Indice

1. NUOVI SOCI

Nel corso del mese di maggio hanno aderito al CLUSIT le seguenti organizzazioni:

Recentemente hanno aderito al CLUSIT le seguenti organizzazioni:

- BSi Management Systems Italia (Milano)
- Kroll Ontrack (Lomazzo)
- Didagroup (Roma)ANTS (Milano)

2. ASSEMBLEA CLUSIT

L'assemblea CLUSIT del 26 maggio è stata particolarmente vivace e ricca di novità.

Ecco le iniziative e le attività che l'associazione ha deciso di portare avanti nei prossimi mesi:

1. Il coinvolgimento delle associazioni degli utenti nelle attività convegnistiche e di formazione.
2. Il consolidamento dei rapporti con ENISA e la partecipazione diretta ai suoi gruppi di lavoro.
3. Una più capillare collaborazione con le Istituzioni.
4. La realizzazione di un'indagine di mercato tra i soci "fornitori" (l'80% dei fornitori di prodotti, servizi e soluzioni di sicurezza informatica aderiscono al CLUSIT) in collaborazione con IDC.
5. L'aumento della visibilità del CLUSIT, particolarmente sulla stampa cartacea (giornali e riviste) e su radio e televisione.
6. La pubblicazione regolare di articoli tecnico-scientifici sulle testate cartacee e on line del gruppo editoriale IDG.
7. La creazione di un portale che serva da punto di incontro tra gli studenti universitari che sono interessati a svolgere tesi sulla sicurezza informatica e aziende, università e centri di ricerca, che suggeriscano gli argomenti di interesse e le tendenze.
8. L'istituzione di un premio CLUSIT, che premierà ogni anno la migliore tesi universitaria in sicurezza informatica.
9. La pubblicazione di 3 nuovi Quaderni CLUSIT.
10. Lo svolgimento del secondo ciclo di Seminari CLUSIT Education.
11. La partecipazione diretta dell'associazione a progetti europei.
12. La messa a disposizione di informazioni e supporto ai soci, per la partecipazione a progetti finanziati dall'Unione Europea.
13. Il rinnovo della partnership con (ISC)² per corsi e certificazioni CISSP.
14. La creazione di uno o più ISAC (Information Sharing and Analisys Center), col progetto ITAISAC.

15. La partecipazione ad una media di 1 convegno alla settimana, a partire da settembre, con una particolare attenzione per i convegni che potranno tenersi anche lontano dalle città di Milano e Roma (isole comprese).
16. La partecipazione a SMAU 2005.
17. L'organizzazione della fase finale del primo campionato nazionale di Hacking, organizzato dal CERT.IT,
18. La partecipazione a Infosecurity 2006 (a Milano in febbraio e a Roma nel mese di giugno).Il CLUSIT e IDC hanno dato il via ad una ricerca, per capire in modo più approfondito le vere condizioni del mercato della sicurezza informatica in Italia.

3. COMPUTER CRIME

CYBERCRIME, UNA RICERCA DAL REGNO UNITO.

I danni della cybercriminalità costano alle aziende inglesi con oltre 1000 impiegati 2,45 miliardi di sterline. Questo è il dato rilevato da una recente ricerca commissionata dalla National High-Tech Crime Unit (NHTCU), struttura istituita dal governo inglese nel 2001 nell'ambito del più ampio programma nazionale di prevenzione e lotta alla criminalità informatica. Su duecento compagnie intervistate, l'89% ha affermato di aver subito attacchi informatici che per la maggior parte hanno riguardato accessi non autorizzati al sistema e furto di dati e informazioni riservate.

Di questi il 97% ha lamentato una perdita di 71 milioni di sterline per attacchi finalizzati alla diffusione di virus, mentre il 9% ha accusato la perdita di 68 milioni di sterline per frodi finanziarie telematiche.

Secondo la NHTCU la ricerca evidenzia anche un altro aspetto: quanto cioè le aziende siano preoccupate della criminalità informatica in termini strettamente finanziari, e quanto poco lo siano invece in termini di danno all'immagine e alla reputazione.

