Indice

1. NUOVI SOCI

Hanno aderito al Clusit:

- Autorità per le Garanzie nelle Comunicazioni (Napoli)
- Cheapware Informatica (Palermo)
- CIDICA (Milano)

2. GERMAN EU COUNCIL PRESIDENCY - INTERNATIONAL CONFERENCE *IT SECURITY 2007*

Il ministero dell'interno Tedesco, nell'ambito del semestre di presidenza della UE organizza il 4 e 5 giugno una conferenza sulla sicurezza informatica.

Interverranno tra gli altri:

- Wolfgang Schäuble, Federal Minister of the Interior
- Viviane Reding, EU Commissioner for the Information Society and Media – tbc
- Willi Berchtold, President of the Federal Association for Information Technology, Telecommunications and New Media e.V. (BITKOM e.V.) – tbc
- Andrea Pirotti, Executive Director of the European Network and Information Security Agency (ENISA).

Il Clusit sarà presente col suo presidente, Gigi Tagliapietra, che è stato invitato a presentare in seduta plenaria i risultati di un gruppo di lavoro dell'ENISA che si è occupato di iniziative di awareness a favore dei cittadini.

Il secondo giorno, in particolare, si affronterà anche il tema di un "CERT per icittadini", per il quale alcuni paesi presenteranno delle iniziative che le proprie istituzioni nazionali stanno già realizzando.

Il Clusit sta proprio lavorando, in collaborazione con le istituzioni nazionali, ad un progetto che prevede, tra l'altro, un servizio di assistenza online dedicato ai cittadini e il presidente Tagliapietra non mancherà di portare il suo contributo alla discussione.

3. INFOSECURITY ROMA: UN'APERTURA DI GRANDE PRESTIGIO

Il giorno 5 giugno, per la manifestazione di apertura di Infosecurity Roma (5-6 giugno), siamo riusciti a coinvolgere le istituzioni ai più alti livelli.

Dopo il benvenuto e l'apertura dei lavori da parte del Ministro delle Comunicazioni, Paolo Gentiloni (*), si terrà una tavola Rotonda con i rappresentanti delle Istituzioni, con la partecipazione eccezionale del Segretario Generale dell'ITU (*), dal titolo:

"Sicurezza delle informazioni e dei sistemi come servizio per il cittadino e le imprese"

Moderatore: Luca De Biase, Capo Redattore Nova24 (Sole24Ore)

Partecipanti alla Tavola Rotonda:

- Hamadoun Touré, Segretario Generale ITU
- Luigi Nicolais, Ministro per le Riforme e l'Innovazione nella Pubblica Amministrazione
- Luigi Vimercati, Sottosegretario di Stato - Ministero delle Comunicazioni
- Francesco Pizzetti, Presidente dell'Autorità Garante per la protezione dei dati
- Danilo Bruschi, Presidente Onorario Clusit

(*) In attesa di conferma

4. CYBERCRIME

Riportiamo integralmente un interessante articolo apparso sull'ultima newsletter ANSSAIF (www.anssaif.it).

Durante il convegno ANSSAIF tenutosi a Vallombrosa lo scorso settembre 2006 ho presentato gli attuali limiti, rischi e i metodi di attacco che possono minare la fiducia del consumatore nel sistema di autenticazione a due fattori (two-factor authentication).

A luglio 2006 l'americana CityBank è stata vittima di un attacco di quello che definisco come il nuovo phishing: per maggiori informazioni potete leggere:

http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html

Se quello di CityBank poteva essere una novità nel panorama delle frodi via Internet, con le ultime notizie provenienti dall'Olanda dobbiamo

oramai accettare il fatto che il panorama dei metodi sta cambiando. I clienti della ABM-Amro hanno subito un attacco in aprile 2007 e alcuni conti correnti derubati dei loro soldi (la notizia è riportata su: www.out-law.com/page-7967

Gli attacchi non hanno presentato novità di esecuzione diverse da quelle descritte al convegno: l'utente è attirato su un sito web che opera come proxy del cliente verso la banca. Un perfetto attacco Man-in-the-middle da manuale. Questo dimostra come è oramai poco costoso scrivere codice che possa fare da "corriere" per le credenziali del cliente, aprendo la strada a tutti gli altri gruppi criminali. Il fattore di interesse è che il concetto del "Man-in-the-middle" non è verticale alla tecnologia delle autenticazioni/autorizzazioni a 2 fattori, ma può essere applicato indiscriminatamente a qualunque tipo di trasmissione non istituita in forma esclusiva tra le parti. Prepariamoci quindi a veder sempre di più attacchi in "real-time".

