

Indice

1. NUOVI SOCI
2. ALLARME PHISHING IN ITALIANO
3. COMPUTER CRIME
4. DATI FEDERCOMIN SULLA SOCIETÀ DELL'INFORMAZIONE
5. INFOSECURITY ITALIA 2006
6. MASTER UNIVERSITARIO UNIMI-CEFRIEL
7. NOTIZIE DAI SOCI
8. SEMINARI CLUSIT DI SETTEMBRE
9. EVENTI SICUREZZA

1. NUOVI SOCI

Recentemente hanno aderito al CLUSIT le seguenti organizzazioni:

- Banca Intesa (Milano)
- Exposervice (Prato)
- Clanius Consulting (Casapulla - Caserta)
- Data Management (Agrate Brianza - MI)
- TÜV Italia (Sesto San Giovanni - MI).

2. ALLARME PHISHING IN ITALIANO

Il fenomeno del Phishing comincia a coinvolgere sempre di più gli utenti italiani. Le email fraudolente, che si rivolgono ai clienti di diversi Istituti Bancari italiani, sono ormai redatte in un buon italiano e non mancano di fantasia nelle argomentazioni utilizzate per invogliare i destinatari a cadere nella trappola. Come abbiamo già scritto più volte, la principale contromisura che le banche possono adottare è l'informazione e l'educazione dell'utente.

Il CLUSIT mette a disposizione 2 documenti generici, uno alquanto sintetico (www.clusit.it/whitepapers/phishing_gg.pdf) ed un secondo più completo (www.clusit.it/whitepapers/phishing_em.pdf). Tali documenti possono essere pubblicati e divulgati a terzi, con il solo obbligo di citarne le fonte.

3. COMPUTER CRIME

Cosa bolle in pentola?

I nostri esperti stanno seguendo con attenzione e preoccupazione l'evoluzione dei virus (worm e trojan), sia nella tipologia che nell'andamento degli attacchi.

Ci riferiamo, ad esempio, ai "virus dormienti", alle centinaia di varianti di una stessa tipologia, ad un trend di diffusione in crescita, ecc.

La paura degli esperti è che si stia preparando un attacco in "grande stile", finalizzato o a mettere in crisi il sistema finanziario occidentale, oppure a rendere ancora più gravi le conseguenze di un attacco terroristico perpetrato con esplosivi o sostanze bio-chimiche; possiamo citare, ad esempio, azioni tese a rendere assai difficoltosi gli interventi di soccorso e di ripristino, quali: eccesso di traffico sulle reti telematiche, blocco dei cellulari

per un lungo periodo, oscuramento dei server dedicati al controllo aereo o alla Protezione Civile, ecc..

Pensiamo al sistema di regolamento fra banche: un attacco terroristico disastroso, ad alto impatto anche emotivo, seguito dal blocco delle comunicazioni e dei sistemi informativi degli intermediari finanziari, se prolungato nel tempo, data la gravità, può avere un effetto drammatico se non ci si è preparati in anticipo.

L'enfasi deve essere sempre orientata al rafforzamento delle difese ed alla predisposizione di opportune misure preventive; pertanto, anche in questo caso, in un'ottica di approccio che tende sempre ad essere pro-attivo, riassumiamo quelle che potrebbero essere delle azioni da intraprendere, sia in un'ottica a brevissimo termine, sia nel lungo periodo; comunque, la tipologia di evento sopra descritta va, a nostro parere, analizzata e simulata a tavolino quanto prima (tra l'altro, rientra pienamente negli scenari descritti da Banca d'Italia nelle sue linee guida del luglio 2004).

Alcune contromisure, da noi riportate qui di seguito, appariranno "vecchie", ma abbiamo ritenuto opportuno ripeterle, in quanto non ci risulta che siano molti gli intermediari che le abbiano introdotte.

L'ANALISI DEI FATTI

Proviamo innanzitutto a sintetizzare le motivazioni alla base di questa crescente preoccupazione.

