Indice

1. NUOVI SOCI

Hanno aderito al CLUSIT le seguenti organizzazioni:

- Adfor (Milano),
- CNA - Associazione Provinciale di Milano (Milano),
- Eclittica (Bergamo),
- Hummingbird (La Chaux de Fonds - CH).
- Ikon Korp (Garbagnate Milanese - MI),
- Lonewolf Engineering (Torino),
- Ministero della Difesa, Direzione Generale Armamenti Terrestri (Roma),
- Oxytel (Guidonia Montecelio - RM)

2. LA METHODE MEHARI

I colleghi del Clusif stanno divulgando l'ultima versione de "la méthode Mehari", per l'analisi e la gestione del rischio. Non si tratta di uno standard alternativo ad altri, ma di uno strumento che può essere utile/interessante per i professionisti del settore. Stiamo preparando la versione italiana della presentazione generale della méthode Mehari e a breve la pubblicheremo sul nostro sito web, tra i whitepapers.

È già possibile consultare le versioni francese e inglese di tutta la documentazione relativa a Mehari V3 all'indirizzo:
www.clusif.asso.fr/fr/production/ouvrages/type.asp?id=METHODES

3. ROSI BENCHMARKING SURVEY

L'FGSec, associazione svizzera dei professionisti della sicurezza informatica www.fgsec.ch, tramite il Clusis, ci chiede di contribuire alla

realizzazione di una loro inchiesta sul Ritorno dell'Investimento in Sicurezza. Si tratta di uno strumento che vuole aiutare a fornire una giustificazione finanziaria per le misure di sicurezza. Si vuole introdurre il termine "rischio" (o piuttosto riduzione del rischio) al calcolo del ROI (o ROC, NPV etc.) normalmente utilizzato nelle organizzazioni per giustificare gli investimenti o le spese.

Questa inchiesta vuole analizzare l'utilizzo del ROSI, rapportato alla gestione tradizionale del rischio. Sono importanti non solo le risposte di chi si occupa dell'analisi del rischio, ma anche di chi decide sugli investimenti in sicurezza informatica nelle varie organizzazioni.

Ringraziamo fin d'ora coloro che vorranno partecipare all'iniziativa. La vostra partecipazione aumenterà il valore dell'inchiesta ed i risultati potranno essere estremamente utili per tutti.

Il questionario (in inglese) è disposibile all'indirizzo:
www.fgsec.ch/misc/rosi/survey_introduction.html

La compilazione richiede circa 20 minuti e saranno presi in considerazione i questionari pervenuti prima del 1 luglio 2006.

I risultati saranno presentati nell'ambito di una conferenza tenuta dal FGSec e la presentazione sarà pubblicata all'indirizzo: www.fgsec.ch/misc/rosi/results.html a fine settembre.

La raccola dei dati è assolutamente anonima: non è richiesto né il nome di chi compila il questionario né quello dell'organizzazione e FGSec garantisce l'anonimato.

4. CYBERCRIME

PHISHING E PHARMING: QUAL'È LA SITUAZIONE?

Era già stata segnalata in precedenza una certa preoccupazione per la crescita nelle varianti di alcuni virus (ad esempio: Beagle.32) e, allo stesso tempo, la paura per una possibile "rilassatezza" nei controlli, a causa del basso numero di attacchi di elevata gravità.

Ultimamente, si segnala anche che, nell'ambiente finanziario e non solo, si rileva una certa convinzione che il "Phishing" sia finito e sia oramai in netta diminuzione. Ciò anche se alcune fonti importanti avvertono sul rischio del "pharming" (variante questa del phishing); ricordiamo che con la parola "pharming" si intende la possibilità di essere dirottati su un altro sito a causa di un intervento criminale di alterazione della cache di un server DNS, ossia, in poche parole, mediante la modifica dell'indirizzo giusto del sito al quale si vuole accedere, ad esempio: la propria banca.

Tecnica questa da noi ipotizzata diversi mesi fa, ma che ancora non appare aver avuto successo, data le non poche difficoltà per attuarla.

Non solo non dobbiamo pensare che attacchi quali il phishing (ci sono sempre "pesci da prendere all'amo") siano in diminuzione, ma si devono migliorare ed intensificare le attività di prevenzione, quali la "awareness" ed il monitoraggio.

Si segnala, a titolo di esempio, quanto emerso nei soli ultimi tre mesi.

1. L'individuazione di gruppi criminali che offrono i loro servigi a basso costo e consistenti nell'iniettare un virus, appositamente studiato per il cliente, ad ignari computer (si parla di 25US$ ogni 10.000 computer

infettati: cifre irrisorie, se se ne infettano pochi.I gruppi pensano di colpirne a milioni!). Il virus, in genere un trojan, cattura i file ed utili informazioni dal computer e le trasmette all'esterno.

