Indice

1. NUOVI SOCI

Hanno aderito al Clusit:

- Ce.S.I.A. - Centro Servizi Informatici di Ateneo - Università di Bologna (Bologna);
- GST Group (Cinisello Balsamo - MI);
- Kryptos (Trebaseleghe - PD);
- Ragioneria Generale dello Stato - Ministero dell'Economia e delle Finanze (Roma).

2. APPLET JAVA COME I CONTROLLI ACTIVEX ?

Un interessante posting sul security blog di ZDNet http://blogs.zdnet.com/security/?p=946&tag=nl.e539 esamina svariati meccanismi possibili per compromettere uno dei meccanismi principali su cui si basa la sicurezza di Internet - la Same Origin Policy, ovvero il concetto che un'applet scaricata da un certo sito possa comunicare soltanto con quel sito (salvo che sia digitalmente firmata).

In sostanza, facendo sì che il browser, "credendo" di comunicare con il sito d'origine dell'applet, in realtà lasci che l'applet usi liberamente la rete, ad esempio per fare un attacco brute force contro un server interno, normalmente schermato dal firewall se attaccato da Internet, ma accessibile dalla rete interna , che, più per disattenzione che altro, consideriamo più fidata.

Lo scenario che si apre è inquietante: la Same Origin Policy è uno dei pilastri della sicurezza su Internet almeno dal 1996, ma già fin d'ora è necessario rivedere quanto ci possiamo affidare ad essa. Non è una vera e propria fuoruscita di Java dalla sua sandbox, ma da parecchio tempo non si registravano attacchi così sofisticati e, tutto sommato, fatti su vulnerabilità non causate da banali errori di programmazione. Il post

promette peraltro un seguito in cui la sandbox venga pienamente abbandonata, con tutti i rischi che ne conseguono.

In conclusione, rimangono sempre valide alcune raccomandazioni. La prima è quella di segmentare e controllare anche la rete interna, perché il lupo spesso è in mezzo al gregge, e morde anche se fino ad un attimo fa era una pecora.

La seconda raccomandazione sarebbe quella di sottoporre ad audit tutto il software. Questo purtroppo non è praticamente fattibile: rimane quindi necessario, come minimo, fare moltissima attenzione a cosa si lascia entrare sul proprio sistema. Avere un software di sicurezza (antivirus, antispyware, personal firewall, ecc.) aggiornato ed all'erta può aiutare.

(Autore: Mauro Cicognini)

3. GUIDA ADICONSUM E ANSSAIF SUL FURTO DI IDENTITÀ

Adiconsum, in collaborazione con Anssaif (Associazione nazionale specialisti sicurezza in aziende di intermediazione finanziaria) e Cec (Centro europeo consumatori), ha presentato il volumetto **Il furto di identità**, con l'obiettivo di mettere in guardia cittadini e consumatori su furbizie, raggiri e truffe su privacy e furti d'identità realizzati attraverso le nuove tecnologie. Secondo i dati forniti dall'associazione dei consumatori, le frodi sono costate alle tasche degli utenti circa 80 milioni di euro, per un importo medio dei casi denunciati pari a 5.300 euro.

Fonte:
www.ilsole24ore.com/art/SoleOnLine4/Tecnologia%20e%20Business/2008/03/furti-identita-vademecum.shtml?uuid=32cd4a1c-fcbe-11dc-a602-00000e251029&DocRulesView=Libero)

Il volumetto è scaricabile da
www.anssaif.it/allegati/IlFurtodiIdentitàADICONSUMANSSAIFdoc2_271.pdf

4. COSTITUZIONE DEL FORUM DELLE COMPETENZE DIGITALI

il 5 marzo il Clusit ha partecipato, assieme ad altre 17 associazioni, alla costituzione del **Forum delle competenze digitali**, che si occuperà di competenze e professionalità nel settore dell'ICMT (Information, Comunication & Media Technology) e delle Tecnologie.

Il Forum avrà sede a Roma presso l'Inforav (Istituto per lo sviluppo e la gestione avanzata dell'informazione)

Sono stati nominati, e rimarranno in carica per i primi tre anni:

- Presidente, l'Ing. Maurizio Bufalini (Presidente Inforav)
- Vicepresidente, l'Ing. Roberto Bellini (Presidente della Sezione AICA di Milano)
- Segretario Generale, l'Ing. Francesco Arciprete.

Il Dott. Massimiliano Manzetti (CD Clusit) siederà nel Comitato Direttivo del Forum

5. SCARSA CONOSCENZA DELLE BEST PRACTICE

La difficoltà principale nella sicurezza oggi... secondo un recente report canadese www.cata.ca/Media_and_Events/Press_Releases/cata_pr02110802.html, è (ancora) la scarsa conoscenza delle best practice.

Come si scrive anche in un articolo di Network World www.networkworld.com/news/2008/030708-it-security-lacking-in-best.html, ciò è sorprendente, visto che ormai da molti anni si insiste sulla necessità di adottare un approccio sistematico all'IT Security, per non farsi trascinare dalle mode tecnologiche del momento.

Dovrebbe essere ormai ben conosciuta anche la filosofia di "miglioramento continuo" che sta alla base di tutti i metodi formali (CoBIT, ISO27000, ecc.) che indirizzano a vario titolo il tema della sicurezza delle informazioni; inoltre, sono da tempo disponibili ricchi contenuti anche a livello di istruzioni di dettaglio: spesso gratuiti, o comunque a prezzi assolutamente accessibili (p.e. il prezzo di un buon libro).