Di quest'ultima considerazione sono consapevoli infatti soltanto il 17% degli intervistati. I dati emersi dalla ricerca indicano inoltre che non sempre l'attività illecita ha un'origine esterna, spesso infatti sono gli stessi impiegati delle aziende gli autori dei reati lamentati.

La ricerca è disponibile all'indirizzo http://www.out-law.com/php/page.php?page_id=hitechcrimecostin1112877173&area=news

(Tratto dalla newsletter N.93 del Ministro per l'Innovazione e le Tecnologie)

Phishing.

Il Laboratorio sul Phishing ci segnala che anche in Italia negli ultimi mesi si sono avuti diversi attacchi di phishing. Questi sono avvenuti nei confronti di: due grandi gruppi bancari, una grande azienda emittitrice di carte di credito, e di una grande azienda nazionale, già Ente Autonomo dello Stato.

Su uno dei due grandi gruppi bancari la modalità non è consistita nella solita email ai clienti, dirottandoli su un sito fasullo e chiedendo di digitare user e password, ma invece è consistita in una richiesta all'help desk della banca dichiarando di essere un cliente dell'home banking e di avere lo user bloccato a seguito di un eccesso di tentativi di digitazione della password.

Malgrado questa recrudescenza da parte della criminalità organizzata, non si segnalano perdite economiche.

Virus.

Desta un certo interesse un articolo apparso recentemente su www.techweb.com nel quale si analizza il worm Bagle.

In estrema sintesi, detto worm ha presentato nel tempo oltre 100 varianti, predisposte a volte in pochissimi giorni, e redatte secondo una metodologia ferrea; infatti, il codice è stato realizzato facendo attenzione ai dettagli e seguendo il processo CMMI (Capability Maturity Model Integration), metodo della Carnegie Mellon's Software Engineering Institute per la valutazione della maturità nello sviluppo del software.

Il virus ha permesso di catturare password. E' stato molto probabilmente realizzato da un team di esperti. Secondo l'autore dell'articolo, quanto realizzato "fa scuola": "In many ways the Bagle history is a blueprint for Web-based criminal success".

Dobbiamo quindi ipotizzare che dietro di esso c'è un pericoloso gruppo criminale che potrebbe realizzare presto altre tipologie di attacco.

Una domanda: i criminali vogliono le password per rubare un po' di soldi? E se fossero terroristi?

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

É apparsa sul web una nuova tecnica di truffa, con tentativo di estorsione, che utilizza la cifratura associata ad un trojan horse.

Il truffatore ha sfruttato un baco di Internet Explorer, individuata e corretta da Microsoft nel luglio 2004. Ha messo a punto un trojan horse (Trojan.Pgpcoder), che ha nascosto in una pagina web. Quando la vittima si è collegata al sito in cui era stato inserito il trojan horse, ha scaricato a sua insaputa un programma maligno, che ha autonomamente scaricato da un'altro sito web e lanciato un'applicativo di cifratura. Ecco che un certo numero di file, principalmente immagini e file di Office, sono stati cifrati e gli originali sono stati distrutti. A questo punto è apparsa la richiesta di un riscatto di 200 dollari in cambio della chiave necessaria a decifrazione dei file. Si tratta per ora di casi isolati, ma il fenomeno è preoccupante. In questo caso, il truffatore ha lasciato delle tracce al momento della richiesta del riscatto; è stato identificato e il sito web è stato chiuso. Per fortuna il programma maligno non era particolarmente complesso ed il codice di cifratura è stato violato, riuscendo a recuperare i file.

4. 1° CAMPIONATO ITALIANO DI HACKING

L'hacking è sicuramente uno dei fenomeni piu controversi della rivoluzione ``Internet''. Nati nei primi anni '60 al MIT, come gruppo di esperti programmatori e conoscitori di computer, gli hacker sono indicati da molti come i pionieri della rivoluzione dell'informazione e come coloro che, con le loro conoscenze approfondite di computer e reti, hanno consentito lo sviluppo della rete Internet come oggi la conosciamo.

Per contro, oggi questo termine viene usato dalla maggioranza dei media per denotare criminali, che usano i computer per perpetrare i propri atti.

