

Dall'Osservatorio Attacchi Informatici in Italia

Rapporto OAI 2010

Contribuiamo numerosi per il settore Pubblica Amministrazione!

Il 2009 ha visto la prima edizione dell'iniziativa OAI, Osservatorio Attacchi Informatici in Italia. Il successo, sia in termini di dati raccolti che di spunti ricavati dagli stessi, ha spinto i promotori a proporre l'Osservatorio su base annuale, perché diventi così un appuntamento costante, autorevole e indipendente, sulla sicurezza ICT in Italia, analogamente a quanto avviene con il Rapporto CSI statunitense. Ad ulteriore sostegno del valore dell'iniziativa, per l'edizione 2010 di OAI è prevista un'introduzione del dott. Domenico Vulpiani, Consigliere ministeriale per il Viminale con delega per la sicurezza informatica, precedentemente Direttore Servizi Polizia Postale delle Comunicazioni della Polizia di Stato.

Un altro obiettivo dell'Osservatorio OAI è far conoscere, aggiornare e sensibilizzare sia gli esperti e i responsabili della sicurezza informatica sia, soprattutto, i vertici delle Aziende/Enti su cosa realmente avviene in Italia sugli attacchi intenzionali ai sistemi informatici. Perché l'Osservatorio abbia successo e possa essere un punto di riferimento affidabile sul mercato, è indispensabile la colla-

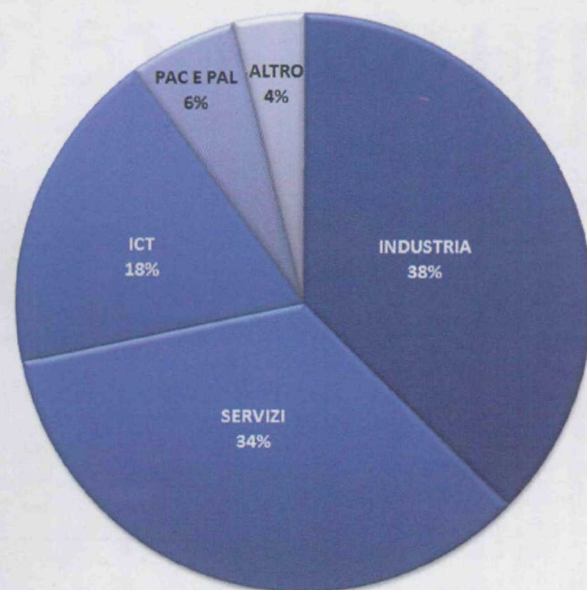
borazione quali-quantitativa dei responsabili delle aziende pubbliche e private nella compilazione del questionario on line. Altro elemento importante che definisce il valore dell'Osservatorio è costituito da un'adeguata rappresentanza delle aziende che vengono monitorate dal questionario. Nella raccolta dei dati del primo Osservatorio, purtroppo, il contributo della Pubblica Amministrazione sia locale che centrale è stato molto modesto (vedi grafico), anche perché ottenere informazioni in questo specifico contesto non è semplice, poiché molte sono le policy che costringono al silenzio sugli attacchi subiti e sulla tipologia degli stessi. Questo per non esporli troppo e non rischiare di subire ulteriori attacchi, cosa che costituirebbe danno grave per quelle attività che gestiscono le risorse e i riferimenti del Paese.

D'altro canto, è anche vero che, per meglio affrontare i crescenti e sempre più sofisticati attacchi, occorre conoscerli e sapere come affrontarli e prevenirli. Per questo motivo il questionario può essere compilato nella più completa anonimata, favorendo, da un lato, la tutela del compilatore, ma garan-

tendo, dall'altro, la disponibilità di una messe di dati di aziende diverse utili, così a rendere autorevole l'Osservatorio. Il questionario, la cui compilazione richiede un tempo contenuto, è strutturato in modo che le informazioni richieste non permettano di risalire a dettagli implementativi o a informazioni riservate sulla natura e il tipo del sistema informativo e del sistema di sicurezza informatica in uso. Le informazioni inserite saranno comunque gestite solo a fini statistici per la creazione del Rapporto 2010 OAI. A tutti i compilatori che vorranno indicare un loro indirizzo di posta elettronica, verrà inviato in anteprima il Rapporto finale, naturalmente garantendo che tale informazione non sarà né divulgata né collegata ai dati del questionario, che rimarranno riservati e anonimi.

L'iniziativa OAI è ancora giovane, ma inizia a essere conosciuta e apprezzata: ad oggi, è l'unica indipendente realizzata in Italia, non

<http://www.soiel.it/questionarioOAI2010/pagina1.html>



Suddivisione per macro settore dei compilatori del questionario

proveniente da società dell'offerta. Il questionario è disponibile on line all'indirizzo indicato, e fa riferimento agli attacchi subiti nel 2009 e nel primo quadrimestre 2010.

