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:

- AIIP-Associazione Italiana Internet Providers (Settimo Milanese),
- COMPIT (Catania),
- Educationlab (Napoli),
- IDG Communication Italia (Milano),
- IT Security (Messina), itSMF Italia (Torino). Management Systems Italia (Milano)

2. ISO/IEC 17799 - NUOVA VERSIONE

ISO/IEC 17799

La nuova versione (Giugno 2005) del documento ISO/IEC 17799 è ora ufficialmente disponibile e rimpiazza la precedente rilasciata nel dicembre 2000.

Questa nuova versione contiene 11 capitoli (domini) rispetto ai 10 della precedente, così organizzati:

1) Security Policy
2) Organizing Information Security
3) Asset Management
4) Human Resources Security
5) Physical and Environmental Security
6) Communications and Operations Management
7) Access Control
8) Information Systems Acquisition, Development and Maintenance
9) Information Security Incident Management
10) Business Continuity Management
11) Compliance.

Per chi è familiare con lo standard ISO/IEC 17799, può notare qualche variazione nella nomenclatura dei capitoli e l'aggiunta del dominio relativo all'Incident Management. Questa versione introduce i "controlli" per l'indirizzamento di alcuni temi quali

l'outsourcing, il provisioning e il patch management, oltre all'estensione di temi già coperti in precedenza. Da segnalare anche lo sforzo per cercare di rendere il documento più "user friendly".

DOVE TROVARLA?

All'indirizzo http://www.standardsdirect.org/iso17799.htm, mentre il Toolkit completo è disponibile all'indirizzo http://www.17799-toolkit.com

Per ulteriori informazioni consultare il sito http://17799-news.the-hamster.com.

3. PREVENZIONE FRODI IN AMBITO BANCARIO

PREVENZIONE DELLE FRODI NELLE CARTE DI CREDITO

L'ABI ha recentemente segnalato agli associati che è all'esame della Commissione Finanze della Camera dei Deputati il disegno di legge n.5263 di iniziativa governativa che, unitamente alla proposta n.4947 presentata da alcuni parlamentari, è diretta ad istituire un sistema di prevenzione delle frodi con carte di pagamento (debito e credito), mediante la costituzione presso l'UCAMP (Ufficio Centrale Antifrode sui Mezzi di Pagamento) di un Archivio informatico alimentato da segnalazioni di determinate categorie di dati identificativi utili a contrastare comportamenti fraudolenti.

Tra gli importanti obiettivi:

- rafforzare la sicurezza del circuito di accettazione, attraverso l'eliminazione dal circuito stesso degli esercizi commerciali che accettano consapevolmente carte di pagamento clonate o contraffatte;

- permettere alle banche e agli intermediari finanziari di conoscere tempestivamente le vicende che sono alla base della segnalazione del singolo dato e di individuare con rapidità eventuali comportamenti anomali (o fraudolenti) attuati presso gli esercizi commerciali.

L'UCAMP, con la collaborazione dell'ABI e di un rappresentativo gruppo di lavoro interbancario, ha in corso di elaborazione una bozza del regolamento di attuazione.

Il 21 e 28 giugno si terranno degli eventi formativi / informativi presso l'UCAMP.

Considerato il trend di crescita delle frodi e la frequente complicità offerta da alcuni esercizi commerciali, l'iniziativa è assolutamente importante e dovrà trovare, negli intermediari finanziari, il giusto sostegno e collaborazione.

PHISHING.

Il laboratorio sul phishing segnala che alcune banche inglesi, a seguito di perdite ammontanti a circa 12 mil. di sterline, hanno deciso di:

- postporre di un giorno i bonifici fra clienti della stessa banca, così da dare l'opportunità di eseguire dei controlli sulle disposizioni;
- realizzare programmi di monitoraggio dei movimenti dei conti, in modo da individuare bonifici anomali.