Iniziamo con il riflettere su alcuni fatti.

- In passato abbiamo assistito a feroci attacchi di alcuni virus (Red code; nimda; gaobot; ecc. per citarne alcuni) che hanno colpito praticamente tutte le aziende a livello mondiale;
- c'è stato poi un calo sia in frequenza di attacchi sia nella severità (19 alert nel 2002; 16 nel 2003); ciò malgrado non fossero migliorate di molto le difese (cfr. indagini: CSI/FBI, Australian High Tech Crime Centre; ecc.);
- anche gli attacchi terroristici erano diminuiti in gravità e frequenza;
- si è poi avuto un incremento nel 2004 e negli ultimi 18 mesi si sono avuti molti più allarmi virus - a parità di gravità - che nei due anni precedenti sommati;
- ma ciò che preoccupa di più, è che si sta assistendo ad un incremento nelle varianti di alcuni worm (ad esempio: ci sono oltre 300 varianti di NETSKY e BAGLE, worms di tipo memory resident; un centinaio di varianti di MYTOB; ecc.), quasi ad indicare un tentativo di sperimentare tutte le possibilità sia su come ingannare l'utente sia sulle finalità (NETSKY e BAGLE, ad esempio, hanno avuto mutamenti nell'oggetto, nel messaggio, negli allegati, ecc.);
- ci sono worm che ingannano il ricevente un messaggio affinché apra un messaggio o si rechi su un certo sito, ed altri che invece sfruttano i "buchi" del sistema operativo del computer;
- riemergono vecchi virus (ad esempio: SOBER, GAOBOT, ecc.) con nuove varianti;
- ci sono virus in "appoggio" all'azione di altri (ad esempio: WURMARK e BOBAX);
- ci sono trojans che cercano file di EXCEL, WINWORD o HTML e li spediscono all'esterno;
- ci sono trojan che incryptano questi file e li lasciano sull'hard disk dove li hanno letti (ad esempio, a fini di ricatto);
- ci sono dei worm che hanno avuto l'unico scopo di entrare nei computer per cancellare precedenti versioni, forse in previsione di una nuova versione che sarebbe probabilmente andata in conflitto (se no, perché?);
- ci sono virus il cui unico scopo è quello di ottenere informazioni sul possessore: nome, cognome, indirizzo, uso del computer, password, abbonamenti, gusti, ecc.; molti a fini commerciali, tanti ai fini di furto d'identità;
- sappiamo, altresì, che non possiamo escludere, per esperienza, che i virus siano utilizzati o creati anche da terroristi;
- e così via: potremmo proseguire ancora, ma riteniamo sufficienti le informazioni elencate, per i nostri fini.

Possono sorgere, alla luce di quanto sopra, domande quali:

- le molteplici varianti di uno stesso worm o trojan sono state create esclusivamente per migliorare l'attacco, oppure nascondono un preparativo per "qualcosa" di grosso, di serio?
- I migliaia di trojan che hanno infettato milioni e milioni di computer (oltre 12 milioni l'anno scorso) cosa hanno raccolto? Quali notizie? (da notare che i Paesi più colpiti sono stati quelli dell'Europa Occidentale e gli USA)

- Le informazioni ottenute dagli hacker a cosa sono servite? Molte informazioni sono state chiaramente utilizzate per ricatto, ripicca, furto, ecc. Sono state utilizzate tutte?
- Ci sono delle informazioni "congelate" da qualche parte? Se sì, per farci cosa?
- Possiamo escludere che degli hacker abbiano raccolto le password degli amministratori dei server e possano quindi prenderne il possesso in qualsiasi momento?

Aggiungiamo qualche altra informazione più recente.

