ATTACCHI INFORMATICI IN ITALIA

PRIME CONSIDERAZIONI DAL RAPPORTO 2013 OAI

Marco Bozzetti, OAI founder

È appena stato pubblicato il Rapporto 2013 OAI, giunto alla quarta edizione, con la sponsorizzazione di due Associazioni, Aica e Aipsi, e di alcune società dell'offerta ICT: Sernet, Seeweb, Technology Estate,Trend Micro. OAI 2013 ha avuto il patrocinio da un ampio ed autorevole insieme di associazioni del settore ICT[1], oltre alla preziosa collaborazione della Polizia Postale e delle Telecomunicazioni. I rispondenti al questionario 2013 sono stati 299, con un significativo incremento rispetto ai 206, 130 e 105 delle precedenti edizioni. Tale incremento ha fatto riferimento prevalentemente al settore industriale, arrivato così al 43%, superando così il settore servizi ora al 24,2%: tutti gli altri settori hanno percentuali al di sotto del 10%.
La maggior parte dei rispondenti sono responsabili dei sistemi informativi (CIO), circa il 38%, e loro collaboratori, 17%; a questi seguono i vertici di piccole organizzazioni, 16,5%; CISO e CSO hanno ancora percentuali basse, dato che la maggior parte delle organizzazioni rispondenti sono medio-piccole, e tali figure sono tipiche di grandi strutture. Quasi la metà del campione emerso è costituito da aziende/enti con meno di 100 dipendenti, poco meno del 27% tra 101 e 1.000, il 16% tra 1.001 e 5.000, l'8,7% più di 5.000.

I sistemi informatici

Anche le dimensioni dei sistemi informatici dei rispondenti confermano la prevalenza di PMI: quasi la metà ha fino a 10 server, fisici o virtuali, e un quarto tra 11 e 100. Un quinto arriva fino a 1.000, e poco più dell'8% supera quest'ultima percentuale. Simile, e logicamente congruente, il numero di posti di lavoro fissi: per più della metà arriva a 100. Per i dispositivi mobili il Rapporto distingue quelli di proprietà dell'azienda/ente, rispetto a quelli dell'utente finale, in modo da poter stimare il fenomeno del Byod (bring your own device) che pone ulteriori problemi nella gestione della sicurezza ICT. Quasi il 60% del campione ha fino a 100 sistemi mobili di proprietà aziendale, e il 50% di proprietà dell'utente. Ma nel 36,3% delle aziende/enti non è permesso il Byod.
I sistemi informatici dei rispondenti, pur nella loro diversità in termini dimensionali, di complessità e di tecnologie utilizzate sono nella maggior parte dei casi aggiornati e di buon livello: molti hanno architetture ad alta affidabilità e multipiattaforma. Un significativo indicatore è dato dai tipi di sistema operativo utilizzati per i server, con risposte multiple: la stragrande maggioranza è di Windows, con quasi il 65% con versioni server pre 2010, il 40,3%

[1] AIPSI (Associazione Italiana Professionisti Sicurezza Informatica), Assintel di Confcommercio (Associazione Nazionale Imprese ICT), Assolombarda di Confindustria, Aused (Associazione Utilizzatori Sistemi e Tecnologie dell'informazione), CDI (Club Dirigenti Informatica di Torino), CDTI (Club Dirigenti Tecnologie dell'Informazione di Roma), Club per le Tecnologie dell'Informazione Emilia Romagna, Club per le Tecnologie dell'Informazione delle Marche, Club per le Tecnologie dell'Informazione di Milano, FidaInform (Federazione dei ClubTI Italiani), Forum d elle competenze digitali, FTI (Forum per le Tecnologie dell'Informazione), IEEE-Computer Society Italian Chapter, Inforav (Istituto per lo sviluppo e la gestione avanzata dell'informazione), itSMF Italy (information technology Service Management Forum).

