OsservatoriO AttacchInformatici

Il giudizio degli esperti sulla situazione italiana

LE VALUTAZIONI EMERSE DURANTE LA TAVOLA ROTONDA CHE HA COMMENTATO I RISULTATI DEL RAPPORTO 2015 OAI

Marco R. A. Bozzetti,
OAI founder

La conferenza stampa di presentazione del Rapporto 2015 OAI, Osservatorio Attacchi Informatici in Italia, realizzata presso il Politecnico di Milano nelle scorse settimane ha visto anche l'organizzazione di una Tavola Rotonda tra esperti rappresentanti degli sponsor del Rapporto. In queste pagine vengono proposte le valutazioni emerse in questa discussione.

Il professor Stefano Zanero, membro del board internazionale della Information Systems Security Association, ha fatto gli onori di casa e nel suo intervento ha sottolineato come OAI sia l'unica indagine indipendente in Italia basata sulla compilazione via web di un questionario anonimo, al quale hanno risposto 424 rappresentanti di entità di varie dimensioni e provenienti da diversi settori merceologici. Il Rapporto viene così a riempire autorevolmente una mancanza di dati sulla realtà italiana e a promuovere una cultura sulla sicurezza ancora embrionale soprattutto a livello di molti vertici/decisori aziendali.

Salvatore La Barbera, della Polizia Postale, ha fatto il punto sul contrasto alla criminalità informatica, in particolare per le infrastrutture critiche, cui è dedicato un capitolo del Rapporto con dati inediti forniti dalla Polizia Postale stessa e dal Cnaipic (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche) ente attivo presso il ministero dell'Interno.

La Tavola Rotonda si è invece sviluppata proponendo le seguentio tre domande ai partecipanti:

- Secondo la vostra esperienza sul campo, i sistemi informatici delle medie/grandi imprese sono ragionevolmente sicuri? E per quanto riguarda le piccole e piccolissime aziende?
- Il vertice aziendale quanto è consapevole della sicurezza informatica in termini di impatto sul business/attività, e quindi di adeguato budget e approvazione dei progetti?
- I CIO dispongono degli strumenti adeguati - economici, tecnici, competenze - per una difesa proattiva?

Lo scenario generale

La maggior parte dei partecipanti ha evidenziato come ci sia ancora molta strada da fare per raggiungere, soprattutto nelle aziende piccole e piccolissime, buoni livelli di sicurezza; la cultura della prevenzione non è elevata in Italia, e il tema della sicurezza, inclusa quella informatica, viene il più delle volte affrontato solo a seguito di un incidente.

È stato però evidenziato come alcune nuove imprese, che basano il loro business prevalentemente sui sistemi informatici, sono molto attente al problema e quindi adottano soluzioni di difesa e tecniche organizzative allo stato dell'arte. La crisi economica ha ridotto in generale il livello di spesa in ICT, e quindi anche il budget della sicurezza.

È difficile perciò trovare disponibilità di budget su progetti strettamente e solamente di sicurezza; più facile che questi siano inclusi in progetti orientati al business, quale l'adozione

di un nuovo applicativo.
La crescente ed economica disponibilità di servizi in cloud facilita l'adozione di più efficaci soluzioni di replica dei dati, di disaster recovery e di business continuity, come evidenziato nel Rapporto, ma tali soluzioni sono adottate prevalentemente da medie/grandi organizzazioni.
La difesa proattiva è ancora più un obiettivo a tendere che una realtà, considerando in particolare l'enorme numero di piccole e piccolissime imprese, molte delle quali non effettuano nemmeno un sistematico back up, con molte difficoltà nel ripristinare la situazione ex ante in caso di attacco/incidente.
La sicurezza assoluta non esiste e non può esistere, e gli attacchi si fanno sempre più sofisticati e complessi. Le misure di sicurezza non possono essere solo tecniche, e non possono essere considerate una commodity. Sono le misure organizzative quelle che incidono maggiormente sulla sicurezza informatica, tenendo conto che la vulnerabilità più critica è data dall'essere umano, sia utente sia operatore dell'ICT. E le misure organizzative, per essere efficaci, devono essere contestualizzate, se non personalizzate, alla specifica realtà in cui devono essere calate.

Le evidenze sui temi più attuali
La discussione nella TR si è poi focalizzata su alcuni temi specifici, anche grazie ad alcuni dati del Rapporto 2015.
1) Il livello di maturità della sicurezza informatica dipende dal livello di competenza delle persone che la governano e la gestiscono. La formazione dei tecnici e la sensibilizzazione dei decisori aziendali sono condizioni 'sine qua non', per le quali le due associazioni sponsor, Aica ed Aipsi, stanno collaborando per attuare corsi e certificazioni in linea con la recente normativa UNI 11506 (che fa riferimento all'eCF) specificata nel D.Lgs 13/2013 sulla riorganizzazione nazionale delle certificazioni per le professioni non regolamentate da Ordini. La richiesta nei capitolati, soprattutto delle Pubbliche Amministrazioni, di esperti certificati secondo le nuove norme dovrebbe essere il fattore trainante, ma a due anni dalla legge siamo ancora in una fase embrionale.
2) In Italia, seppur lentamente, stanno diffondendosi tecniche di identificazione biometrica, in particolare la grafometria per la gestione di documenti digitali con firme autografe. Ma se qualcuno accede illegalmente agli identificativi biometrici e li usa, come ci si può difendere? Non si può, nel breve periodo, ed occorre che le registrazioni degli identificativi biometrici siano realmente inviolabili. Come ottenere tale obiettivo e come 'certificarlo'? Si è evidenziato come non tutte le soluzioni presenti sul mercato abbiano un medesimo livello di sicurezza, ma come, al momento, sia difficile per un cliente discernere tra loro. Certificazioni di autorevoli terze parti, oltre che una seria pubblicità comparativa, possono essere le prime risposte al problema.
3) Il Rapporto evidenzia come quasi la metà dei rispondenti già svolge, o intende svolgere, una periodica analisi del rischio. Il dato, nella attuale situazione italiana, è assai positivo e indica come diversi passi in avanti 'culturali' siano stati fatti.
4) Gli attacchi TA ed APT, di cui il Rapporto evidenzia una crescita non trascurabile tra il 2013 e il 2014, sono di difficile individuazione e riconoscimento.

GLI ESPERTI DELLA TAVOLA ROTONDA

Pierpaolo Alì, *south europe sales manager di HP Enterprise Security Products.*
Stefano Barboni, CEO di Riesko.
Roberto Bellini, vice presidente di Aica.
Lorenzo Betti, CEO di Soiel International.
Mariangela Fagnani, ICT security & governance senior advisor di Sernet.
Fabio Inches di Business-e.
Elio Molteni, presidente di Aipsi.
Gastone Nencini, country manager di Trend Micro Italia.
Mario Pitassi, CEO di Technology Estate.

Marco R. A. Bozzetti, *OAI founder*
marco.bozzetti@malaboadvisoring.it