Da qualche tempo a questa parte è aumentato il numero dei sistemi operativi i cui "buchi" possono essere sfruttati da nuovi virus: parliamo di sistemi SAP, CISCO, piuttosto che EPOC o SYMBIAN (telefoni cellulari). I mainframe sono fino ad oggi rimasti immuni: perché? Non hanno il TCP/IP a bordo? (o lo sono già stati e non ce ne siamo accorti?).

In aggiunta, nei computer si trovano dei virus la cui "firma" o tipologia è sconosciuta: trattasi di virus "dormienti"? In attesa di cosa?

A questo punto possiamo trarre queste conclusioni:

- vi è una crescente sperimentazione di nuovi worm e trojan;
- si riscontrano virus dormienti;
- le informazioni nel frattempo raccolte dai vari trojans forse non sono state totalmente sfruttate;
- vi è un incremento notevole nel numero e tipologia di sistemi che possono essere violati;
- le contromisure adottate dalle aziende rispettano senz'altro i requisiti "minimi" richiesti, ma nella maggior parte dei casi non sono ancora aggiornate in base alla recrudescenza del crimine.

Possiamo allora, alla luce di quanto sopra, escludere che qualcuno, chissà dove, stia preparando un attacco, non solo sui computer di casa, ma contemporaneamente sulle reti di computer, cliente e server, firewall e routers di un'azienda?

Perché? Ci possono essere tanti perché. Perché l'azienda è un intermediario finanziario, oppure perché collabora con una Nazione presa di mira, oppure perché è inglese, o spagnola, o italiana.

Chiaramente non abbiamo la risposta. Ma qualcosa dobbiamo fare.

Nessuno di noi si può scordare la giornata in cui Red Code ha colpito le aziende in tutto il mondo. Forse oggi siamo tutti più pronti, ma per un attacco "tradizionale". Se i programmi virali giacciono nelle nostre reti, già la situazione è diversa.

Se l'attacco è contemporaneo su tutti i computer dell'azienda, abbiamo una situazione ancora più grave.

LE POSSIBILI SOLUZIONI

Cosa fare?

Elenchiamo qui di seguito quello che l'esperienza suggerisce.

Approccio orientato prevalentemente alla prevenzione e graduato nel tempo, in modo da essere ragionevolmente certi di ottenere risultati concreti:

- nel brevissimo termine (contromisure tecniche e procedure per la gestione della continuità in caso di emergenza);
- nel medio (ad es: incremento nella quantità e qualità dei controlli; modifiche organizzative);
- nel lungo (ad es: creazione in azienda di una cultura della sicurezza in termini di qualità del servizio e prevenzione da incidenti).

Operare gli interventi nel breve-medio suddividendo l'approccio in due aree distinte:

- le infrastrutture,
- gli utilizzatori.

Dedicare due team distinti (a pensare, progettare, realizzare i controlli e l'"hardening"; ecc.) per le due aree indicate; in particolare, non trascurare affatto la possibilità di affidare in toto l'hardening delle infrastrutture a terze parti specializzate, concentrando il personale interno sugli aspetti ove è maggiormente richiesta la conoscenza dei processi aziendali, maggiore riservatezza, ecc.

Eseguire attività quali:

- Individuare Virus "non firmati", non riconosciuti fra quelli noti (possono nascondere sw ad hoc per catturare informazioni);
- Non limitare la sorveglianza sui sistemi di sicurezza perimetrale ed interna al solo orario d'ufficio;
- Individuare attività anomale di eccesso di traffico su una lan;

