

Comunicato Stampa

Milano, 10 febbraio 2014

Pubblicato il Rapporto 2013 OAI, Osservatorio Attacchi Informatici in Italia

Il Rapporto 2013 OAI rileva che gli attacchi ICT intenzionali in Italia nel **2012** hanno interessato il **38,7%** del campione di aziende/enti rispondenti, e nel **1° semestre 2013** il **32%** del campione. Di questi attacchi solo una piccola parte, **tra il 5 ed il 7%, ha avuto impatti significativi**, come confermato anche dai tempi medi per il ripristino delle condizioni ex-ante: entro un giorno per il 57.1%, in 3 giorni per il 23.4%, in una settimana per il 5.2%, entro, e mai oltre, un mese per il 2.6 %.

Facendo riferimento alle principali tipologie di attacco subite dai sistemi informativi del campione 2013, il Rapporto 2013 OAI evidenzia che :

- al primo posto il **malware** che nel 2012 ha coinvolto il **64,8%** dei rispondenti, e nel 1° semestre 2013 il 57,7%;
- al secondo posto il **social engineering**, che nel 2012 ha colpito il **46,5%** dei rispondenti, e nel 1° semestre 2013 il 44,4%; questa tipologia di attacco include gli attacchi di **phishing**, che dalla posta elettronica si è esteso negli ultimi anni agli SMS, alle chat, ai social network;
- al terzo posto si posiziona il **furto di dispositivi ICT** che nel 2012 ha colpito il **44,4%** dei rispondenti, e nel 1° semestre 2013 il 33,1%; nella precedente edizione era al quarto posto preceduto dalla **saturazione di risorse** (DoS/DDoS), che è ora al quarto posto, con **34,5%** nel 2012 e 28,9% nel 1° semestre 2013.

Confrontando sempre a puro scopo indicativo e non statistico la diffusione degli attacchi subiti nelle edizioni precedenti di OAI, le quattro tipologie di cui sopra sono sempre in testa alla classifica degli attacchi più diffusi. Tutti questi dati sono congruenti con le indicazioni che emergono da recenti indagini internazionali, che rilevano che l'Italia si attesta a meno dell'1% a livello mondiale sul numero complessivo di attacchi subiti.

I rispondenti al questionario 2013 OAI 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 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 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 1000, il 16% tra 1001 e 5000, l'8,7% più di 5000.

Anche le dimensioni dei sistemi informatici dei rispondenti confermano la prevalenza di PMI: quasi la metà ha fino a 10 server, fisici o virtuali, ed 1/4 tra 11 e 100. 1/5 arriva fino a 1000, e poco più dell'8% supera quest'ultima cifra. 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, ed 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 multiplatforma. La **virtualizzazione è diffusa, con un 45,3%** di hypervisor. In termini di gestione e di governo dei sistemi informativi e della loro sicurezza, ben **più di 1/3 dei rispondenti terziarizza** parte o tutto il proprio sistema informativo e la sua gestione e più di 1/4 dei rispondenti, **il 27,5%, utilizza soluzioni in cloud**.

I tipi di attacchi più temuti nel prossimo futuro sono prevalentemente quelli ora più diffusi e sopra elencati. Le motivazioni degli attaccanti sono soprattutto per un **illecito guadagno**.

Riguardo agli strumenti ed alle politiche di sicurezza impiegate la situazione emersa è abbastanza positiva. Per la sicurezza fisica il 3/4 dei rispondenti è dotato di sistemi per garantire la continuità elettrica, il 70% dispone di sistemi di climatizzazione e quasi il 65% di protezioni perimetrali. A livello di reti il 3/4 dei rispondenti è dotato di dispositivi firewall e di DMZ, DeMilitarized Zone, e quasi il 65% utilizza soluzioni VPN, Virtual Private Network. I software antivirus e antispyware sono usati dal 70,4% dei rispondenti, ed il 50,7% dichiara di usare sistemi ad alta affidabilità. Per la protezione degli applicativi il 66,2% usa firewall applicativi e reverse proxy. Per la protezione dei dati il 62,7% utilizza l'archiviazione remota, tipicamente con ISP/ASP e con cloud; più di 1/4 critta i dati archiviati, anche grazie ai servizi in cloud, ed il 22,5% utilizza tecniche e strumenti di DLP, Data Loss Prevention.

Per quanto riguarda gli aspetti organizzativi, il campione emerso è **meno avanzato** che sul piano tecnico: più del 60% dei rispondenti ha definito e gestisce "policy" sulla sicurezza e le relative procedure organizzative, più della metà svolge o svolgerà auditing, ma solo un 38,3% ha definito un ruolo di "responsabile della sicurezza informatica", e solo il 27,1% ha effettuato una analisi dei rischi. Per quanto riguarda il riferimento o la certificazione per gli standard internazionali, sia a livello aziendale che personale (questi ultimi normalizzati in Italia dal D.Lgs 13/2013), la situazione è attualmente "tiepida": la metà dei rispondenti non li considera (forse nemmeno li conosce) e sono seguiti solo se richiesti da specifici capitolati o da normative relative allo specifico settore merceologico di appartenenza.

In conclusione il Rapporto OAI 2013 riconferma che i sistemi informatici delle aziende e degli enti in Italia **non sono per ora nell'occhio del ciclone** dei principali sempre più sofisticati e pericolosi attacchi cibernetici, ad eccezione di qualche infrastruttura ICT particolarmente critica e di sistemi ICT di aziende e brand famosi a livello mondiale.

Il Rapporto 2013 OAI, giunto alla quarta edizione, è ideato e realizzato da Marco R. A. Bozzetti con la collaborazione di vari esperti, ed è edito da Soiel International (www.soiel.it); ha la sponsorizzazione di due Associazioni, AICA ed AIPSI, e delle aziende Gruppo Sernet, Seeweb, Technology Estate, Trend Micro, oltre al patrocinio di un ampio ed autorevole insieme di Associazioni del settore ICT¹, e alla preziosa collaborazione della Polizia Postale e delle Telecomunicazioni.

Il Rapporto OAI 2013 è riservato in esclusiva **per i primi quattro mesi dalla pubblicazione** agli interlocutori degli Sponsor, che potranno scaricare gratuitamente il Rapporto in formato elettronico (pdf) tramite uno specifico codice-coupon.

Nell'ambito della presentazione in anteprima dei principali dati emersi dal Rapporto 2013 OAI in Assolombarda del 27/1/2014, il dott. Salvatore La Barbera, Direttore per la Regione Lombardia della Polizia Postale e delle Comunicazioni, ha sottolineato che il Rapporto OAI rappresenta attualmente un significativo ed indispensabile riferimento per le attività della stessa Polizia Postale.

Per ulteriori informazioni: oai@aipsi.org, oai@malaboadvorsing.it

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 delle 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).