Nonostante ciò, nei laboratori di ricerca, nelle Università e in Rete, hanno continuato ad operare, e sono cresciuti, gruppi con elevate competenze relative a sistemi informatici e telematici, il cui modo di operare è del tutto assimilabile a quello degli hacker di prima generazione, che sono definiti, dagli addetti ai lavori e dalla stampa specializzata, true-hacker per distinguerli dai criminali tecnologici solitamente definiti cracker.

Ai true-hacker è dedicata questa iniziativa, mirata a stimolare e a misurare le loro capacità.

Nell'ambito di questa challenge ad ogni gruppo partecipante (di max 6 componenti) sarà fornita una macchina virtuale, i cui dettagli saranno resi noti solo all'inizio della prova. Ogni squadra dovrà dimostrare di saper difendere la propria macchina dagli attacchi degli altri gruppi, preoccupandosi allo stesso tempo di attaccare con successo quelle degli altri. Questo schema di gara è stato inizialmente introdotto al Defcon, con il Capture The Flag e, successivamente, ripreso e organizzato su scala internazionale dal Prof. Giovanni Vigna nell'ambito del primo Capture The Flag internazionale dell'University of California, Santa Barbara (Computer Science department).

Saranno fissati obiettivi da raggiungere e proteggere, e ogni obiettivo raggiunto porterà alla squadra dei punti. Al termine della competizione vincerà la squadra che avrà totalizzato più punti.

L'intera competizione sarà organizzata e gestita dal CERT-IT (Computer Emergency Response Team - Italian) del Dipartimento di Informatica e Comunicazione dell'Università degli Studi di Milano.

(Fonte: http://security.dsi.unimi.it/ctf/)

Maggiori informazioni sono disponibili all'indirizzo sopra riportato.

La manifestazione si terrà sabato 15 ottobre.

Il CLUSIT parteciperà all'organizzazione di una fase finale, tra le squadre che risulteranno le migliori della competizione, che si terrà il sabato successivo, 22 ottobre, nell'ambito di SMAU 2005.

5. SMAU 2005

É stato costituito il Comitato di Programma per i convegni che saranno organizzati a SMAU, sulla sicurezza informatica.

Ne fanno parte:

- DANILO BRUSCHI, Prof. Ordinario di Sicurezza dei calcolatori e delle Reti presso il Dipartimento di Informatica e Comunicazioni dell'Università degli Studi di Milano, Membro del Comitato Tecnico Nazionale sulla Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni, Presidente del Comitato Internet e Minori e Presidente onorario del CLUSIT.

- LUISA FRANCHINA, Direttore Generale dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCOM), Ministero delle Comunicazioni, rappresentante italiano nel Management Board di ENISA (European Network and Information Security Agency).

- PAOLO GIUDICE, Segretario Generale dell'Associazione Italiana per la Sicurezza Informatica (CLUSIT).

- CLAUDIO MANGANELLI, Membro del Collegio del Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA) e Presidente del Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle Pubbliche Amministrazioni.

- MARIO PELOSI, Capo del Dipartimento per l'Innovazione e le Tecnologie, Presidenza del Consiglio dei Ministri.

- ERMINIO SEVESO, Direttore Organizzazione Sistemi BTicino e Presidente dell'Associazione Utilizzatori Sistemi E tecnologie Dell'informazione (AUSED).

- DOMENICO VULPIANI, Direttore del Servizio Polizia Postale e delle Comunicazioni, Ministero dell'Interno.

- Un Dirigente dell'Associazione Bancaria Italiana (ABI).

Segnaliamo che Promotor International, già proprietaria di SMAU, ha recentemente acquisito anche il marchio Webbit.

6. BLACK HAT EUROPE 2005

Dal 29 marzo al 1 aprile, si e' tenuta ad Amsterdam la conferenza "Black Hat Europe 2005". "Black Hat", che si ripete tre volte all'anno negli Stati Uniti, in Europa e in Asia, e' riconosciuta come la piu' importante manifestazione nell'ambito della "scena" della security, mescolando competenze di altissimo livello dell'underground, gruppi di ricerca indipendenti e risultati di punta nell'R&D di societa' che operano nel settore.

