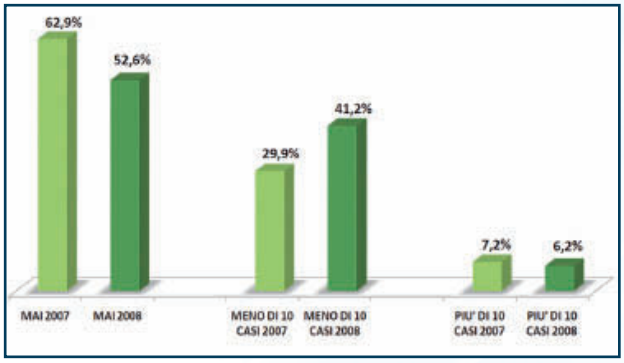
Considerazioni sull'Ultimo Rapporto sugli **Attacchi Informatici in Italia**

Marco Bozzetti | GeaLab - CD Aipsi, ClubTI Milano, FidaInform

FidaInform e ClubTi di Milano hanno deciso di rilanciare l'Osservatorio sugli Attacchi Informatici in Italia (OAI), condotto dal 1997 al 2004 da FTI-Sicurforum, che patrocina la nuova iniziativa insieme ad altri Enti, quali AIPSA, AIPSI, Aused, Inforav e la collaborazione della Polizia delle Comunicazioni. Qui alcuni dati e commenti su quanto emerso dalla consuntivazione delle rilevazioni condotte nel corso del 2009.



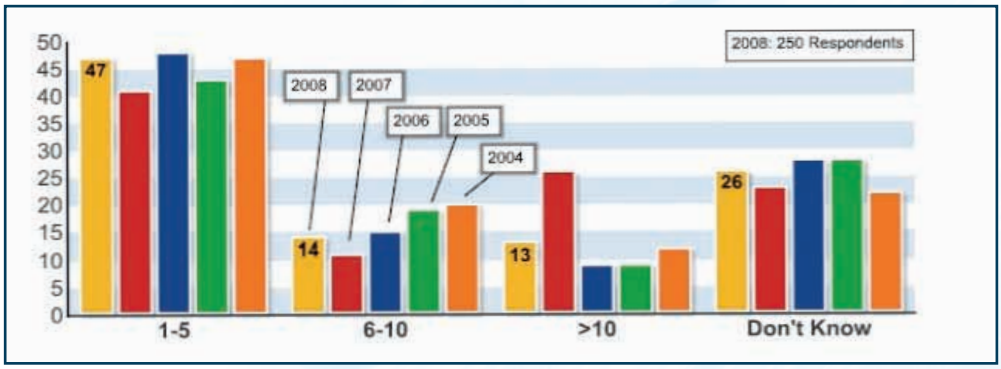


Fig. 1 - Fig. 2 Raffronto tra quantità di attacchi rilevati rispettivamente negli anni 2007 e 2008 in Italia e quelli riportati su scala internazionale per lo stesso periodo, dal Rapporto CSI statunitense del 2008.

L'OAI (Osservatorio sugli Attacchi Informatici in Italia) fornisce concrete indicazioni sugli attacchi ai sistemi informatici delle Aziende e degli Enti Pubblici italiani. Infatti, mentre a livello internazionale ci sono numerosi Rapporti di questo genere, dati specifici riguardanti l'Italia normalmente non ci sono, o se esistono, sono piuttosto carenti o non aggiornati. Così, sebbene la sicurezza informatica, così come le sue minacce, siano di carattere globale, la disponibilità di dati "locali" sugli attacchi rilevati, sulla tipologia e sull'ampiezza del fenomeno risulta fondamentale per effettuare concrete analisi dei rischi e attivare le idonee misure di prevenzione e protezione.

L'OAI avrà cadenza annuale ed il Rapporto 2009, appena pubblicato, rappresenta il "numero 0" iniziale, necessario per la messa a punto del meccanismo di raccolta delle informazioni e per far conoscere l'iniziativa ai responsabili dei sistemi informativi, della sicurezza informatica, e più in generale dei Manager delle imprese.

L'indagine condotta per compilare Rapporto OAI 2009 è stata svolta tramite un questionario compilato OnLine dai CIO (Chief Information Officer), dai CSO (Chief Security Officer) e dai CISO (Chief Information Security Officer) individuati dai vari Patrocinatori, oltre che dal ClubTI di Milano e da Fidainform, di un centinaio di aziende ed enti pubblici centrali e locali, numero valutato positivamente per costituire un campione significativo della popolazione IT nazionale. Per avere un parametro di riferimento, l'analoga iniziativa statunitense CSI, utilizza un campione di circa 500 interlocutori per tutti gli Stati del Nord America.

I compilatori hanno potuto rimanere anonimi, e per ovvi motivi di riservatezza, non sono state chieste loro informazioni di dettaglio sull'azienda/ente e sui sistemi informativi, così da non consentire di risalire alla stessa.

