Indice

1. NUOVI SOCI

Durante l'ultimo mese hanno aderito al CLUSIT le seguenti organizzazioni:

- ADL Ingegneria Informatica (Conegliano - TV),
- AlgolProducts (Milano),
- BLS Consulting (Pavia),
- Brionregina (Roma),
- CERT-IT ComputerEmergency Response Team (Milano),
- Errevi System (Reggio Emilia),
- Netpeople (Milano),
- Sheltering (Roma),
- T-Systems Italia (Assago - MI).

2. CONFERMATO IL RINVIO PER LA PRIVACY

Come vi avevamo annunciato in anteprima il mese scorso, sono stati prorogati i termini per la presentazione del DPS e per adottare le misure minime di sicurezza previste dal dlg 196/2003. Il provvedimento, riportato nell'Art.6 del decreto-legge 9 novembre 2004, n. 266, relativo a "Proroga o differimento di termini previsti da disposizioni legislative", è stato pubblicato nella Gazzetta Ufficiale n. 264 del 10 novembre 2004 ed è disponibile su www.parlamento.it/parlam/leggi/decreti/04266d.htm

3. OSSERVATORIO PERMANENTE DELLA SOCIETA' DELL'INFORMAZIONE

E' stato presentato a Parma, nel corso della Giornata dell'Innovazione promossa da Confindustria, l'Osservatorio permanente della Società dell'Informazione, realizzato dal Dipartimento per l'Innovazione e le Tecnologie e Federcomin, con la collaborazione di due istituti di ricerca (IDC e Nielsen Media Research).

L'Osservatorio, che ha periodicità semestrale, intende analizzare la domanda nei segmenti delle imprese, cittadini ed istituzioni, aggregando i dati intorno a due focus principali: l'utilizzo dell'ICT, come misura della competitività del Paese, e lo sviluppo dei servizi innovativi. Osservando globalmente tutti gli indicatori che sono stati esaminati nella ricerca, il quadro che ne deriva riflette zone di luce e zone di ombra: se da un lato i servizi internet di base presentano tassi di adozione in netta crescita (come ad esempio la banda larga), l'utilizzo di applicazioni più sofisticate, quali e-Procurement, e-Commerce, e-Learning, è ancora molto contenuto.

La ricerca è disponibile su
www.federcomin.it/Sviluppo/Produzio.nsf/all/6E514EBFD1E47E88C1256F4E003D0FAB/$file/OSSERVATORIO.pdf

(Fonte: FEDERCOMIN. www.federcomin.it)

4. COMPUTER CRIME

COMPUTER CRIME. Trojan finalizzato a catturare i dati dei clienti di una ben determinata banca.

Avevamo accennato molto tempo addietro alla possibilità che dei virus fossero "personalizzati" per attaccare i clienti di una determinata azienda: ciò per ragioni di concorrenza, piuttosto che per ricatto, vendetta, od altro. Tra l'altro, il criminale è facilitato nel suo lavoro, potendo indirizzare la sua attività ad un ben determinato "target".

Ebbene, la Società Sophos segnala che è stato individuato il virus Troj/Ibank che si posiziona sui computer e se l'utilizzatore accede al servizio on-line della National Australia Bank, il trojan intercetta la user-id e la password e li trasmette a ignoti destinatari.

Per ulteriori informazioni: http://www.sophos.com/virusinfo/articles/ozphish.html

CYBER EXTORTION.

Secondo uno studio della Carnegie Mellon University, supportato dall'FBI e da società specializzate, le aziende, non avendo adottato tutte le opportune misure preventive e di gestione dell'incidente, sono sempre oggetto di questa tipologia di attacco che, come dice la parola, ha l'obiettivo di estorcere denaro. L'attacco avviene o con un defacement del sito o la cattura di informazioni riservate, mediante intercettazione o virus. Anche se il 70% dei tentativi di estorsione non va a buon fine, è forse il caso di prepararsi anche a questa tipologia di crimine, vecchia come idea, ma nuova come modalità di esecuzione.

Un'indagine a questo proposito è contenuta nel documento:

InformationWeek-CMU_Cyber_Extortion_Study.pdf, reperibile nell'area Documenti per consultazione del sito istituzionale.

PHISHING.

Il nostro laboratorio sul Phishing segnala che la banca irlandese AIB è stata nuovamente attaccata tramite email scamming; infatti, diverse centinaia di clienti hanno segnalato di avere ricevuto email che sembravano provenire dalla banca. Ricordiamo, che già in un'altra newsletter avevamo riportato la notizia di un primo attacco a detta banca ed accludevamo l'avviso che la AIB aveva prontamente inviato a tutti i clienti, pregandoli di fare estrema attenzione a possibili tentativi di frode, tramite richiesta dello user-id e della password; ciò alle prime "avvisaglie" del pericolo.

Grazie al messaggio di avviso, non si sono registrate conseguenze negative per la banca e per la clientela.

Le autorità irlandesi ritengono che dietro all'attacco ci sia la mafia russa.