Sono queste le prime misure adottate, in considerazione del trend di crescita di questa tipologia di frode.

La nuova precauzione non ci risulta sia stata gradita dalle associazioni dei consumatori che, invece, chiedono una maggiore velocità di esecuzione delle disposizioni dei clienti e migliori misure di sicurezza.

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

In queste ultime settimane si è parlato molto di phishing, in particolare in relazione a massicci invii di email fraudolente, per la prima volta in lingua italiana.

A tal proposito, osserviamo che già da tempo, nella loro comunicazione (generalmente tramite il sito web della banca), molte banche avvertono i propri clienti che non

chiederanno mai agli stessi di collegarsi al sito della banca per inserire codici utente, User Name, Password.

Ci preoccupiamo però di un fenomeno che ci viene segnalato negli USA, dove è ormai frequente che servizi online, anche di carte di credito, inviino ai propri clienti email che vanno proprio nel senso opposto. Il caso tipico è quello di una banca che offre un nuovo servizio ed invia a tutti i propri clienti via email l'annuncio del servizio con l'URL da cliccare per attivarlo; il messaggio dice anche che cliccando l'URL verranno chieste le username e password del servizio online che già si ha presso la banca, e questo attiverà automaticamente il nuovo servizio, che poi sarà possibile personalizzare.

Per ora non ci risultano pratiche di questo tipo nella comunicazione delle banche italiane ed europee e vogliamo proprio sperare che ciò non avverà mai, in quanto potrebbe rendere vano qualunque sforzo di educazione dell'utente da parte di Istituzioni, Polizia, Associazioni di consumatori e Istituti Finanziari.

4. ACCORDO CLUSIT/IDG

CLUSIT ed il gruppo editoriale IDG hanno firmato un'accordo di partnership che prevede tra l'altro:

1. La possibilità per CLUSIT di far pubblicare in modo ricorrente su alcune riviste del gruppo editoriale IDG (Computerworld, Networkworld e gli allegati CIO e CSO) articoli tecnico-scientifici e divulgativi. Tali articoli, di taglio scientifico e quindi non commerciale, potranno anche essere scritti direttamente dai soci CLUSIT e, in tal caso, saranno sottoposti al vaglio del Comitato Tecnico Scientifico (CTS) del CLUSIT.
2. La possibilità per CLUSIT di promuovere le attività dell'associazione, con cadenza mensile, tramite una pagina dedicata, sia su ComputerWorld che su NetworkWorld.
3. La possibilità per CLUSIT di utilizzare, per le pubblicazioni di cui sopra, anche le varie testate online di IDG Italia.
4. La possibilità per i soci di sottoscrivere il doppio abbonamento alle testate Computerworld e Networkworld a condizioni particolari.

L'idea è quella di avere alcune riviste di larga diffusione che supportino l'associazione e la comunità che questa rappresenta, facendoci da veicolo di diffusione periodica.

5. CLUSIT CHIEDE UN SOSTEGNO AGLI INVESTIMENTI IN SICUREZZA INFORMATICA

Riportiamo il testo della lettera che il Clusit ha inviato il 22 giugno all'On. Lucio Stanca.

Egregio Signor Ministro,

in nome e per conto dell'Associazione Italiana per la Sicurezza Informatica (CLUSIT), che rappresenta oltre 400 imprese ed organizzazioni, significative per l'intero Sistema Paese, desidero trasmetterLe un appello, che corrisponde ad una precisa esigenza, emersa nel corso dell'assemblea generale dell'Associazione dello scorso 27 maggio.

Mi riferisco alla necessità che il Governo inserisca iniziative di sostegno alla sicurezza informatica nell'ambito dei finanziamenti previsti per la diffusione della banda larga.