Interessante e vario come sempre il pubblico (composto da utenti finali, consulenti di alto livello... e dagli speaker delle edizioni precedenti !), e ottima la qualita' delle presentazioni, accuratamente selezionate per escludere qualsiasi deriva commerciale. Le tematiche si sono articolate su quattro tracce (Zero Day Attack, Deep Knowledge, Zero Day Defense, Situation Awareness).

La conferenza ha alternato temi sociali (introdotti da Simon Davies, un noto difensore del diritto alla privacy) a temi altamente tecnici, decisamente di alto profilo. In particolare ho apprezzato la competenza di Joe Grand, che ha introdotto i problemi di sicurezza legati all'affidabilita' dell'hardware, e Johnny Long che ha dimostrato quanto sia facile reperire informazioni preziose semplicemente attraverso Google. Tuttavia, la palma della miglior presentazione a mio avviso andrebbe conferita ad Adam Laurie, Martin Herfurt e Marcel Holtmann di Trifinite, che hanno presentato tecniche di Bluetooth Hacking veramente divertenti ed inquietanti.

Tra i "soliti noti" che non hanno perso occasione di riconfermarsi come i migliori sulla scena, David Litchfield (che ha presentato tecniche inferenziali per la SQL Injection cieca), Dan Kaminsky (che con piglio da showman ha dimostrato tutte le vulnerabilita' dell'architettura DNS), e the Grugq (che ha presentato tecniche di forensics e anti-forensics).

E' stato un piacere poter rappresentare anche quest'anno l'Italia in questo consesso, presentando i risultati delle nostre ricerche nel campo della sicurezza delle web application, proponendo un tool per l'identificazione di vulnerabilita' nel codice sorgente.

Tutte le presentazioni sono come sempre disponibili sul sito www.blackhat.com

(Autore: Stefano Zanero, socio CLUSIT)

7. NOTIZIE DAI SOCI

Stefano Quintarelli, socio fondatore del CLUSIT, è stato nominato Presidente dell'Associazione Italiana Internet Providers (Aiip).

I.F.O.A. ci segnala la disponibilità di alcuni stagisti, in prevalenza ingegneri in TLC, che stanno partecipando ad un Master specialistico in telecomunicazioni.

Il tirocinio aziendale si svolgerà orientativamente a partire dal mese di luglio o settembre a seconda delle esigenze aziendali ed avrà una durata di 480 ore. Di cui 100 ore saranno dedicate a un Project Work. Per qualunque informazione, potete rivolgervi alla Sig.ra Alda Manini (manini@ifoa.it, Tel. 0522-329341 fax 0522-791692).

8. EVENTI SICUREZZA (Tutti i dettagli sulle manifestazioni sono disponibili sul sito CLUSIT alla voce EVENTI)

6-10 giugno 2005, Roma
Corso di certificazione OPST

9 giugno 2005, Settimo Milanese
I.NET Security Day 2005

11 giugno 2005, Milano
Esame CISSP

13-17 giugno 2005, Roma
Seminario di preparazione all'esame CISSP

16-17 giugno 2005. Ginevra
MIS Traning's CISO Executive Summit

16 giugno 2005, Roma
Sicurezza in Banca
La continuità operativa: problematiche organizzative ed informative

17 giugno 2005, Roma
Mattino: Il Management delle informazioni in Azienda: Sicurezza e Privacy
Pomeriggio: Sicurezza Informatica e tutela dei dati personali in ambito sanitario: esperienze a confronto

20 giugno 2005, Rimini
1° Forum Internazionale sui Sistemi di Gestione per la Sicurezza delle Informazioni

20-21 giugno 2005, Milano
Firma digitale, e-mail certificata, carta nazionale dei servizi

5 luglio 2005, Milano
Seminario CLUSIT "Controllo dei lavoratori"

13-14 luglio 2005, Milano
Bank Security Days

16 luglio 2005, Roma
Esame CISSP

19 luglio 2004, Roma
Seminario CLUSIT "Controllo dei lavoratori

27-28 luglio 2005, Las Vegas
BlackHat USA 2005

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