rischio: il 57% di chi ha risposto (il 60% in Italia) ha adottato sistemi di pagamento via mobile. Da evidenziare l'aumento di nuove e diverse forme di partnership tra aziende tecnologiche, finanziarie, retail e telco.

Investimenti nelle assicurazioni: E' sempre possibile che criminali particolarmente abili riescano comunque ad aggirare le difese. Per questo molte aziende (59% nel mondo, 67% in Italia) stanno iniziando a proteggersi con assicurazioni dedicate, al fine di mitigare gli impatti finanziari in caso di attacco informatico.

Le indagini dei governi hanno impatto sugli investimenti: In diversi paesi gli investimenti sono in fase di revisione (34% nel mondo, 35% in Italia) o avvengono meno di frequente (22% nel mondo, 29% in Italia), come risultato di notizie o informative in merito a indagini che il proprio governo starebbe effettuando su prodotti (hardware/software) e servizi forniti da paesi terzi.

Autori degli incidenti: Al primo posto i dipendenti, sostanzialmente stabili al 34%, con un incremento significativo dei business partner, che salgono al 22% (+22%); per quanto riguarda l'Italia sono prevalenti i

dipendenti e business partner passati (rispettivamente 27% e 21%) mentre spicca ancora un 40% di mancata individuazione degli autori.

Siccome i rischi legati ai cyber attacchi sono sempre più all'attenzione delle C-Suite e dei Consigli di Amministrazione, i Business Leader stanno sempre più ripensando alle proprie Cybersecurity Practice, focalizzandosi su un insieme di tecnologie innovative in grado di ridurre i rischi d'impresa e migliorare le prestazioni aziendali. La maggior parte delle aziende, il 91% (il 90% in Italia) ha adottato un framework di sicurezza o, più di frequente, una combinazione di diversi framework.

“Stiamo assistendo alla trasformazione di quanto una volta veniva percepito come molto rischioso in una possibile soluzione al problema”, Spiega Merello. “Per esempio, molte aziende stanno adottando soluzioni in Cloud di Advanced Authentication in luogo di soluzioni basate unicamente sull'utilizzo di una password”.

L'adattamento delle tradizionali misure di Cybersecurity ad un ambiente sempre più Cloud-Based è un esempio di questo impegno che richiede investimenti considerevoli per sviluppare nuove funzionalità a livello di infrastruttura di rete che consentano una migliore raccolta di informazioni, migliore identificazione delle minacce, migliore difesa contro gli attacchi e migliore risposta agli incidenti.

Secondo il survey, il 69% (79% in Italia) di coloro che hanno risposto dicono di utilizzare servizi di sicurezza Cloud-Based per proteggere i dati sensibili e garantire privacy e protezione dei dati dei clienti.

Connesse ai sistemi Cloud-Based, le soluzioni legate ai Big Data e all'Internet of Things presentano una serie di sfide e opportunità. Nel caso dei Big Data, il 59% di chi ha risposto (56% in Italia) sta sfruttando l'analisi di grosse quantità di dati per migliorare la sicurezza spostando il focus oltre le difese perimetrali e permettere così di elaborare informazioni in tempo reale al fine di creare valore aggiunto.

Dato il crescente numero di dispositivi connessi a Internet, l'Internet of Things porterà inevitabilmente ad un incremento dei requisiti di sicurezza nell'ambito delle reti Cloud-Based. Gli investimenti destinati ad affrontare queste tematiche sono raddoppiati nel corso del 2015, ma solo il 36% (il 45% in Italia) delle persone che hanno risposto dispone di una strategia indirizzata specificatamente verso l'Internet of Things.

“Non c'è una soluzione unica che vada bene per tutte le aziende. Si tratta di un processo di trasformazione continua, che si basa sul giusto mix di tecnologia, processi e, soprattutto, consapevolezza e capacità delle persone, volto a proteggere l'azienda e a creare valore aggiunto”, ha aggiunto Fabio Merello, Responsabile Cybersecurity per PwC Italia “In questo modo la Cybersecurity può diventare un potente fattore abilitante e distintivo”.

Nel corso degli ultimi tre anni è aumentato, attestandosi al 65%, il numero di società che ha deciso di collaborare con l'esterno (partner, clienti e fornitori) per migliorare la sicurezza e per gestire al meglio minacce e risposte.

“Un programma di sicurezza avanzato e migliorato non solo consentirà alle aziende di difendersi meglio contro le minacce informatiche, ma aiuterà anche a creare vantaggi competitivi e a favorire la fiducia tra clienti, fornitori e partner commerciali”, asserisce Bob Bragdon, editore e Vice Presidente di CSO.



METODOLOGIA DI RICERCA

"The Global State of Information Security® Survey 2016" è uno studio condotto su scala mondiale da PwC, CIO magazine e CSO. È stato effettuato on line dal 7 maggio 2015 al 12 giugno 2015.

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 10.000 CEO, CFO, CIO, CISO, CSO, VP, manager IT e responsabili delle procedure di sicurezza di oltre 127 Paesi. Il 37% degli intervistati sono del Nord America, il 30 % dell'Europa, il 16% dell'Asia, il 14% del Sud America e il 3% di Africa e Medio Oriente. Il margine di errore è minore dell'1%.

CIO

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

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.

PWC

PwC è un network presente in 157 Paesi con oltre 208.000 professionisti, di cui 4.000 in Italia, impegnati a garantire qualità nei servizi di revisione, di advisory e di consulenza legale e fiscale alle imprese. Maggiori informazioni sul sito www.pwc.com.

© 2015 PricewaterhouseCoopers. Tutti i diritti riservati

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