Senza sicurezza informatica, la vita delle imprese e dell'intero Sistema Paese è a rischio. Le infrastrutture informatiche sono ormai da considerare infrastrutture critiche e vitali per tutti. Più le connessioni veloci e continue si diffondono, più si alza il rischio che un computer non protetto entri in rete divenendo sia vittima di intrusioni che veicolo di attacchi agli altri sistemi. Soluzioni di sicurezza perimetrale e barriere ai

virus e ai worm hanno la stessa funzione che hanno avuto le vaccinazioni di massa per debellare gravi malattie epidemiche.

Oltre che incentivare la connessione ad alta velocità, occorre che vengano incentivati anche l'adozione di idonee soluzioni per la sicurezza informatica. È inoltre necessaria un'operazione di sensibilizzazione di tutti gli utenti delle linee a banda larga, ADSL e fibra, affinché capiscano l'importanza di dotarsi di adeguati sistemi di protezione.

Sono certo che Ella saprà valutare l'importanza e l'urgenza di tali azioni di sostegno da parte del Governo, e La prego fin d'ora di considerare l'Associazione che rappresento a Sua completa disposizione in tutte le iniziative in cui Ella ritenesse di coinvolgerla.

Con osservanza,

Gigi Tagliapietra

Presidente CLUSIT

6. LA FINE DI MD 5

Nell'agosto 2004 alcuni ricercatori annunciarono la scoperta di alcune preoccupanti vulnerabilità nell'algoritmo di Hash MD5. MD5 è sicuramente l'algoritmo crittografico di Hash più in uso. Dato un documento od una qualsiasi stringa di bit, un algoritmo crittografico di Hash produce una impronta di lunghezza fissa che lo individua praticamente in maniera unica.

L'impronta di un documento prodotta da un algoritmo crittografico di Hash viene usata principalmente per identificare il documento stesso e verificare che il documento non sia stato modificato. Gli algoritmi crittografici di Hash e le impronte da loro generate sono elementi fondamentali della maggioranza dei protocolli crittografici attuali, dalle firme digitali alle VPN cifrate. In particolare, i certificati digitali, le CA, PKI ed i protocolli per le firme digitali basano molte delle loro caratteristiche sulle proprietà degli algoritmi crittografici di Hash, ed in particolare quasi tutti adottano MD5.

Purtroppo le vulnerabilità di MD5 scoperte lo scorso agosto si sono rivelate anche più severe di quanto si potesse immaginare inizialmente.

E' ora possibile, anche se non è ancora facile, costruire due documenti simili ma dal significato del tutto diverso, che hanno la stessa impronta MD5. Ad esempio sul sito http://www.cits.rub.de/MD5Collisions/ due ricercatori tedeschi mostrano due documenti in formato Postscript diversi nei contenuti ma con la stessa impronta MD5. E' facile e consigliato a tutti, scaricare i due documenti di una sola pagina e verificare di persona che hanno la stessa impronta MD5, ma che invece l'algoritmo crittografico di Hash SHA1 genera per loro impronte diverse.

Si possono facilmente immaginare le possibili conseguenze di una firma digitale che utilizzi MD5 su di un contratto elettronico.

Cosa fare ora? Ovviamente cercare di evitare di usare MD5. Di solito i certificati digitali durano un anno, e le CA dovrebbero emettere i nuovi certificati digitali utilizzando un altro algoritmo di Hash. Anche chi utilizza la firma digitale dovrebbe fare lo stesso, ovvero non usare più MD5, il che potrebbe non essere così facile se le firme sono fatte in smart-card o simili. Inoltre tutti i documenti elettronici già firmati e per i quali era stato usato MD5 come algoritmo di Hash, dovrebbero essere firmati digitalmente di nuovo con un diverso algoritmo di Hash.

Quale algoritmo di Hash usare oggi? Il sostituto naturale di MD5 è SHA1, purtroppo anche SHA1 ha delle vulnerabilità simili a quelle di MD5, anche se per il momento meno gravi. Passare oggi a SHA1 potrebbe voler dire ritrovarsi tra un anno nell'identica situazione di oggi ma per SHA1. Le alternative sono gli algoritmi SHA256, SHA512 e Whirpool che purtroppo sono molto recenti, poco studiati e poco diffusi. Quindi la strada che i più stanno adottando è quella di passare subito a SHA1 già prevedendo di doverlo sostituire a breve.