2. L'incremento negli attacchi denunciati. Infatti, le denunce di nuove email di phishing sono cresciute quasi del 20% negli ultimi tre mesi, rispetto allo stesso periodo dell'anno precedente. Ad aprile vi è stato un altro attacco ad alcune note aziende anche in Italia. Le email di spamming sono cresciute sino ad arrivare a quasi 6 milioni al giorno, e tale dato è in crescita.
3. Un incremento nelle prove di attacchi triplici mediante la generazione di tre virus "trojan"(un programma "scaricatore" inietta un programma ed una DLL che si inserisce nei processi di Explorer.exe, crea chiavi di start-up e status key nel registry di Windows) in grado di disabilitare l'antivirus, aprire una porta del computer ed inviare all'esterno informazioni sul computer e file di documenti contenuti sull'hard disk.
4. Il mese scorso vi sono stati ben 17 "trojans" (alcuni dei quali varianti di Riler, Nethief e Dloader) indirizzati ad agenzie ed enti governativi inglesi. Un attacco quindi mirato (ricordiamo la nostra newsletter di dicembre). I trojan sfruttavano i buchi di DCOM e RPC.

Tutto ciò non può non far riflettere e deve indurre ad intensificare i sistemi vuoi di prevenzione vuoi di gestione dell'emergenza.

Gli interventi devono avvenire nella sensibilizzazione della clientela sia interna sia esterna all'Azienda (far adottare un atteggiamento di giusta cautela quando si è avvicinati da persone sconosciute per mezzo di contatto fisico, telefonico o per email), e nell'adozione di strumenti software anche ridondanti (ad esempio, alcune aziende non si sono accontentate di installare un solo antivirus, ma di averne diversi, in modo da creare barriere progressive e specializzate).

Ricordiamo che ICAA è in grado di offrire assistenza alle aziende nella rilevazione del grado di percezione del rischio da parte del proprio personale dipendente.

(Fonte: ANSSAIF - Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria www.anssaif.it)

5. NOTIZIE DALL'ENISA

Sono disponibili due ulteriori posizioni lavorative all'interno di ENISA (vedi www.enisa.eu.int/recruitment/contract_agents/index_en.htm)

- IT Assistant (M/F) closing date: 05/05/2006
- Financial Assistant (M/F) closing date: 05/05/2006

Vi ricordiamo che chiunque fosse interessato a ricevere l'ENISA Quarterly (la newsletter trimestrale dell'ENISA) può inviare una email all'indirizzo press@enisa.eu.int, scrivendo nel Subject dell'email la parola "Subscribe".

Per chi volesse contribuire alla prossima versione dell' ENISA Quarterly, teniamo a disposizione le "Guidelines for Authors".

Le deadlines sono:

- Last Day for Submitting a 300 Word Proposal for Submission: May 15th
- Selection of Proposals and Notification to Authors: May 20th.
- Last Day for Submitting First Draft: June 5th.
- Feedback from First Draft Sent to Authors: June 13th.
- Deadline for Final Draft: June 17th
- Publication Date: June 30th

(Fonte: Daniele Perucchini, ENISA Liaison Officer)

6. SEMINARIO CLUSIT A INFOSECURITY VERONA

Stanno per chiudersi le iscrizioni al seminario Clusit

PROGRAMMAZIONE SICURA
VERONA 9 maggio 2006

Il seminario si svolgerà nell'ambito del primo evento locale di Infosecurity Italia www.infosecurity.it/Verona/index.php

Luogo: Centro Congressi Verona, Viale del Lavoro 8
www.infosecurity.it/Verona/location.php

Agenda:
- 10,15 Registrazione
- 10,30 Inizio Seminario
- 17,00 Fine lavori

Docente:
Mattia Monga (http://homes.dico.unimi.it/~monga)

SOMMARIO
Le applicazioni vanno progettate e realizzate tenendo ben presente i rischi ai quali il loro uso espone. E` necessario evitare quanto più possibile l'introduzione di vulnerabilità che possano essere sfruttate da un attaccante per acquisire il controllo del sistema. Inoltre, poiche` i sistemi fanno spesso uso di componenti non del tutto fidati, occorre tutelarsi in maniera tale da ridurre i danni che eventuali vulnerabilità sconosciute potrebbero provocare. Il corso di una giornata fornirà una panoramica delle vulnerabilità più comuni (specialmente nella programmazione C) e delle possibili contromisure.