Per ulteriori informazioni:
http://home.eircom.net/content/unison/national/4025676?view=Eircomnet

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

5. SICUREZZA INFORMATICA: UNA SFIDA PER GLI UTENTI

Gli utenti americani che si connettono alla rete da casa sottovalutano la questione sicurezza e trascurano lo stato di salute dei pc che utilizzano. E' quanto emerge dall'analisi "Online Safety Study" curato da America Online e dalla National Cyber Security Alliance.

La ricerca, condotta tramite interviste ad oltre 300 utenti adulti con connessione a banda larga e dial-up durante i mesi di settembre e ottobre 2004, ha coinvolto più di 22 grandi città e una dozzina di stati o aree metropolitane sul territorio americano.

Alle dichiarazioni rilasciate ai ricercatori, sono seguiti sopralluoghi sulle macchine per verificare la congruenza o meno con quanto affermato dagli intervistati e i risultati hanno causato un certo sconcerto.

I ricercatori infatti hanno verificato che, nonostante le affermazioni di condotta razionale e sicura rilasciate dal 77% degli utenti, i 2/3 delle macchine non presenta dispositivi particolari di sicurezza, tipo firewall, o si affida a sistemi antivirus obsoleti e non aggiornati, quindi inefficaci.

In aggiunta le verifiche dei ricercatori hanno scoperto che su circa l'80% dei pc esaminati si nascondono, all'insaputa degli utenti, dozzine di programmi spyware in grado di raccogliere e trasmettere informazioni quali uso della tastiera, abitudini di navigazione del Web, password, indirizzi e-mail e altro.

Lo studio è disponibile su http://www.staysafeonline.info/news/safety_study_v04.pdf

(Tratto dalla newsletter n.86 del Ministero per l'Innovazione e le tecnologie)

6. IL RUOLO DEL SISTEMA BANCARIO NELLA LOTTA ALL'INSICUREZZA INFORMATICA

Riportiamo integralmente un articolo del Prof. Danilo Bruschi, pubblicato sul numero di novembre di "Azienda Banca".

Il sistema bancario costituisce uno dei settori più informatizzati del nostro paese e sicuramente quello che dal ricorso alle tecnologie dell'informazione e della comunicazione trae i maggiori profitti. Le esperienze delle carte bancomat, delle carte di credito, delle borsa online, hanno contribuito a creare in questo ambito un nucleo di competenze altamente specializzato, da cui sarebbe il caso di attingere per accelerare il processo di informatizzazione di alcuni settori trainanti del nostro paese come la pubblica amministrazione.

Nell'ambito del sistema bancario, ancora molto legato alla tecnologia main frame e alle reti chiuse, sono maturate notevoli esperienze in materia di protezione dei dati e delle comunicazioni. Oggi la stragrande maggioranza delle transazioni bancarie avviene ancora sulla rete interbancaria, rete privata particolarmente protetta, ma è anche vero che l'home banking sta crescendo ed in prospettiva il problema della sicurezza di Internet sarà anche un problema di sicurezza delle banche, come per altro lo è già in altre realtà.

In questo settore va registrato, da parte del sistema bancario nazionale, un atteggiamento generale di attesismo. L'impressione che se ne ricava, osservando dall'esterno il mondo bancario, è che si stia ancora cercando di valutare la gravità della minaccia per decidere sul da farsi. Per convincersi di questa affermazione basta considerare che, a 16 anni dall'Internet Worm, il sistema bancario italiano non ha ancora emesso alcun documento ufficiale in relazione al problema sicurezza del mondo Internet, e quando parlo di sistema bancario ovviamente non intendo i singoli istituti bancari ma faccio riferimento al sistema nel suo insieme. Non una linea guida, non una best practice, nessuno studio mirato, solo qualche convegno tematico e niente più; queste sono le iniziative che, da interlocutore esterno al settore, ho potuto sinora registrare.

Il black out dello scorso Settembre ha risvegliato la sensibilità di molti ed in particolare ha messo in evidenza quanto il mondo bancario, e non solo, siano oggi fortemente dipendenti dalle infrastrutture informatiche. Congiuntamente alle indicazioni di Basilea 2, questo evento ha scatenato una reazione rilevante in merito al problema della business continuity e disaster recovery. I primi documenti ufficiali sul tema sono apparsi, e oramai quasi tutti gli istituti bancari sono coinvolti nella predisposizione e messa in opera di piani di business continuity. Lascia però perplessi il fatto che ci fosse bisogno di un evento come il black out per smuovere le sfere decisionali. Dobbiamo attendere un altro Internet worm (o black out logico) prima di vedere qualcosa muoversi nel settore della prevenzione degli attacchi informatici?

Il sistema bancario, con il suo bagaglio di competenze tecnologiche e di sicurezza può, e deve, farsi promotore di una cultura della sicurezza informatica che investa tutte le infrastrutture critiche nazionali. Questo è ciò che sta accadendo in altri paesi, e auspichiamo che anche nel nostro si avviino al più presto iniziative concrete, capaci di produrre risultati tangibili, che possano posizionare il sistema bancario nazionale nel suo giusto ruolo nella lotta all'insicurezza informatica del mondo Internet.