(Autore: Andrea Pasquinucci, CTS CLUSIT)

7. NUOVO SYLLABUS DELLE CERTIFICAZIONI EUCIP ADMINISTRATOR

Sono stati pubblicati i nuovi sillabi (versione 2.0) delle certificazioni Eucip IT Administrator.

Il Modulo 5 - Sicurezza Informatica è disponibile in italiano all'indirizzo:

http://www.eucip.it/it_administrator/pages/IT_ADM_Sillabus2_0/Module5_ita.pdf.

Clusit ha partecipato alla revisione di tutti i moduli e in particolare a quella del mod 5 che ha visto un notevole incremento e revisione delle voci, proprio per la rapidità di evoluzione di questo argomento rispetto agli altri moduli.

Dal 23 giugno è disponibile nelle librerie il libro

"**Sicurezza Informatica. EUCIP IT Administrator - Modulo 5 2/ed**

(http://www.catalogo.mcgraw-hill.it/catLibro.asp?item_id=1940).

La presentazione del libro è disponibile su:

http://www.catalogo.mcgraw-hill.it/pdf/indice_pref/4423-3_pref.pdf.

Per consultare l'indice del libro:

http://www.catalogo.mcgraw-hill.it/pdf/indice_pref/4423-3_indice.pdf.

8. BREVETTABILITÀ DEL SOFTWARE

Riportiamo il testo di un messaggio che il Clusit ha appena inviato a tutti gli europarlamentari italiani.

In vista del voto previsto dal Parlamento Europeo il prossimo 6 luglio, il Clusit, l' Associazione Italiana per la Sicurezza Informatica , che rappresenta oltre 400 imprese ed organizzazioni, significative per l'intero Sistema Paese, esprime la sua contrarietà all'ipotesi di brevettabilità del software, in quanto ritiene che tale approccio costituisca un freno allo sviluppo di adeguati sistemi di sicurezza che basano la propria solidità su protocolli e standard aperti arricchiti e rafforzati dalla collaborazione del maggior numero di contributi possibili.

Le sfide alla sicurezza a cui si dovrà far fronte nell'immediato futuro, richiedono un approccio di grande apertura, le reti e i sistemi su cui il nostro paese e l'Europa baseranno il proprio futuro potranno essere adeguatamente protette solo con uno sforzo cooperativo di molteplici soggetti, che garantisca ai sistemi di sicurezza facilità di integrazione e soprattutto tempestività nella adozione di contromisure efficaci e condivise.

9. NOTIZIE DAI SOCI

CEFRIEL e MIP Politecnico di Milano, propongono la **4a Edizione del Corso di formazione in Information Security Management** con inizio a Settembre 2005, con due edizioni a Milano e a Roma.

Il Corso si articola in sessioni quindicinali nei giorni di venerdì (8 ore) e sabato mattina (4 ore) lungo un arco di circa 8 mesi, per un totale complessivo di 200 ore, e prevede la realizzazione di un project work di gruppo incentrato su problematiche reali.

L'ammissione al Corso è limitata ad un numero massimo di 40 partecipanti per edizione, ed è prevista una selezione basata sulla valutazione preliminare dei curricula dei candidati e

un colloquio individuale. La domanda di ammissione dovrà essere compilata direttamente sul sito ww.securman.it entro il 31 luglio 2005.

Per informazioni: Ciro Marconi, Coordinamento ISM, tel. 02.2399.2881,

e-mail: securman@cefriel.it, web site: www.securman.it.