Certamente se i Clienti non cadessero nei trabocchetti delle email "invitanti", evitando quindi di accedere a siti ove i criminali possono inviare ed attivare sul computer della vittima i trojan responsabili dei "dirottamenti" ai siti fasulli, non sarebbero accaduti i casi citati dalla stampa. Ma il Cliente è sempre "padrone", dice il noto adagio, ed allora le aziende di servizio devono affrontare nuovi rischi, nuovi investimenti, se vogliono che il Cliente sia protetto.

Queste le brutte notizie, passiamo ora alle buone.

Abbiamo un immenso vantaggio competitivo sui gruppi criminali: conosciamo i nostri clienti. So che molti di voi, come il sottoscritto, alla menzione del "Behavioral Profiling" si trovano a disagio, ma è anche una delle armi più interessanti contro questi attacchi. Behavioral Profiling è oggi utilizzato negli aeroporti, soprattutto americani, con risultati molto alterni, così come dai grandi gruppi di carte di credito. Cosa

potrebbe fare una banca che non ha mai applicato questa metodologia? Si può cominciare, ad esempio, con operazioni a basso costo, come il controllo della provenienza delle connessioni. Alcune ditte offrono database costantemente aggiornati sulla posizione geografica degli IP. Un investimento di pochi euro, tra database ed implementazione dei controlli, permette di avere il polso della situazione sulla provenienza dei nostri clienti. Se proprio vogliamo essere più sofisticati potremmo legare insieme le posizioni geografiche dei nostri clienti con le operazioni da loro fatte. Questi accorgimenti, con il tempo, ci danno il prezioso vantaggio di poter creare un cruscotto di pre-allarme. Ma i nostri clienti non si contano nelle unità, ma nelle decine di migliaia, a volte nei milioni.

Ecco come il Behavioral Profiling può diventare veramente interessante: osservare un numero rilevante di connessioni originanti dallo stesso IP sito presso uno stato estero, che guarda caso risulta in una lista nera, diventa un ottimo indicatore di un attacco verso i nostri clienti in atto.

Un altro uso degli indicatori geografici è quello relativo alle distanze: è possibile per un cliente collegarsi dall'Italia e, 2 ore dopo, collegarsi dalla Korea? Un certo sospetto diventa legittimo. Interessante l'articolo di Mr. Richard Baker, Chief Identity Architect della BT: www.out-law.com/page-7927, dove ci informa come sta cominciando a profilare i propri clienti

proprio in base alle loro abitudini, aggiungendo così un ulteriore tassello nella maglia della sicurezza contro le frodi telefoniche.

Ma cosa succederà quando tutti faranno Behavioral Profiling? Tra 2 o 3 anni circa cominceremo a vedere collegamenti provenienti dall'interno della nostra nazione, magari sfruttando siti precedentemente hackerati. E allora a cosa sarebbe servito tutto questo sforzo? A guadagnare quei 2 anni che ci servono per implementare una soluzione a lungo termine: estendere le nostre maglie di difesa alla clientela.

Come ho già avuto modo di proporre, perché non estendere il concetto del perimetro di sicurezza anche al cliente? E' oramai indubbio che la soluzione perfetta è parte di un futuro lontano, una firma digitale è ben poca cosa senza un adeguato sistema sicuro. Dobbiamo quindi sempre più investire sul fattore umano, formare i nostri clienti e lavorare insieme ai produttori di browsers, sistemi operativi e gli enti di certificazione (IETF fra tutti) per fornire un adeguato "kit del piccolo meccanico" che non sia invasivo ma al tempo stesso altamente efficace. Un modo per "abbracciare" i nostri clienti, rassicurandoli del fatto che li riconosciamo mantenendoli protetti.