A mio parere non ci sono scuse, salvo, per assurdo, il fatto che una tale mole di documentazione può spaventare il non iniziato: ed è corretto, in questo caso, affidarsi ad uno specialista, così come si fa con i medici.

Questo non ci esime, tuttavia, dal conoscere le regole di base, e saper distinguere un'aspirina da uno sciroppo per la tosse credo sia possibile e doveroso per tutti, anche in tema di sicurezza informatica.

Autore: Mauro Cicognini

6. MEHARI 2007

I colleghi del Clusif hanno messo a disposizione, in libera consultazione, la versione 2007 della metodologia MEHARI.

Tutta la documentazione è disponibile in francese ed inglese e parzialmente in altre lingue su

https://www.clusif.asso.fr/fr/production/ouvrages/type.asp?id=METHODES.

Sul sito del Clusit, tra i whitepapers, è disponibile la versione aggiornata, in italiano, della presentazione generale della metodologia MEHARI: www.clusit.it/whitepapers/mehari_2007.pdf

Ringraziamo Massimiliano Manzetti, che ha realizzato la versione italiana della presentazione.

7. NOTIZIE E SEGNALAZIONI DAI SOCI

La deadline per l'invio di eventuali segnalazioni dei soci per la pubblicazione sulla newsletter è il 25 di ogni mese

Alla ricerca di nuove motivazioni professionali, è disponibile una figura professionale di livello manageriale con pluriennale esperienza negli ambiti Information Technology, Security e Business Continuity

Management. Tale esperienza è maturata all'interno di un istituto di credito facente parte di un importante gruppo bancario internazionale, dove ha avuto la responsabilità di progetti per l'evoluzione del livello di Security aziendale aderente agli standard ISO270001 e di progetti per la Business Continuity e Disaster Recovery secondo la metodologia BS25999. Nelle precedenti esperienze ha avuto responsabilità di progettazione del Sistema Informativo e di Organizzazione della funzione IT.

Le aziende interessate possono scrivere a info@clusit.it

LoCSI e **LoCSI-PMI** di AIPSI: grandfathering ed esami

AIPSI, Associazione Italiana Professionisti della Sicurezza Informatica, ha creato due certificazioni professionali destinate ad attestare le competenze del professionista della sicurezza informatica rispetto alla conoscenza delle norme, regolamenti e legislazione Italiana ed Europea attinenti.

Le certificazioni LoCSI costituiscono un vantaggio per i professionisti ma anche per le aziende. Esse permettono di attestare e far riconoscere le proprie competenze specifiche per il contesto italiano, facilitando così lo sviluppo della propria carriera e offrendo alle aziende clienti la certezza di rivolgersi a personale specializzato e competente.

Per ottenere la certificazione, il candidato deve superare un esame per il quale è prevista la prima sessione il 10 maggio 2008 a Milano e Roma.

Dal 15 febbraio 2008 al 31 marzo 2008 è inoltre possibile conseguire la certificazione LoCSI o LoCSI PMI partecipando alla prima sessione del programma "grandfathering", un meccanismo attraverso il quale professionisti, che in ogni caso soddisfino i requisiti per ottenere le suddette certificazioni, possono ottenere la certificazione attraverso una procedura semplificata che non prevede l'esame. I dettagli per l'ottenimento delle certificazioni, sia tramite l'esame sia attraverso il grandfathering, sono consultabili sul sito AIPSI nell'area "Certificazione".

Per maggiori informazioni consultare il sito www.aipsi.org.

8. EVENTI SICUREZZA

2 aprile 2008, Milano

Seminario Clusit - Computer forensics: aspetti legali e strumenti operativi

https://edu.clusit.it/scheda_seminario.php?id=20

2-3 aprile 2008, Amsterdam

Forrester's Security Forum EMEA 2008 (Sconto 20% per i soci Clusit)

www.forrester.com/events/eventdetail?eventID=2068

11 aprile 2008, Verona

Nuove tecnologie: Possono cambiare il nostro modo di lavorare?

www.alba.st/invito1104.pdf

19 aprile 2008, Monza
Esame CISSP
www.clusit.it/isc2/calendario_isc2.htm

22 aprile 2008, San Donato - MI
Wlan Business Forum 2008 e M2M Forum 2008
www.wlanforum.eu - www.m2mforum.com

22-24 aprile 2008, Londra
Infosecurity Europe
www.infosecworld.com/page.cfm/Link=11/t=m/goSection=4

22 maggio 2008, Roma
Seminario Clusit - Computer forensics: aspetti legali e strumenti operativi
https://edu.clusit.it/scheda_seminario.php?id=22

5 giugno 2008, Firenze
Seminario Clusit: Dal Penetration Testing alla Risk Analysis: la metodologia OSSTMM 3.0, lo standard ISO 27001 ed i punti di incontro
https://edu.clusit.it/scheda_seminario.php?id=23

10-11 giugno 2008, Roma
Infosecurity Italia - Storage Expo - trackability
www.infosecurity.it/IT/roadshow/roma%202008.aspx

10 giugno 2008, Roma
Seminario Clusit: Dal Penetration Testing alla Risk Analysis: la metodologia OSSTMM 3.0, lo standard ISO 27001 ed i punti di incontro

CLUSIT - ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA*
Dipartimento di Informatica e Comunicazione
Università degli Studi di Milano
Via Comelico 39 - 20135 MILANO - cell. 347.2319285
* associazione senza fini di lucro, costituita il 4 luglio 2000