E' arrivata all'ottava edizione, la **Global Information Security Survey**, ricerca annuale realizzata da Ernst & Young e che ha l'obiettivo di analizzare la domanda di Information Security presso le più importanti realtà di mercato, al fine di capire come aziende, enti pubblici e non-profit stiano attrezzandosi per rispondere efficacemente ai problemi legati a questi temi.

E' un'iniziativa che ha ormai una tradizione pluriennale anche in Italia e che, negli anni scorsi, ha dato spunti di riflessione veramente interessanti.

Per chi fosse interessato i risultati dell'ultima ricerca sono disponibili all'indirizzo: www.ey.com.

Da quest'anno è stata introdotta anche una novità: alla tradizionale ricerca basata su questionari rivolti al management aziendale, si affianca un secondo momento di indagine, attraverso la compilazione, da parte di personale Information Security dell'azienda, di un questionario on line, basato sullo standard ISO 17799 che permetterà ai partecipanti, di ottenere immediatamente un benchmarking e la produzione di grafici di posizionamento.

La Survey sarà condotta nel mese di giugno e luglio 2005 e i risultati saranno disponibili a partire da settembre: ogni partecipante riceverà una copia del report EYG insieme ai dati sulla situazione del mercato italiano.

Chiunque volesse partecipare alla survey può scrivere a: Raffaella.Dalessandro@it.ey.com

ANSSAIF ha organizzato un Seminario di studio specialistico sulla Business Continuity: "**L'attuazione del piano operativo di business continuity: problematiche realizzative, di aggiornamento e di auditing**".

Il Seminario si terrà a Siena, il giorno 8 luglio, presso: Monte dei Paschi di Siena, Centro di Formazione di Gruppo, Villa Isabella, V.le Camillo Benso di Cavour, 24.

Il programma è disponibile all'indirizzo http://www.clusit.it/eventi/050708_anssaif.pdf.

Il Seminario è gratuito e riservato ai soci AIEA, ANSSAIF e CLUSIT.

Si prega confermare la partecipazione inviando una email a info@anssaif.it.

10. SEMINARI CLUSIT DI LUGLIO

SEMINARIO CLUSIT

L'utilizzo delle strumentazioni informatiche e telematiche aziendali e il controllo sui lavoratori

MILANO 5 luglio 2005

ROMA 19 luglio 2005

Per la sessione di Milano solo due posti disponibili,

Per quella di Roma sono aperte le iscrizioni.

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

Per i Soci Clusit la partecipazione è gratuita*

PROGRAMMA

Aspetti giuridici sottesi all'utilizzo delle strumentazioni informatiche e telematiche da parte dei lavoratori

Gli abusi da parte dei lavoratori
Casistica esemplificativa
Diritti e doveri del lavoratore
Diritti e doveri del datore di lavoro
Principi giuridici applicabili
- i principi del codice civile
- i prinicipi dello Statuto dei Lavoratori
- i prinicipi stabiliti dalle normative in materia di riservatezza
- i prinicipi in tema di segretezza della corrispondenza

Limiti e poteri di controllo da parte del datore di lavoro
- il potere disciplinare
- i controlli difensivi

I controlli specifici:
- la posta cartacea
- la posta elettronica
- l'uso di internet
- il contenuto del pc

L'assunzione degli elementi probatori
La funzione delle policy interne:
- cosa prevedere
- come negoziarle

L'esperienza della Fondazione Centro San Raffaele del Monte Tabor

---

Agenda:
-Registrazione: 13,50
-Inizio Seminario: 14,10
-Fine lavori: 18,10
Docenti: Gabriele Faggioli, Piergiorgio Sammartino
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

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

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

8 luglio 2005, Siena
Seminario ANSSAIF "L'attuazione del piano operatico di business continuity: problematiche realizzative, di aggiornamento e di auditing"

13-14 luglio 2005, Milano
Bank Security Days

16 luglio 2005, Roma
Esame CISSP

19 luglio 2004, Roma
Seminario CLUSIT "Controllo dei lavoratori

23-28 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