Nella figura 1 è stata evidenziata la quantità di attacchi rilevati rispettivamente negli anni 2007 e 2008, come valore in percentuale sul totale dei rispondenti, e come il singolo attacco sia spesso iterato più volte. Tali dati sono in linea con quelli riportati da analisi internazionali per lo stesso periodo, così come confema la figura 2 che riporta i trend emersi dal Rapporto CSI statunitense del 2008.

La Tabella 1 mostra i tipi di attacchi più diffusi nel 2008 in Italia, per il campione considerato.

Il primo posto è occupato dai codici maligni, analogamente a quanto rilevato anche da CSI per lo stesso periodo. Al secondo posto per diffusione si trovano gli attacchi di "social engineering", che abbracciano un ampio spettro di casi, tutti relativi al comportamento, alle abitudini, il più delle volte alla disponibilità, alla non conoscenza e alla non malizia dell'utente cui si vogliono carpire fraudolentemente e a sua insaputa informazioni sulle sue identità digitali, quali codici bancari, password e così via.

Una così forte percentuale di attacchi di social engineering è un significativa conferma, anche per l'Italia, che gli attacchi informatici sono sempre più orientati a frodi economiche.

Gli attacchi ai sistemi informativi ci sono sempre stati, e con il loro crescere e diffondersi è cresciuta l'adozione di misure di sicurezza: ma dal 2007 si è avuto, a livello mondiale, un significativo incremento delle frodi informatiche e degli attacchi strutturati ed a fini di lucro.

Il 2007 segna l'ingresso in grande stile della criminalità organizzata nel "business" delle frodi informatiche. A questo fenomeno si affiancano i crescenti timori per attacchi informatici di matrice terroristica e/o di guerra elettronica mirati a colpire le infrastrutture "critiche" di un Paese o di intere aree (sistemi dei trasporti, dell'energia, della finanza, ecc.), infrastrutture ormai gestite totalmente tramite sistemi informatici.

La sicurezza informatica è diventata un problema a livello nazionale ed internazionale, ed è arrivata sui tavoli dei politici e dei governi. Una conferma di questa attenzione è, ad esempio, la nomina a "consigliere" del Presidente Obama per la sicurezza informatica negli USA di Howard Schmidt, precedentemente Presidente di ISSA e per l'Italia la nomina del dott. Domenico Vulpiani a Consigliere ministeriale per il Viminale con delega per la sicurezza informatica, precedentemente Direttore Servizi Polizia Postale delle Comunicazioni della Polizia di Stato.

La Tabella 2 elenca i principali strumenti tecnici ed organizzativi di protezione in uso nei sistemi informativi del campione.

Dall'esame degli strumenti in uso emerge che le aziende/enti sono posizionate nella fascia alta come sicurezza ICT, con sistemi informatici abbastanza ben dotati di strumenti tecnici e organizzativi per la loro sicurezza.

DIFFUSIONE ATTACCHI PER TIPOLOGIA 2008	COPERTURA (%)	GRADUATORIA
Utilizzo codici maligni (malware) sia a livello di posto di lavoro che di server	84%	1°
Attacchi di Social Engineering e di Phishing	58%	2°
Furto di apparati informatici contenenti dati (laptop, hard disk, floppy, nastri, chiavetti	50%	3°
Attacchi alle reti, fisse o wireless, e al DNS (Domain Name System)	42%	4°
Accesso e ed uso non autorizzato degli elaboratori, delle applicazioni supportate e de	34%	5°
Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni ec	28%	6°
Frodi tramite uso improprio o manipolazioni non autorizzate e illegali del software ap	22%	7°

Tab. 1 Gli attacchi più diffusi in Italia (Rapporto 2009 OAI)

Approfondendo l'analisi degli strumenti di sicurezza in uso per settore industriali, dal Rapporto 2009 emerge che:

- i settori servizi (include Banche, Assicurazioni, Utilities, Distribuzione/Retail, Trasporti, Servizi Professionali, Sanità, Istituzioni Finanziarie non Bancarie, Istruzione & Ricerca) e ICT hanno un buon "bilanciamento" tra i diversi tipi di misure e strumenti;

- il settore industria (include l'industria manifatturiera e farmaceutica) è piuttosto carente sui vari strumenti di controllo, monitoraggio,

Tab. 2. I principali strumenti di protezione in uso (Rapporto 2009 OAI)