E il "Man-in-the-middle"? Lo ritroveremo di nuovo: cercheranno di inserire programmi nei computer degli utenti allo scopo di manipolare gli stati di memoria, ma converrete anche voi che tra scrivere un programmino in PHP e/o ASP e scrivere un codice Assembler per la manipolazione della memoria esiste una differenza d'investimento elevata, oltre a dover accedere ad un know-how che ad oggi non è particolarmente diffuso. Ed ecco che abbiamo guadagnato altri 3 anni di difesa.

Complessivamente questi investimenti porteranno l'aspettativa di vita delle protezioni a 5/6 anni. E fra 6 anni avremo sistemi che potranno degnamente lavorare a stati di memoria stagni per così implementare le vere firme digitali.

Forse.

I.P.ANSSAIF

5. INCHIESTA SUPSI

Il Dipartimento Tecnologie Innovative della SUPSI (Scuola Universitaria Professionale della Svizzera Italiana) ha promosso un'inchiesta sulla sicurezza informatica nelle piccole e medie aziende della Svizzera italiana per poter capire quanto si sta facendo per la protezione dei dati aziendali e dei sistemi informativi. Sia nel caso di una piccola realtà con pochi computer, così come nella grande organizzazione con una complessa rete aziendali, i risultati raccolti permettono di fare un confronto tra situazioni analoghe, non solo sulle soluzioni tecniche ma anche sui processi e le regole di comportamento.

E possibile consultare i risultati su
www.dti.supsi.ch/Content/main/pdf/X_isi_Documento.pdf

Su http://isi.dti.supsi.ch è anche disponibile uno strumento di analisi dinamica dei dati.

6. NOTIZIE DA AICA

È stato prorogato al 14 Maggio il termine per l'invio delle proposte di contributo (tra i temi richiesti vi è anche "Sicurezza e Privacy") per il prossimo Congresso Nazionale AICA sul tema: "Cittadinanza e Democrazia Digitale" Milano, 20-21 Settembre, Mantova 27-29 Settembre.

Ulteriori informazioni e istruzioni per gli autori sono disponibili sul sito del congresso: www.aicanet.it/congressoaica2007

Il 25 maggio a Milano avrà luogo il primo workshop su "Professioni e Certificazioni Informatiche" organizzato da AICA e Commissione ICT Ordine degli Ingegneri della Provincia di Milano, in collaborazione con Fondazione CRUI e CINI.

Il workshop, che si terrà presso la sede dell'Ordine degli Ingegneri della Provincia di Milano - Corso Venezia 16 alle ore 15, si propone di approfondire il tema delle competenze ICT, della loro classificazione, misurazione e riconoscimento attraverso il modello europeo EUCIP.

La partecipazione al workshop è libera previa registrazione.

Per informazioni e iscrizioni www.aicanet.it/convegni/1070525.htm.

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

Nei giorni 24 e 25 maggio 2007 si terrà il ***XXI Convegno Nazionale AIEA***, presso l'Accademia Navale di Livorno.

L'agenda del convegno è disponibile su:
www.aiea.it/pdf/convegni/livorno%202007/Convegno%20AIEA%202007.doc

Il modulo di iscrizione è disponibile su :
www.aiea.it/pdf/convegni/livorno%202007/Modalita%20iscrizione%20e%20costi.doc

Nei giorni 29 e 30 maggio 2007 si terrà un seminario dal titolo ***La dinamica dei contratti ICT. Dal body rental all'outsourcing***, corso a due voci tenuto da Luigi Vannutelli e Daniela Rocca. Per maggiori informazioni ed iscrizioni: www.iter.it/seminari_01.htm. Per i soci Clusit è previsto uno sconto del 15%.

Il 6 Giugno 2007, in collaborazione con Infosecurity, si terrà a ROMA, presso l'hotel Sheraton Via del Pattinaggio 100, l'edizione 2007 della "***ISSA European Security Conference***".

Si segnalano, fra gli interventi, i due "keynote" (mattino e pomeriggio) rispettivamente di:

- Howard Schmidt, Presidente di ISSA International, nonché "Former White House Cyber Security Advisor" del presidente americano Bush nel 2002-2003.

- Antonio Amendola, Senior Adviser to the Secretary General of AGCOM, the Italian Communications Authority.