- Indurre gli amministratori dei server a cambiare la password, almeno una volta al mese, controllando non sia la stessa ripetuta ogni due mesi!;
- O meglio ancora, dotare gli amministratori di sicurezza di "one time password", nonchè valutare con attenzione la possibilità di introdurre sistemi biometrici di controllo accessi;
- Non rimandare dei controlli, su eventi anomali, al giorno dopo;
- Controllare minuziosamente l'elenco delle macchine in rete, senza escludere nessuna lan (ad esempio: quelle degli "architetti" o di test);
- Cercare di evitare di avere database con dati riservati o peggio sensibili direttamente collegati ad internet;
- Individuare Attività anomale del pc, ad esempio, segnalando accessi fuori orario;
- Sviluppo software: disegno include la sicurezza;
- Cultura di sicurezza agli sviluppatori di software;
- Disseminare, in generale, una cultura della sicurezza in azienda, verificandola periodicamente;
- Inserire i controlli sulla compliance alle esigenze di sicurezza e business continuity nei processi di disegno e realizzazione di nuovi sistemi;
- Sensibilizzare gli utenti - interni ed esterni - alle tematiche di protezione dei dati, continuità del business, qualità del servizio;
- Eseguire almeno annualmente una analisi del rischio ICT (in modo "serio", non in via simbolica., come avviene in molte aziende);
- Integrare le esperienze, conoscenze, attività, dei colleghi impegnati nell' ORM (Operational Risk Management), sicurezza fisica ed ICT, Business Continuity, auditing, usando come "collante" l'Organizzazione e le Risorse Umane, in modo da facilitare sia la comprensione dei fatti individuati sia la individuazione delle possibili soluzioni;
- Ipotizzare l'assenza dei sistemi informativi a sostegno dei processi di regolamento e compensazione e, pertanto, redigere, e sperimentare, gli opportuni piani di gestione dell'emergenza.

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

4. DATI FEDERCOMIN SULLA SOCIETÀ DELL'INFORMAZIONE

Il 29 giugno 2005 è stato diffuso il secondo numero dell'Osservatorio semestrale della Società dell'Informazione, voluto dal ministro per l'Innovazione e le Tecnologie, Lucio Stanca, e realizzato da Federcomin.

L'Osservatorio, che analizza semestralmente lo stato e le dinamiche di utilizzo di nuove tecnologie da parte delle imprese, dei cittadini e della Pubblica Amministrazione è uno strumento di monitoraggio della domanda e dell'utilizzo delle tecnologie. I dati elaborati, aggiornati generalmente a dicembre 2004, rappresentano il risultato di analisi condotte da diversi istituti di ricerche secondo i parametri del Piano eEurope 2005.

*** La spesa in innovazione: 5,5% del PIL ***

La spesa in ICT è stata pari, nel 2004, al 5,5% del PIL, e la parte preponderante riguarda la spesa in telecomunicazioni (3,6%). Il valore totale risulta in leggera crescita rispetto a quello dei tre anni precedenti (intorno al 5,3%), ma la percentuale di spesa in IT è rimasta sostanzialmente invariata negli ultimi anni.

*** I cittadini e l'innovazione tecnologica: 7,9 milioni utilizzano la banda larga ***

Secondo le rilevazioni di Nielsen//NetRatings è aumentato il numero di famiglie che possiede un PC in casa: il 58%, rispetto al 55% del primo semestre 2004. Nel 2004 hanno navigato ad alta velocità 7,9 milioni di italiani, il 47% di tutti gli utilizzatori (il numero di accessi in banda larga è pari invece a 4,7 milioni). Il navigatore in banda larga ha un profilo più maschile e maggiormente concentrato nelle fasce giovani di quello a banda stretta.

*** La sicurezza on-line: un problema per il 33% delle imprese ***

Per le imprese: il 33% di imprese ha riscontrato problemi di sicurezza informatica e la percentuale è sostanzialmente uniforme tra aziende di dimensioni differenti. Per i cittadini: l'esperienza di trovarsi di fronte a finestre aperte in maniera automatica con pubblicità di

altri siti è comune al 57,6% dei navigatori, mentre il 31,5% di loro ha dovuto fronteggiare contenuti indesiderati od offensivi.