OAI è promosso e attuato dal ClubTI di Milano, da FidaInform (www.fidainform.it), la Federazione dei ClubTI Italiani e dall'Editore Soiel International (www.soiel.it), con il Patrocinio di AIPSA (Associazione Italiana Professionisti Security Aziendale), AIPSI (Associazione

Italiana Professionisti Sicurezza Informatica), Assintel di Confcommercio (Associazione Nazionale Imprese ICT), Assolombarda di Confindustria, Aused (Associazione Utilizzatori Sistemi e Tecnologie dell'informazione), Inforav (Istituto per lo sviluppo e la gestione avanzata dell'informazione), itSMF Italia (Information Technology Service Management Forum) e con la collaborazione della Polizia delle Comunicazioni.

IL PUNTO DI VISTA DI GFI

Attacco a LinkedIn

Nei giorni scorsi, il social network professionale LinkedIn è stato vittima di un imponente attacco che ha messo a rischio gli account dei suoi utenti. Come riportato dagli esperti di Cisco, l'attacco è stato individuato qualche giorno fa, ed è ancora in circolazione. Si tratta di e-mail di spam, indirizzate ai membri della rete sociale professionale che hanno ricevuto messaggi di posta con false richieste di contatto che contengono un link malevolo. Cliccando direttamente sul link contenuto nell'e-mail, bastano 4 secondi affinché il malware possa infettare il pc e sottrarre le informazioni degli utenti. Sebbene non si tratti della prima volta che i criminali informatici lancino un attacco criminale verso brand noti di social media online, il carattere professionale di LinkedIn, ed il fatto che questo network non fosse mai stato direttamente attaccato finora, hanno evidentemente amplificato ulteriormente la notizia. I social network sono bersagli particolarmente appetibili per i cyber criminali, per la portata degli utenti potenzialmente raggiungibili e perché sfruttano caratteristiche quali la fiducia verso gli altri utenti della comunità e del network a cui si è connessi. GFI ribadisce che questo genere di attacchi sono piuttosto comuni e allerta gli utenti su alcune utili abitudini di

sicurezza che possono aiutare a non cadere vittime di questo genere di trappole, a distinguere le e-mail malevole da quelle autentiche di LinkedIn, e non solo:

1. mantenere il software di sicurezza antispam e antivirus costantemente aggiornato all'ultima versione disponibile;
2. se il mittente è sconosciuto, è opportuno cancellare l'email di invito. In ogni caso, controllare i messaggi accedendo al proprio account LinkedIn, mai cliccando direttamente il link contenuto nell'email;
3. le aziende o gli utenti che fanno un uso massiccio di operazioni di banking online dovrebbero avere un computer dedicato che non presenti altre applicazioni;
4. le piccole aziende dovrebbero installare un gateway antivirus e antispam per utilizzare un servizio hosted di e-mail filtering, come ad esempio GFI MAX MailProtection, oltre a delle specifiche soluzioni antivirus (come ad esempio VIPRE Premium), che preven- gono e sono in grado di bloccare questo tipo di attacchi nel caso un utente clicchi accidentalmente su un link malevolo.

GFI MailEssentials blocca infatti questi tipi di spam utilizzando Spamrazer, che grazie agli aggiornamenti costanti e a URI DNS Blocklist è in grado di bloccare immediatamente questi nuovi invasori.

RSA PROTEGGE I PIÙ PICCOLI

Consigli per i genitori

Trascorrendo sempre più tempo online e intrecciando nuove relazioni sul Web, che si tratti di siti di social networking, della ricerca di informazioni o di shopping on line, è importante far conoscere ai più giovani alcune misure di sicurezza per proteggerli. Per essere sicuri on line non è necessario essere degli esperti di tecnologia, ma sapere fare le scelte giuste, analisi critiche e relazionarsi con gli altri sul Web in modo appropriato. Come i genitori conoscono bene l'importanza di educare e supportare i propri figli nella vita di tutti i giorni, allo stesso modo possono aiutarli a navigare e ad usare il PC in maniera consapevole e sicura. Per questo, RSA ha creato una serie di semplici consigli per iniziare il percorso verso una navigazione più sicura di tutta la famiglia:

- posizionare il computer di casa in una stanza centrale, e non in una camera appartata.

È importante essere a conoscenza dell'esistenza di

- ogni PC che i vostri figli potrebbero utilizzare;
- impostare alcune semplici regole e linee guida per le attività dei ragazzi quando navigano on line e lasciarle sul computer come promemoria;
- impostare i parental control del browser cliccando in "Strumenti" dalla barra del menu, poi "Opzioni Internet" e "Contenuti", e selezionare il pulsante "Attiva" sotto "Contenuto verificato";
- considerare l'eventuale acquisto di un software che consenta di monitorare le attività online;
- conoscere le persone con cui sono in contatto i figli e supervisionare mentre chattano con qualcuno;
- sottolineare l'importanza di non dare informazioni personali quando sono on line;
- Se vostro figlio si ritrova in situazione pericolosa, informatevi su chi poter contattare (www.getnetwise.org), o contattate direttamente le forze dell'ordine in caso di pericolo immediato.

Scanner Kodak

www.kodak.com
Per ulteriori informazioni contattare i numeri 02-66028.338 / 06-88172.232
o scrivere a: it-di@kodak.com

Kodak