L'agenda della conferenza è disponibile su
www.aipsi.org/eventi/download/agenda_issa_rome_2007.pdf

La partecipazione è libera previa registrazione su
www.aipsi.org/eventi/evento_0bcf4d2e3d4cc27a44e6138916063b5bc5ace414/form

Segnaliamo la traduzione in italiano della newsletter Cobit Focus n. 3 - Aprile 2007: www.isacaroma.it/pdf/news/CobitFocus-v1-2007.pdf

La Fondazione Ugo Bordoni e l'OCSI stanno organizzando l''ottava edizione della ***International Common Criteria Conference*** (ICCC) che si terrà dal 25 al 27 settembre a Roma. La conferenza ha l'obiettivo di riunire organismi di certificazione, laboratori di valutazione, esperti e responsabili della sicurezza IT, utilizzatori di sistemi IT critici e sviluppatori di prodotti commerciali che hanno interesse nella progettazione, nell'implementazione, nella valutazione e certificazione della sicurezza IT.

Per ulteriori informazioni sulla conferenza, incluse quelle relative ad una eventuale partecipazione in qualità di Sponsor o di Speaker in una delle sessioni, si invita a consultare il sito www.8iccc.com.

Segnaliamo ***Azienda aperta, mobile e collaborativa: come garantire la sicurezza?***, un evento patrocinato dal Clusit che avrà luogo a Milano il prossimo 17 aprile.

L'incontro, destinato agli utenti e la cui partecipazione è gratuita, fa parte del ciclo di riunioni "Incontri a cena con gli utenti" che ZeroUno periodicamente organizza per analizzare, insieme a imprese, fornitori e osservatori di mercato, le tendenze evolutive dell'Information Technology applicate al business di impresa.

Per maggiori informazioni:
www.zerounoweb.it/index.php?option=com_tipologia&id=1673&id_tipologia=20&task=visualizza

8. EVENTI SICUREZZA

9 maggio 2007, Firenze - Seminario CLUSIT

L'utilizzo delle strumentazioni informatiche e telematiche aziendali. Poteri di controllo e repressione degli abusi da parte del datore di lavoro

https://edu.clusit.it/scheda_seminario.php?id=7

La partecipazione e' gratutita per il soci Clusit, che possono registrarsi online su https://edu.clusit.it

Istruzioni per la registrazione su www.clusit.it/registrazioni2007.htm

15-17 maggio 2007, Milano - ***6th OWASP AppSec Conference***

www.owasp.org/index.php/6th_OWASP_AppSec_Conference_-_Italy_2007

18 maggio 2007, Cernobbio (CO) - ***Realizzare un Data Centre sicuro, performante, scalabile e di facile gestione, i trend tecnologici e i requisiti da considerare per realizzare e disporre di una struttura Ced integrata e pronta alle nuove esigenze del sistema informativo aziendale***

21-23 maggio 2007, Roma - ***Corso OCSI sulla Certificazione della sicurezza informatica: guida per l'applicazione dei Common Criteria***
www.ocsi.gov.it/LinkClick.aspx?link=195&mid=195

23-25 maggio 2007, Parigi - ***EUROSEC 2007*** - 18ème Forum européen sur la sécurité del systèmes d'information
www.devoteam.fr/eurosec/2007/home.php?lang=fr

5-6 giugno 2007, Roma - ***INFOSECURITY Roma***
www.infosecurity.it/IT/roadshow/programma.aspx

6 giugno 2007, Roma - Seminario CLUSIT
Il Social Engineering e la sua applicazione nel penetration testing professionale
https://edu.clusit.it/scheda_seminario.php?id=8

14 giugno 2007, Milano - Seminario CLUSIT
Computer forensic: aggiornamenti
https://edu.clusit.it/scheda_seminario.php?id=9

20 giugno 2007, Roma - Seminario CLUSIT
Computer forensic: aggiornamenti
https://edu.clusit.it/scheda_seminario.php?id=10

26 giugno 2007, Segrate (MI) - ***La Security nei sistemi di controllo ed automazione, nelle reti ed infrastrutture***
www.anipla.it/FILE_ANIPLA/FILE_MENU/File_Archivio/PROG/2007/gds_26-06-07.pdf

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