*** e-Government: 10,4 milioni di cittadini visitano i siti della P.A. ***

L'81% dei comuni capoluogo di provincia (rispetto al 75% rilevato a giugno 2004) offre la possibilità di scaricare direttamente dal sito i moduli necessari per il pagamento delle tasse. La grande impresa mostra maggiore attitudine nella gestione di pratiche interamente on-line (61%). La percentuale scende al 39% per le PMI. I cittadini: nel quarto trimestre del 2004 10,4 milioni di navigatori hanno visitato uno dei siti della PA, circa 300 mila in più rispetto al secondo trimestre dell'anno, il 21% in più rispetto a dodici mesi prima.

*** Aumenta l'accesso delle imprese a Internet: 54% con banda larga ***

Il valore medio delle imprese che accedono ad Internet è passato dal 45,5% nel primo semestre 2004 al 46,8% nel secondo semestre, ma per quelle di più grandi dimensioni la percentuale è vicina al 100%. Per quanto riguarda le piattaforme IPbased che abilitano le aziende ad aprirsi verso l'esterno per dialogare con interlocutori interni (Intranet) o esterni (Extranet), o non conosciuti a priori (sito web), nel secondo semestre del 2004 si è rilevato un dinamismo significativo, con un tasso di crescita di circa cinque punti percentuali: la presenza sul web passa dal 26% al 31% (percentuale calcolata sul totale delle aziende), oppure dal 48% al 55% se si calcola la percentuale sulle aziende con accesso a Internet. La diffusione della banda larga nelle imprese ha raggiunto nel 2004 il 54% circa delle aziende che accedono a Internet, contro il 45% del primo semestre 2004.

*** Il Voip: 39.000 aziende lo utilizzano ***

Il lancio, da parte di diversi operatori di telecomunicazione, di offerte di VoIP (Voice over IP) destinate alla clientela business e consumer è stato uno degli eventi più significativi del mercato dei servizi su rete fissa nel 2004. Si stima che alla fine del 2004, circa 39.000 aziende abbiano utilizzato tali servizi

*** e-Learning ***

Le imprese: il 26% delle imprese con oltre 250 addetti utilizza applicazioni di e-Learning per la formazione del proprio personale, mentre quelle con minor numero di dipendenti si attestano mediamente tra il 4,8% e il 7,4%. I cittadini: si stima che a metà 2004 la maggior parte dei navigatori abbia utilizzato Internet per ricercare informazioni su argomenti di studio o di lavoro (con una sostanziale uguaglianza di valori tra uomini e donne), mentre ancora bassa è la percentuale che utilizza il web per seguire reali corsi di formazione.

*** e-Health: in aumento le prenotazioni on-line ***

La prenotazione on-line di una visita è ancora una pratica poco diffusa, ma in crescita rispetto all'ultima valutazione. A livello nazionale passa dal 4% all'8%. Sul totale di navigatori attivi maggiori di 14 anni, solo il 9,4% ha utilizzato il canale on-line per reperire informazioni di carattere sanitario o per prenotare una visita medica.

*** e-Business: il 6,1% delle imprese opera attraverso il commercio elettronico ***

Le imprese: il peso del commercio elettronico sul fatturato delle imprese ammonta al 6,1%. Ancora basso è il numero di imprese che si rivolgono a tecnologie di e-Procurement per acquistare prodotti o servizi: 6% con punte del 34% nelle aziende con più di 250 dipendenti. Più alto è il numero delle aziende che hanno ricevuto ordini mediante applicativi di e-Commerce, circa il 20%. I cittadini: L'utilizzo di Internet per finalità di e-Commerce è ancora ad uno stadio semiiniziale: a metà 2004 solo il 6,8% dei navigatori attivi utilizza il web con questa finalità.

