OsservatoriO
AttacchInformatici

Attacchi e frodi: un binomio sempre più stretto e con un preoccupante aumento nel 2011

Nel corso del convegno ISSA-AIPSI si è analizzato lo stato della sicurezza ICT in Italia, considerando anche i problemi legati a cloud computing e dispositivi mobili.

M.R.A.Bozzetti, OAI founder

In occasione del Convegno annuale ISSA-AIPSI tenuto a Roma lo scorso 9 novembre, si è fatto il punto sullo stato dell'arte della sicurezza ICT in Italia, con particolare focalizzazione sui 'nuovi' problemi derivanti dal cloud computing e dai dispositivi mobili. Oltre alla distribuzione del Rapporto OAI 2011 e alla presentazione dei dati più significativi emersi, di particolare interesse sugli attacchi sono stati alcuni interventi, in particolare quelli di **Kevin L. Richards**, presidente dell'intera ISSA internazionale, di **Antonio Apruzzese**, direttore Polizia Postale e Comunicazioni, e dei responsabili del Comitato Tecnico Antifrode delle telecomunicazioni (CTA).

In estrema sintesi, il quadro sulla sicurezza ICT emerso dal convegno è in linea con quanto riportato nel Rapporto OAI 2011, ed è sintetizzabile nei seguenti punti:

- enorme aumento dei dati ovunque;
- molte organizzazioni, aziendali e di enti pubblici, non hanno o hanno una limitata conoscenza (aggiornata) delle loro risorse ICT;
- il cloud computing sta spostando i dati e i relativi trattamenti al di fuori dell'effettivo controllo da parte dei committenti;
- i dispositivi mobili intelligenti, usati sia in ambito domestico sia di lavoro, proliferano e sono nella maggior parte dei casi al di fuori del controllo dei sistemi di sicurezza aziendali;
- sono attive molte migliaia di botnet che coinvolgono svariati milioni di sistemi e che, insieme alle vulnerabilità 'zero day', stanno invadendo i sistemi informativi e costituiscono una parte significativa del business degli attaccanti per le frodi;
- i rischi non sono statici, ma dinamici, mutevoli, temporali, relativi; per gli attaccanti al contrario i rischi (scoperta, cattura, pena) sono bassi e le ricompense in caso di successo sono significative;
- gli attacchi sono sempre più sofisticati e mirati: originati in diverse parti del mondo, costituiti da diverse fasi successive e organizzati in modo 'scientifico', condotti su un periodo di tempo lungo: gli APT, approfonditi in un precedente articolo (Office Automation, aprile 2011);
- da varie indagini, inclusa una recente di Accenture, emerge che sicurezza e privacy sono le principali motivazioni per non adottare soluzioni di cloud, soprattutto di tipo pubblico;
- a fronte dell'occorrenza di attacchi, cresce ed è più intensa la presenza sui media con un'alta esposizione per le aziende coinvolte;
- considerando anche la perdurante crisi economica mondiale, i budget e gli staff relativi alla sicurezza ICT continuano a restringersi, dando ulteriore spazio agli attaccanti.

La mobilità è divenuta un fattore molto critico per la sicurezza dei sistema informativi, anche se ormai è un elemento imprescindibile per la sua funzionalità e comodità. Il problema è che per i dispositivi mobili, ormai intelligenti come se non più di un personal computer, non si adottano ancora le misure di sicurezza che si usano normalmente per un PC. A conferma, da un'indagine Forrester negli USA, emerge che sui dispositivi mobili:

- il cambio o recovery password è il principale problema per il 55% delle aziende;
- sono troppe le password da ricordare: l'87% delle aziende richiedono ai loro utenti di avere 2 o più password per accedere ai sistemi, il 27% hanno 6 o più password;
- le password sono deboli: 1 utente su 5 utilizza password molto semplici e solo il 30% richiede un'autenticazione forte (strong authentication).

I dispositivi mobili intelligenti hanno anche un ruolo crescente nel 'mobile banking' e tendono a diventare nel prossimo futuro il 'borsellino elettronico' per i piccoli pagamenti in ambito retail: si va diffondendo anche in Italia l'uso del cellulare per il pagamento dei parcheggi, dei mezzi di trasporto, e nel breve – medio tempo per acquisti al bar.

Frodi con furto dei contenuti delle carte di credito

Nel corso del convegno, Apruzzese ha ribadito come ormai la quasi totalità degli attacchi è finalizzata a frodi e a crimini di tipo economico. Tra i vari concetti discussi, ha descritto un tipico esempio di frode e di organizzazione criminale, di recente scoperta e debellata dalla Polizia delle Comunicazioni, che chiaramente evidenzia come da 'piccoli' attacchi per 'piccole' frodi si passa ad ampie azioni ben strutturate per 'grandi' frodi. Due giovani di origine africana, regolarmente immigrati, convinsero alcuni loro connazionali, operanti come portieri d'albergo a Roma, a copiare le carte di credito di alcuni clienti dei loro alberghi. Grazie a questi dati attivarono poi dei 'servizi di pagamento' per altri loro connazionali, tipicamente pagamenti di bollette, di tasse, eccetera. Il pagamento era a debito sui conti degli ignari clienti, e una percentuale del pagamento come guadagno, esentasse, ai truffatori. L'iniziativa ebbe un tale successo, che le copie di carte di credito negli alberghi della sola Roma non bastarono più, e si coinvolsero connazionali in altre città. Con l'incremento del business divenne però chiaro che l'approvvigionamento dei dati dalle carte di credito dei clienti degli alberghi era insufficiente. Furono quindi arruolati due giovani informatici connazionali, con elevate capacità di hacking, che iniziarono a rubare interi file con le identità digitali. Raggiunto questo apice dell'iniziativa, arrivò l'identificazione dei criminali da parte della polizia, che pose fine alla frode.