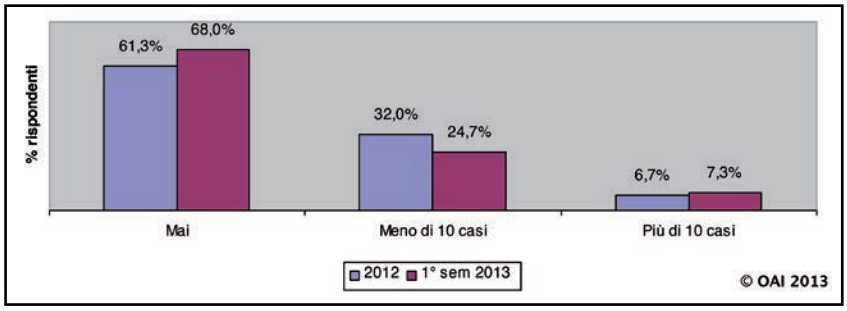

Fig. 1 - Attacchi rilevati nel 2012 e nel 1° semestre 2013

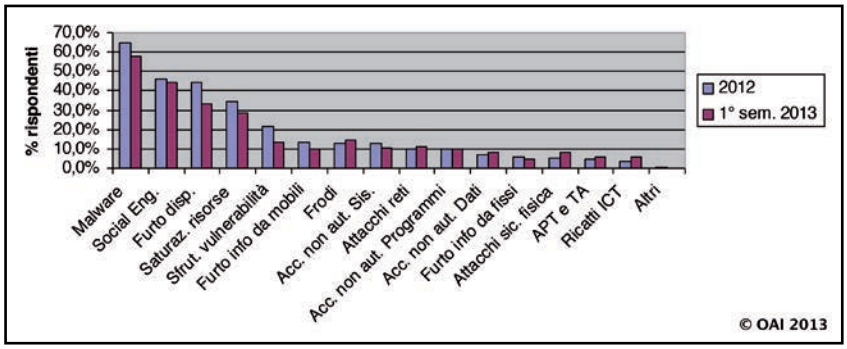

Fig. 2 - Diffusione tipologia attacchi subiti 2012 - 1° semestre 2013 (risposte multiple)

Win server 2012 ed il 39% v. 2010. Linux è diffuso al 53,5% mentre Unix, nei vari tipi e versioni, al 22%. La virtualizzazione è diffusa, con un 45,3% di hypervisor, mentre i sistemi AS400 sono al 18,2% del campione e i mainframe e i supercomputer al 10% circa.

Modalità di fruizione

Quasi il 37% dei rispondenti utilizza hosting ed housing, il 27,6% utilizza il cloud, il 15% terziarizza la gestione del sistema informatico e il 10,6% la gestione della sicurezza informatica (risposte multiple). Tali dati meritano un commento: più di 2/3 del campione ormai esternalizza e utilizza il cloud, con incrementi significativi rispetto a quanto emerso nelle precedenti edizioni di OAI, pur tenendo conto del campione diverso nei vari anni. È un chiaro indicatore del cambio di mentalità e di percezione in Italia nel passare a forme di 'sourcing', ma la quota percentuale maggiore tra i tradizionali hosting e housing rispetto al cloud evidenzia il persistere di una certa riluttanza verso il cloud dovuta probabilmente ad aspetti di sicurezza e della disponibilità di banda in alcune zone. Idonee le misure tecniche di sicurezza in atto, un poco meno le misure organizzative e procedurali, di cui tratteremo nel prossimo numero.

Il crimine informatico non dorme mai

In questo contesto, nel periodo 2012 - 1° semestre 2013 gli attacchi intenzionali rilevati sono percentualmente indicati nella fig. 1. Di questi attacchi solo una piccola parte, tra il 5 ed il 7%, ha avuto impatti significativi, come confermato anche dai tempi medi richiesti per il ripristino delle condizioni ex-ante: 57,1% dei ripristini in giornata, 23,4% in 3 giorni, 5,2% in una settimana, 2,6 % entro, e mai oltre, un mese.
La fig. 2 mostra quali sono stati le tipologie di attacco più diffuse: malware e social engineering sono ancora in testa alla classifica, mentre quest'anno il furto dei dispositivi ICT ha superato la saturazione delle risorse (DoS e DDoS), sicuramente grazie al crescente furto di smartphone e tablet. In OAI 2013 si è introdotta la tipologia dei TA, Targeted Attack e degli APT, Advanced Persistent Threat, non presente nelle precedenti edizioni. Questi tipi di attacchi nelle precedenti edizioni del rapporto venivano probabilmente inseriti nella voce 'altri'.
Il quadro complessivo dell'indagine mostra che gli attacchi intenzionali, pur tendenzialmente in crescita, sono stati subiti da poco meno del 40% del campione, ma hanno avuto limitati impatti, a parte pochi casi.

Marco Bozzetti
marco.bozzetti@malaboadvisoring.it