*** I media televisivi: 6 milioni di cittadini accedono alla TV digitale ***

Sono circa 21,8 milioni le abitazioni dotate di apparecchio televisivo, pari al 96,4% del totale delle abitazioni. Le abitazioni dotate di televisione digitale (digitale terrestre, via satellite e via cavo) sono quasi 6 milioni. La televisione digitale terrestre: a fine 2004 erano presenti nelle famiglie italiane quasi un milione di decoder (16% su un totale tv digitale). La televisione digitale via satellite: alla fine del 2004, 4,8 milioni di abitazioni erano in grado di ricevere la televisione digitale direttamente da satellite, grazie all'installazione di una parabola. Queste rappresentano il 23% delle famiglie televisive e l'80% dell'universo digitale. La televisione digitale via cavo: a fine 2004 gli abbonati ai servizi video erano 241.500. Di questi, il 61% riceve la televisione tramite connessione ADSL, il 39% tramite fibra ottica. Il numero totale degli abbonati alla Pay-Tv in Italia è pari a 3.341.500, il 15,9% delle abitazioni TV.

*** La pubblicità on-line ***

I dati consuntivi rilasciati dall'Osservatorio IAB/ACP on-line relativi alla raccolta pubblicitaria attestano che in Italia, a dicembre 2004, il peso di Internet all'interno del media mix complessivo è circa del 1,4%. Tale valore è ancora limitato, ma va contestualizzato in un marcato trend di sviluppo, con un valore assoluto degli investimenti pari a 107 milioni di Euro e una variazione rispetto al 2003 pari al 24,7%.

*** Le previsioni per il 2005: crescono le TLC e i nuovi servizi ***

Per il 2005 si attende una crescita più importante sia per il settore delle TLC che per quello dell'IT. Sono molteplici le opportunità di business che si presentano per l'ICT e sono legate soprattutto alla crescente adozione di tecnologie innovative: i nuovi servizi legati alla televisione digitale terrestre, la banda larga, le tecnologie Wireless, il mercato dei contenuti digitali, l'atteso sviluppo delle tecnologie di infomobilità e RFID.

Al sito www.federcomin.it sono disponibili il Summary ed il testo integrale dell'Osservatorio.

(Tratto da FEDERCOMIN MAIL N.34)

5. INFOSECURITY ITALIA 2006

È stata rinnovata la partnership tra CLUSIT e Fiera Milano International, per l'organizzazione di Infosecurity 2006, che prevede per la prima volta, oltre alla manifestazione milanese (8-10 febbraio, Fiera Milano), una manifestazione a Verona (9-10 maggio, Centro Congressi Fiera Verona) ed una a Roma (21-22 giugno, Hotel Sheraton Roma).

Tra le novità per il 2006, oltre alle 2 nuove manifestazioni di Verona e Roma:

- la costituzione di un Comitato Scientifico allargato (15/18 membri), che vedrà un maggior coinvolgimento del mondo accademico e delle associazioni del settore;
- la costituzione di un Comitato Strategico, cui parteciperanno le aziende espositrici;
- l'organizzazione di una competizione, tecnologica e metodologica, cui potranno partecipare le aziende espositrici;
- la partecipazione di alcune figure estremamente significative, a livello mondiale, per il mondo dell'ICT security;
- la presentazione dei risultati della ricerca di mercato CLUSIT/IDC;
- la presentazione delle migliori tesi universitarie in sicurezza informatica e la consegna del relativo Premio CLUSIT;
- l'organizzazione di seminari tecnici di alto livello (a pagamento).

6. MASTER UNIVERSITARIO UNIMI-CEFRIE

Sono aperte le iscrizioni alla Quinta Edizione del Master Universitario di primo livello in Sicurezza delle informazioni e delle Reti, organizzato dal Dipartimento di Informatica e Comunicazione dell'Università degli Studi di Milano e CEFRIEL, con il patrocinio del CLUSIT.