Frodi nelle TLC

Il fenomeno delle frodi nelle telecomunicazioni, sia mobili sia fisse, è così grave in Italia che per contrastarle le principali società dell'offerta hanno creato un Comitato Tecnico Antifrode, CTA, di cui è attualmente presidente Egidio Paraggio di Wind e vice presidente Simone Pecorelli di Intermatica. Il CTA si articola in due gruppi, uno per la telefonia fissa e l'altro per la telefonia mobile, coordinati rispettivamente da Cristoforo Lignola di Telecom Italia e da Giorgio Corsi di Vodafone. Tutti questi responsabili erano presenti al convegno e in una specifica tavola rotonda hanno illustrato l'attuale situazione. Gran parte delle frodi nelle telecomunicazioni deriva da attacchi informatici, il resto da azioni 'tradizionali', come la falsa sottoscrizione e raggiri su servizi ingannevoli ad alto costo.
A livello mondiale la stima delle perdite dovute a frodi nelle telecomunicazioni è per il 2011 di 40,1 miliardi di dollari, pari al 1,88% dei ricavi complessivi. Le cinque principali frodi riguardano:

- Hacking dei PBX/voicemail per 4,96 miliardi di dollari;
- Sottoscrizione falsa/furto di identità per 4,32 miliardi di dollari;
- International Fraud Revenue Share (IRSF) per 3,84 miliardi di dollari;
- Frode da rivendita di traffico per 2,88 miliardi di dollari;
- Frode da carta di credito per 2,40 miliardi di dollari.

Le stime per il 2011 indicano un calo delle perdite da frodi del 33% rispetto al 2008 (si veda fig.1 sottostante), dovuto alla maggiore efficacia dei programmi anti-frode adottati nel settore ed al rafforzamento della cooperazione tra gli operatori.

	2005	2008	2011	% Var.
Estimated Global Revenues	$1.2 Trillion (USD)	$1.7 Trillion (USD)	$2.1 Trillion (USD)	+26%
Estimated Global Fraud Loss* (recalculated)	$61.3 Billion (USD)	$60.1 Billion (USD)	$40.1 Billion (USD)	–33%
% Loss* (recalculated)	5.11%	3.54%	1.88%	–1.66%

Fig. 1 Perdite da frodi sul fatturato a livello mondiale (Fonte: CFCA, 2011 Global Fraud Loss Survey)

Per contrastare questo genere di frodi, in Italia è stata emanata la direttiva AGCom 418/07/Cons che prevede un tavolo tecnico tra gli operatori e la possibilità per l'utente finale del blocco di chiamata permanente per tutte le numerazioni a più alta criticità, tranne quelle relative ai servizi informazione abbonati.

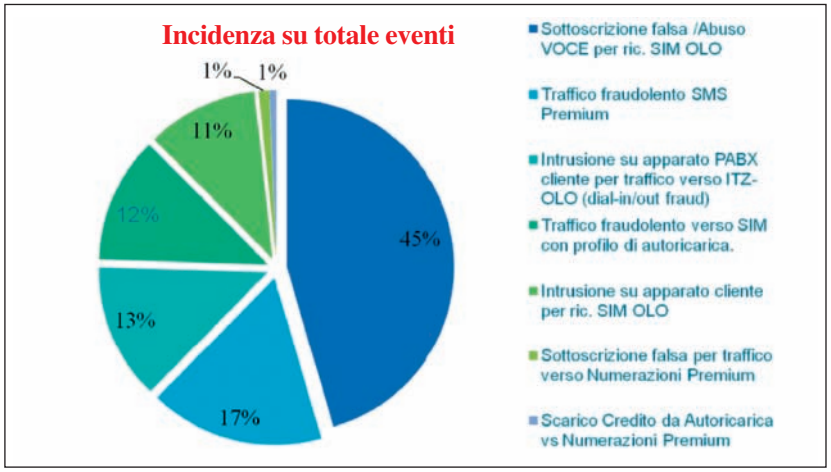

Fig. 2 Ripartizione % degli eventi fraudolenti segnalati nel 1° quad. 2011 (Fonte: CTA)

Per ottemperare a questa disposizione, gli operatori italiani di telecomunicazioni hanno provveduto, tra l'altro, a mettere a punto un Protocollo d'Intesa per la cooperazione nella prevenzione e contrasto delle frodi, realizzando un processo operativo interoperatore per il monitoraggio e la risoluzione congiunta dei tentativi di frode e creando il citato Comitato Tecnico Antifrode in grado di gestire le regole e modalità operative da rispettare per la loro gestione congiunta.

La fig. 2 evidenzia la tipologia di eventi fraudolenti segnalati al CTA nel 1° quadrimestre 2011, che vede al primo posto, per quasi la metà delle denunce, la falsa sottoscrizione e/o l'abuso nella ricarica della SIM.

L'Osservatorio Attacchi Informatici
è sbarcato su Linkedin.

Cerca il gruppo e iscriviti!