Danilo Bruschi

7. PREVISIONI DI CRESCITA DEI PROFESSIONISTI IN INFORMATION SECURITY

Una ricerca effettuata da (ISC)2® e IDC prevede una crescita annuale della forza lavoro in Information Security del 13.7%, arrivando a contare fino a 2.100.000 professionisti nel settore per il 2008 di cui 680.000 in Europa.
Il comunicato stampa è disponibile su
www.clusit.it/isc2/news_ISC2_2004_11_08.pdf
Per avere una copia della ricerca contattare wfstudy@isc2.org

8. SEMINARI DI DICEMBRE

SEMINARIO CLUSIT Crittografia Quantistica
ROMA 7 dicembre 2004

Ci sono ancora posti disponibili.
Il modulo per registrarsi: www.clusit.it/edu/reg_sem_form_2004.pdf
Per i Soci Clusit la partecipazione è gratuite*

PROGRAMMA

1.1 cosa vuol dire QC e QKD (Quantum Key Distribution)
1.2 storia, stato attuale e futuro di QC
1.3 implementazioni di QC e paragone con le tecnologie classiche
1.4 le principali leggi fisiche su cui si basa
1.5 i vari protocolli proposti

2.1 il protocollo BB84 in dettaglio
2.2 dalla teoria alla pratica: gli errori
2.3 tipi di "eavesdropping"
2.4 teoria dell'informazione, leggi di Shannon ed informazione quantistica
2.5 come distinguere gli errori dall'eavesdropping

3.1 vari tipi di implementazioni, in aria ed in fibra e loro problemi
3.2 sistemi a Faint Laser Pulses
3.3 sistemi a photon pairs ed entanglement
3.4 attacchi contro le implementazioni

4.1 descrizione del sistema Plug&Play
4.2 caratteristiche tecniche del sistema Plug&Play
4.3 altri modelli sul mercato e prospettive future
4.4 dimostrazione pratica

Agenda:

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

Docenti: Andrea Pasquinucci, Gregoire Ribordy
Luogo: Centro di formazione Percorsi Srl - Viale Manzoni 22

SEMINARIO CLUSIT Reti WiFi
MILANO 14 dicembre 2004

Sono aperte le iscrizioni.
Il modulo per registrarsi: www.clusit.it/edu/reg_sem_form_2004.pdf
Per i Soci Clusit la partecipazione è gratuite*

PROGRAMMA

1 -Introduzione alle evoluzioni dello standard 802.11x
Cenni all'evoluzione negli standard 802.11
Implementazioni in sicurezza WI-FI, dal WEP all'802.11i
Regolamentare il traffico WPA (WI-FI Protected AREA)

2 - Problemi e rischi in azienda leagti all'uso una rete WiFi
Accesso ed utilizzo illegale della rete aziendale
Fuga ed intercettazione di informazini aziendali sensibili
Attacchi e situazioni non desiderate, la loro probabilità e come mitigarne il rischio:
Policy di sicurezza Aziendale:
Implementazione della security policy:

3 - Case Study: Wireless LAN distribuita
Un tipico setup complesso:
Gli elementi architetturali:
Ridondanza degli elementi
802.1x Metodi a confronto (Sicurezza versus complessità)
Alternative all'802.1x: metodi a confronto:
Cifratura (roadmap)

4 - Le operazioni di Auditing su reti Wi-Fi secondo la metodologia OSSTMM
OSSTMM, metodologia ed ambito di applicazione
Valutare le necessità di business, le policies e gli usi.
Testare hardware firmware e updates degli apparati
Valutare i controlli di accesso, la sicurezza perimetrale, e la possibilità di intercettare ed interferire con le comunicazioni
Valutare le possibilità di accedere a device Wireless con utenze di Amministrazione
Valutare Configurazioni dinamiche di Autenticazione e Cifratura di una rete Wireless
Valutare la sicurezza dei Client di una rete Wireless

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

Docenti: Andrea Baldi, Fabrizio Sensibile
Luogo: StarHotel Splendido - Viale Andrea Doria, 4

*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)

3 dicembre 2004, Milano
Assemblea generale CLUSIT

7 dicembre 2004, Roma
SEMINARIO CLUSIT - "Crittografia Quantistica"

7-8 dicembre 2004, Amsterdam
"The Symposium for Information Security Management"

14 dicembre 2004, Milano
SEMINARIO CLUSIT - "Reti WiFi"

18 gennaio 2005, Roma
SEMINARIO CLUSIT - "Reti WiFi"

25 gennaio 2005, Milano
SEMINARIO CLUSIT - "Tecniche Biometriche"

25 gennaio 2005, Roma
"Migliorare la qualità dei beni e servizi nei contratti ICT delle PA"
Convegno CNIPA/Federcomin

9-11 febbraio 2005, Fiera di Milano
Infosecurity Italia

15 febbraio 2005, Roma
SEMINARIO CLUSIT - "Tecniche Biometriche"

22 febbraio 2005, Milano
SEMINARIO CLUSIT - "Sicurezza VLAN e LAN"

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