REQUISITI
È necessaria la conoscenza del linguaggio C

PROGRAMMA

1. Introduzione metodologica

2. Problemi ricorrenti nella programmazione C
   - Buffer overrun
   - Heap overrun
   - Format bug
3. Contromisure e strumenti di analisi
4. Altri problemi nella programmazione delle applicazioni
   - Randomizzazioni
   - Concorrenza
   - Untrusted input e rappresentazioni canoniche
   - Socket
5. Conclusioni

- **Per registrarsi è sufficiente inviare una e-mail a info@clusit.it.**
- **Per i soci Clusit la partecipazione è gratuita**
- **La partecipazione riconosce 6 crediti/ore CPE**

7. NOTIZIE DAI SOCI

Il British Standard definisce nuove regole per garantire l'accesso ai siti internet da parte dei disabili

BSI ha predisposto un nuovo standard sulla "usabilità" dei siti internet per le persone disabili. Il documento avrà la sigla BS PAS 78 (ricordiamo che PAS significa "publicly available specification"). Il documento è nato dalla richiesta della commissione per la tutela dei diritti dei disabili che nel 2004 aveva rilevato che l'80% dei siti internet presentavano "barriere" all'accesso. La norma è una guida che permetterà di fornire siti user-friendly anche a soggetti con problemi, particolarmente adatta a chi si rivolge ai consumatori o svolge servizi di pubblica utilità. Secondo la suddetta commissione, i siti conformi allo standard BSI miglioreranno anche le loro relazioni commerciali con i disabili, i quali avranno ora accesso a servizi prima non disponibili, per esempio per effettuare prenotazioni o pagamenti direttamente on-line. Lo standard potrà essere utilizzato anche per la progettazione di siti per i quali il committente o la legge richiedano requisiti generici di usabilità; potra' essere anche una guida utile al rispetto delle disposizioni legislative italiane (Legge Stanca sull'accessibilità - Legge n. 4 del 9 gennaio 2004). La norma è applicabile a tutte le organizzazioni pubbliche e private, prevede il recepimento dei requisiti e delle guide W3C e definisce le buone pratiche di settore. È particolarmente adatta come requisito in sede di offerta o di appalto di un servizio di realizzazione e manutenzione di un sito internet.

(Fonte: BSi Management Systems Italia)

AIPSI – Associazione Italiana Professionisti Sicurezza Informatica, ha organizzato un evento in forma di "talk show" dal titolo **La sicurezza ICT... e le persone**, che si terrà a Milano il prossimo 8 Maggio, alle ore 18:00, presso Mondadori Multicenter in Via Marghera n° 28.

Nel corso dell'incontro si tratterà in particolare del ruolo delle persone e delle figure professionali dell'ICT Security. Si cercherà, con l'aiuto di alcuni

responsabili della formazione e della selezione del personale, di comprendere l'importanza di definire i profili degli operatori e l'utilità dei processi di certificazione del personale. Al "talk show", che sarà moderato dal giornalista Marco Gatti, Direttore di Week.it, parteciperanno il Prof. Francesco Tisato dell'Università Milano Bicocca, Giorgio Marietti, Direttore del Personale di Etnoteam, Maurizio Bedarida, Corporate ICT Security Manager di SIA e Maurizio Mapelli, Segretario Generale AIPSI.

I soci Clusit sono invitati, ma è necessario registrarsi, seguendo le istruzioni presenti sul sito www.aipsi.org.

9. EVENTI SICUREZZA

4 maggio, Milano
Seminario CLUSIT "Crittografia Moderna: Teoria e Pratica"
www.clusit.it/edu/index.htm#CR02

9-10 maggio, Verona
Infosecurity Italia 2006
www.infosecurity.it/Verona/index.php

9 maggio, Verona (nell'ambito di Infosecurity)
Seminario CLUSIT "Programmazione sicura"
www.clusit.it/edu/index.htm#PR01

12 maggio, Firenze
Convegno in tema di sicurezza informatica nell'ambito della manifestazione "VIVERE SICURI" (12-14 maggio)
www.viveresicuri.it/infor.htm

25 maggio, Roma
Seminario CLUSIT "Crittografia Moderna: Teoria e Pratica"
www.clusit.it/edu/index.htm#CR02

5-9 giugno, Milano
Seminario CISSP
www.clusit.it/isc2

14-16 giugno, Barcellona
CISO Executive Summit & Roundrable
www.clusit.it/eventi/060614_ciso.pdf

20-21 giugno, Roma
Infosecurity Italia 2006
www.infosecurity.it/Roma/index.php

21 giugno, Roma (nell'ambito di Infosecurity)
Seminario CLUSIT "Web Application Security: linee guida per la progettazione e l'audit"
www.clusit.it/edu/index.htm#WG01

22 giugno, Milano
Seminario CLUSIT "Aspetti legali della sicurezza informatica: lo stato dell'arte"
www.clusit.it/edu/index.htm#CF02

23 giugno, S. Felice Segrate (MI)
"La security nei sistemi di controllo ed automazione, nelle reti ed infrastrutture"
www.clusit.it/eventi/060623_anipla.pdf

6 luglio, Roma
Seminario CLUSIT "Aspetti legali della sicurezza informatica: lo stato dell'arte"
www.clusit.it/edu/index.htm#CF02

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