Il corso, che avrà inizio il 14 novembre 2005 e terminerà a fine Luglio 2006, prevede una parte di didattica, in aula ed in laboratorio, di 500 ore e uno stage aziendale di 300 ore, per un totale di 800 ore e 60 crediti formativi. La frequenza è obbligatoria e full time, secondo il calendario che verrà distribuito a inizio corso. I dettagli sugli argomenti trattati nel corso, sono disponibili sul sito:

<http://www.cefriel.it/formazione/masteruniversitari/mastersicurezza.html?lang=it>

La quota di partecipazione è di EUR 6.000 + IVA. Borse di Studio a copertura parziale della quota di partecipazione sono offerte dagli sponsor del corso. È inoltre possibile ricorrere a prestiti e finanziamenti a tasso agevolato da parte di Istituti di Credito convenzionati. Tutte le informazioni sulle agevolazioni potranno essere richieste alla Segreteria del Corso. Per ulteriori informazioni Intesa Bridge <http://www.intesabridge.it/piu/jsp/IntesaBridge/Home>.

La domanda di ammissione dovrà essere compilata direttamente dal sito http://studenti.unimi.it/sifacap/sifa_online.htm dell'università degli Studi di Milano entro e non oltre il giorno 30 Settembre 2005 e comporterà il versamento di una quota di iscrizione alle selezioni pari a EUR 50.

I laureati presso l'università degli studi di Milano avranno accesso al servizio tramite il numero di matricola, gli altri inserendo il codice fiscale.

Il Curriculum Vitae e gli eventuali titoli con allegata la copia dell'avvenuta iscrizione e del versamento devono essere presentati alla Segreteria del Corso presso CEFRIEL, via Fucini 2, 20133 Milano.

Il bando completo è disponibile all'indirizzo:

http://studenti.unimi.it/master/master0506/area_sc/schede/Bruschi.htm

7. NOTIZIE DAI SOCI

Segnaliamo il primo corso SANS a Roma (modalita' Mentor), dal titolo "System Forensics, Investigation and Response",

Il corso, che si terrà presso la Sede di Hewlett Packard di Roma (Via A. Campanile 85 CAP: 00144), affronta una delle aree più interessanti della sicurezza informatica: le tecniche di indagine e di risposta a incidenti di sicurezza. Durante il corso si potrà comprendere quando e come utilizzare tools come Sleuthkit, Autopsy Forensic Browser, Windows Forensic Toolchest (WFT), ecc.

Il corso in modalita' Mentor è suddiviso in 11 sessioni di 2 ore, che si terranno ogni martedì dalle 17,30 alle 19,30 dal 15 Novembre al 31 Gennaio.

Gli studenti avranno a disposizione delle dispense in inglese relative alle sessioni standard del corso e, durante le sessioni, avranno la possibilità di rivedere le sezioni principali con il mentor Alfredo Rinaldi (Solution Architect di HP).

Le sessioni condotte da Rinaldi saranno in italiano: uno dei principali vantaggi dei corsi in modalita' mentor.

L'iscrizione al corso consente inoltre di poter sostenere gli esami per la GCFA (GIAC Certified Forensic Analyst) certificando la conoscenza e gli skill relativi a scenari avanzati di risposta ed indagini formali ad incidenti di sicurezza informatica.

Dal sito del SANS (<http://www.giac.org/certifications/security/gcfa.php>):

"GIAC Certified Forensic Analysts (GCFAs) have the knowledge, skills, and abilities to handle advanced incident handling scenarios, conduct formal incident investigations, and carry out forensic investigation of networks and hosts."

Prezzo speciale per i soci CLUSIT: per chi si iscrive entro il 18 Ottobre: 1700\$; dopo il 18 ottobre: 1800\$.