STRUMENTI E METODOLOGIE DI PROTEZIONE IN USO	%
Antivirus and antispyware	95%
Firewall e DMZ	85%
Identificazione dell'utente con identificativo d'utente e password	84%
VPN (Virtual Private Network)	79%
Strumenti di gestione delle autorizzazioni (Active Directory, Ldap, Access Control List, policy server)	77%
Uso di strumenti per la gestione delle patch, degli aggiornamenti, delle release	60%
Archiviazione e gestione dei log	52%
Politiche (policy) tecnico-organizzative di sicurezza ICT	52%
Uso sistemi ad alta affidabilità	47%
Disaster Recovery Planning	39%
Uso di procedure organizzative formalizzate nel supporto ai processi inerenti la sicurezza informatica	38%
Sistemi di PKI (Public Key Infrastructure)	20%
Identificazione dell'utente "forte" con certificati digitali	20%
Identificazione dell'utente biometrica	6%

FIDAInform ed i ClubTI

FIDAInform è la Federazione Nazionale delle Associazioni Professionali di Information Management sviluppatesi spontaneamente a partire dal 1984 in diverse regioni italiane come associazioni di professionisti dell'ICT che vi partecipano a livello personale e non aziendale. I Club e la Federazione si propongono come "nodo" attivo del Sistema-Paese per lo sviluppo del Settore delle tecnologie dell'Informazione e della Comunicazione, promuovendo la professionalità dei Soci. FIDAInform è governata da un proprio Statuto e da un Consiglio Direttivo. Organizza iniziative proprie, a valenza nazionale ed internazionale, oltre a supportare quelle locali dei singoli Club. I ClubTI federati, per totale di circa 1000 Soci, sono ad oggi i ClubTI di Campania, Marche, Milano, Emilia Romagna, Liguria, Puglia, Triveneto, Umbria ed i Club Dirigenti di Informatica di Torino e Roma.Il sito di FidaInform è ***www.fidainform.com****.*

IPS/IDS, e sui sistemi più avanzati di identificazione e autenticazione;

• le PA (Pubbliche Amministrazioni sia Centrali che Locali) non dispongono o dispongono in maniera ridotta di sistemi ad alta affidabilità, di strumenti di crittografia, di autenticazione forte degli utenti. È anche limitata la diffusione di policy della sicurezza e delle procedure organizzative.

Di particolare importanza gli aspetti organizzativi per gestire correttamente ed efficacemente la sicurezza di un sistema informativo: aspetti che erano, fino a pochi anni fa, assai deboli se non inesistenti in gran parte delle Aziende/Enti in Italia. La situazione, almeno per i compilatori del questionario, risulta nettamente migliorata: ben il 58% dei rispondenti afferma di avere delle policy di sicurezza. In comincia a diffondersi l'auditing per la sicurezza informatica: ben il 50% dei rispondenti indica che già effettua tale attività, ed il 28% ha pianificato di attuarla a breve.

E' possibile scaricare gratuitamente il Rapporto 2009 integrale dai seguenti siti: www.fidainform.it; www.clubtimilano.net; www.aipsi.org.

I prossimi passi dell'iniziativa OAI

Come indicato all'inizio del presente articolo, l'iniziativa OAI intende produrre ogni anno un Rapporto. Si sta già impostando la raccolta on-line delle risposte per il prossimo Rapporto OAI 2010, che farà riferimento agli attacchi rilevati nell'intero arco del 2009 e nel primo trimestre 2010:

- migliorando il questionario;
- coinvolgendo come patrocinatori altre Associazioni ed Istituzioni ;
- ampliando e bilanciando meglio il numero di rispondenti per settore.

Il nuovo questionario on line su web per il 2010 sarà disponibile per la fine di giugno/primi di luglio 2010, e la disponibilità del Rapporto 2010 è prevista entro fine ottobre 2010.

L'Ing. Marco Rodolfo Alessandro Bozzetti, autore del Report, si occupa di ICT da più di 35 anni, avendo operato con responsabilità crescenti presso primarie imprese di produzione, quali Olivetti e Italtel, e di consulenza. È stato anche il primo responsabile dei sistemi informativi dell'intero Gruppo ENI. È Amministratore unico di Malabo (www.malaboadvisoring.it) e opera con GeaLab (www.gealab.it), società di consulenza direzionale operante nell'ICT che nasce da GEA Consulenti Associati di Direzione Aziendale (www.gea.it).

È stato uno dei primi a livello mondiale a occuparsi di internetworking e di sicurezza ICT, e fu ideatore di EITO, European IT Observatory, e di OCI, Osservatorio Criminalità ICT in Italia, pubblicato dall'FTI, Forum delle Tecnologie dell'Informazione. È stato Presidente di FidaInform, di SicurForum in FTI e del ClubTI di Milano, oltre che componente del Consiglio del Terziario Innovativo di Assolombarda. È ora membro del Consiglio Direttivo di FIDAInform, del ClubTI di Milano e di AIPSI, Socio fondatore e componente del Comitato Scientifico dell'FTI, socio di itSMF. Ha pubblicato articoli e libri sull'evoluzione tecnologica, la sicurezza informatica e sul lavoro, gli scenari e gli impatti dell'ICT. Appassionato di alpinismo e sci, pratica anche vela, sub e golf. ■