RAPPORTO 2012 OAI: UNA SINTESI DEI DATI EMERSI

ARCHITETTURE AGGIORNATE E MAGGIORE CONSAPEVOLEZZA.

Marco Bozzetti, OAI founder

Ai primi di dicembre 2012 è stato pubblicato il Rapporto 2012 OAI, arrivato alla terza edizione. Per la prima volta è stato sponsorizzato da importanti aziende della domanda e dell'offerta ICT ed ha avuto il patrocinio da un ampio ed autorevole insieme di associazioni del settore ICT, oltre alla collaborazione della Polizia Postale e delle Telecomunicazioni.
I dati del Rapporto si basano sulle risposte al questionario messo on-line da fine luglio a fine ottobre 2012, ed al quale hanno risposto 206 interlocutori, rispetto ai 130 e ai 105 delle due precedenti edizioni. Il bacino delle persone contattate via posta elettronica e in alcuni casi anche telefonicamente si aggira attorno alle 6000 persone, rispetto a più di 1800 della scorsa edizione. Il target del questionario è tipicamente il responsabile dei sistemi informativi (CIO), il responsabile della sicurezza ICT (CSO), le terze parti che gestiscono la sicurezza informatica in logica di ousourcing.
Le risposte avute rispetto al bacino contattato sono estremamente basse: le possibili motivazioni sono molteplici e differenti a secondo del tipo e delle dimensioni dell'azienda/ente: politiche interne di non comunicare questo tipo di informazioni, necessità di chiedere permessi a più alti livelli, mancanza di tempo del possibile compilatore, incapacità di rispondere a tutte le domande, ecc.
Il numero di risposte ricevute sono comunque sufficienti e significative a fornire delle concrete indicazioni sugli attacchi ai sistemi informativi in Italia. L'analoga iniziativa statunitense promossa dal CSI (Computer Security Institute), consolidata da anni e modello di riferimento anche per OAI, raccoglie un campione di poco più di 500 interlocutori per tutti gli Stati Uniti.

Un mercato attento ai cambiamenti

Come ruolo dei rispondenti, il 30,8% è dei CIO, il 17,1% dei top manager (il che evidenzia che nelle PMI è il vertice aziendale che decide sull'ICT e sulla sua sicurezza), il 16,2% dei CSO, il 12,8 % delle terze parti.
La ripartizione per settore di industria vede al primo posto l'ambito dei servizi-distribuzione con il 30,7%, l'industria con il 21,1%, telecom e media con il 18,4,%, tutti gli altri settori merceologici, incluse le pubbliche amministrazioni, tra il 7 e l'1,8%.
I sistemi informatici dei rispondenti, pur nella loro diversità in termini dimensionali, di complessità e di tecnologie utilizzate, in funzione anche delle caratteristiche dimensionali e di settore delle aziende/enti, sono nella maggior parte dei casi ben aggiornati, con architetture ad alta affidabilità e multipiattaforma. Significativo che poco meno della metà dei rispondenti faccia uso di terziarizzazione e cloud computing.
Questo aumento, forte rispetto alle edizioni precedenti, è un chiaro indicatore del cambio di mentalità e di percezione in Italia nel passare a nuove forme di sourcing, superando la tradizionale riluttanza, dovuta soprattutto alla sicurezza e alla disponibilità. Questo cambio è stato favorito anche dai problemi economici dovuti al perdurare dell'attuale crisi economica.

Tempi di ripristino rapidi

Nel periodo 2010 - 1° quadrimestre 2012 è cresciuto in percentuale il numero di aziende/enti che hanno subito attacchi. Facendo riferimento alle principali tipologie di attacco i più diffusi riguardano il "malware", il "social engineering", la saturazione delle risorse (DoS e DDoS) ed il furto dei dispositivi ICT, in particolare di quelli mobili tipo "smartphone" e "tablet".

Rispetto alle edizioni precedenti, il questionario 2012 ha aggiunto alle domande sugli attacchi subiti, per ogni tipo di attacco, se questi hanno avuto impatti poco o molto significativi. Per non appesantire la lunghezza del questionario, non si è voluto dettagliare il tipo di impatto, ad esempio economico, legale, di immagine, lasciando al compilatore la libertà di rispondere considerando qualitativamente l'intera valenza del termine impatto per la sua azienda/ente. Dall'analisi emerge come la maggior parte degli attacchi ha avuto impatti poco significativi, ma alcuni attacchi (6,5-6,7% fino a 10 casi, circa la metà oltre) hanno comportato forti impatti: tra questi furti di dispositivi ICT, attacchi fisici, accessi non autorizzati, modifiche non autorizzate dei sistemi e dei dati, "social engineering", codici maligni, utilizzo vulnerabilità (exploit), saturazione risorse. Tali attacchi sono occorsi ad aziende/enti dei settori merceologici industria, PAC, sanità, servizi, TLC & media, utility. La conferma che la maggior parte degli attacchi non abbia avuto gravi impatti è data dai tempi di ripristino: la situazione 'ante' è ripresa in media in meno di un giorno, e complessivamente in circa il 90% dei casi la situazione è ripristinata entro 3 giorni dall'attacco.

Maggiore consapevolezza

Tale situazione, sul campione emerso dall'indagine, è dovuta anche al buon livello di sicurezza ICT posto in essere e nella sua efficace gestione. Le misure di sicurezza sono più diffuse a livello infrastrutturale che applicativo e per la protezione dei dati: inizia comunque a diffondersi una maggior consapevolezza, e quindi attenzione, sulla sicurezza intrinseca del software messo in produzione e sulla protezione delle informazioni. Sul piano organizzativo, per una non trascurabile percentuale del campione, le aziende/enti sono meno avanzate che sul piano tecnico, ma sembrano migliorare rispetto a quanto rilevato nelle precedenti edizioni. In buona parte delle organizzazioni è definita la figura del CSO; vengono seguite, almeno nella sostanza e per gli aspetti più importanti, le linee guida e le metodiche dei principali standard e delle best practice internazionali; viene svolto con una certa regolarità l'auditing informatico, ed infine cresce la consapevolezza dell'importanza della sicurezza ICT a livello dei vertici/decisori dell'azienda/ente. Per contro la gestione della sicurezza è ancora prevalentemente separata e frammentata a livello di silos, poco centralizzata ed integrata con la più generale gestione dell'intero sistema informativo, è poco diffusa l'analisi del rischio informatico, embrionali risultano la stima economica degli impatti di un attacco e la riassicurazione del rischio residuo, carente la separazione delle responsabilità tra i vari attori della sicurezza ICT, i piani di emergenza e il disaster recovery, più formali che sostanziali.

Marco Bozzetti
marco.bozzetti@malaboadvisoring.it