Riferimento specifico alla sessione in modalita' Mentor di Roma:

<http://www.sans.org/mentor/details.php?nid=1177>

Per i dettagli relativi al corso: <http://www.sans.org/mentor/description.php?tid=161>

8. SEMINARI CLUSIT DI SETTEMBRE

SEMINARIO CLUSIT

Posta elettronica:

Progettare un servizio di posta elettronica sicuro

MILANO 13 settembre 2005

ROMA 27 settembre 2005

Il modulo per registrarsi: www.clusit.it/edu/reg_sem_form.pdf

Per i Soci Clusit la partecipazione è gratuita*

PROGRAMMA

1. Introduzione al problema degli abusi della posta elettronica

- 1.1 Definizioni; motivazioni economiche; evoluzione del fenomeno nel tempo
- 1.2 I costi dello spam
- 1.3 Rapido sommario del quadro legislativo in Italia e nel mondo
- 1.4 Tipologie di spam (per contenuti/scopi)
- 1.5 Truffe via spam e educazione dell'utenza

- 1.6 Strategie per contrastare il fenomeno e ridurre il suo impatto
- 1.7 Aiutare la causa: invio di segnalazioni, archiviazione pubblica

2. SMTP e abusi email

- 2.1 Il protocollo SMTP (RFC2821) e sue implicazioni (falsificazioni)
- 2.2 Passaggio attraverso catene di server e generazione di notifiche DSN
- 2.3 Informazioni dall'header (RFC2822)
- 2.4 SMTP AUTH e Message Submission (RFC2476)
- 2.5 Panoramica dei metodi di trasmissione dello spam; sorgenti pure e miste
- 2.6 Metodi anti-falsificazione (SPF, Sender ID, DKIM)

3. Riduzione della posta abusiva entrante

- 3.1 Definizione delle politiche di filtraggio/blocco
- 3.2 Metodi di notifica di mancate consegne
- 3.3 Analisi pre-DATA: dominio mittente, HELO, IP, rDNS
- 3.4 I database di Spamhaus, e altre liste di blocco pubbliche
- 3.5 Analisi post-DATA: pattern particolari in header
- 3.6 Analisi post-DATA o dopo l'accettazione: filtri sul contenuto
- 3.7 Whitelist e apertura di passaggi garantiti
- 3.8 Tipologie particolari: truffe nigeriane; phishing; virus; 'backscatter'
- 3.9 Nota sui metodi 'Challenge/Response'

4. Eliminazione della posta abusiva uscente

- 4.1 Definizione delle politiche di uso accettabile e di sicurezza email
- 4.2 Filtri sulla porta 25, e il problema degli utenti fuori sede
- 4.3 Identificazione e chiusura dei punti potenzialmente vulnerabili e abusabili da spammers
- 4.4 Riduzione al minimo del backscatter
- 4.5 Acquisire segnalazioni di posta abusiva emessa dalla propria rete

Agenda:

- Registrazione: 13,50
- Inizio Seminario: 14,10
- Fine lavori: 18,10

Docente: Furio Ercolessi**Luogo:**

- Milano allo StarHotel Splendido - Viale Andrea Doria, 4
- Roma al Centro di formazione Percorsi Srl - Viale Manzoni 22

*Condizioni e modalità di iscrizione per Soci e non soci su www.clusit.it/edu
Per ogni informazione chiedere a edu@clusit.it

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

13 settembre 2005, Milano
Seminario CLUSIT "Posta elettronica: Progettare un servizio di posta elettronica sicuro"

27 settembre 2005, Roma
Seminario CLUSIT "Posta elettronica: Progettare un servizio di posta elettronica sicuro"

4 ottobre 2005, Milano
Seminario CLUSIT "Elementi probatori negli illeciti"

7 ottobre 2005, Udine

"Tutti i vantaggi della Rete...SENZA RISCHI 2005: l'Alra Affidabilità nella gestione del Dato"

8 ottobre 2005, Milano

Esame CISSP

18 ottobre 2005, Roma

Seminario CLUSIT "Elementi probatori negli illeciti"

8 novembre 2005, Milano

"ICT, dalla Sicurezza alla Gestione Continua del Business"

14-18 novembre, Milano

Seminario di preparazione all'esame CISSP

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

© 2005 Clusit - Vietata la riproduzione

Clausola di esclusione della responsabilità e informazioni relative al
Copyright: www.clusit.it/disclaimer.htm