Indice

1. NUOVI SOCI

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

- CONFORTI (S. Martino Buon Albergo - VR),
- EDISON Informatica (Cosenza),
- NEMESI IT (Vicenza),
- LOTTOMATICA (Roma).

2. UN ITALIANO ALLA DIREZIONE DELL'ENISA

Andrea Pirotti è stato nominato Direttore esecutivo dell'ENISA (European Network & Information Security Agency).

L'ENISA, con sede a Creta, avrà il compito di accelerare i tempi di risposta dei network europei alle minacce emergenti.

Siamo molto lieti per questa nomina, che mette l'italia in prima linea nella lotta alla criminalità organizzata su Internet e facciamo i nostri migliori auguri al neoeletto Direttore.

Ulteriori informazioni sull'ENISA sono disponibili su www.enisa.eu.int

Il profilo di Andrea Pirotti è disponibile su www.pirotti.com

3. LA BANCA APERTA

CLUSIT e ANSSAIF hanno organizzato, assieme a Edipi Conference, un convegno sul tema "La Banca Aperta. Business continuity e sicurezza nella banca multicanale". Il convegno si terrà a Milano il prossimo 14 ottobre.

PROGRAMMA (Chairman Andrea Bigi, direttore AziendaBanca)

8,30 Registrazione

9,00 Apertura dei lavori a cura di Danilo Bruschi, presidente del Clusit

9,15 La Business Continuity nel mondo finanziario, Renato Bruno, direttore principale, Ufficio Sorveglianza sul Sistema dei Pagamenti, Banca d'Italia.

9,45 Business Continuity oggi in Italia: stato dell'arte, problematiche, primi risultati dai progetti ANSSAIF, Antony C. Wright, presidente di Anssaif

10,15 Riavvicinamento al cliente, quale impatto sulla sicurezza?, Stefano Cabianca, Responsabile Servizio Gestione Sicurezza Informatica, Direzione Sistemi Informativi, Banca Intesa

10,45 Business Continuity: competenze, tecnologia e infrastutture, Franco Masone, responsabile Area Gestione e Progetto di Business Continuity Cedacri

11,15 Coffee break

11,40 La protezione invisibile dei clienti e dei dipendenti della banca. Giuseppe Gangai, marketing manager sicurezza, Elsag Divisione Finance Solutions

12,10 Business Continuity: la metodologia IBM, Sergio Eufemi, Business Continuity & Recovery Services IBM South Region Leader

12,40 Il nuovo T.U. sulla protezione dei dati: quale impatto sull'IT delle banche?, Avv. Andrea Monti, Comitato Tecnico Scientifico del Clusit

13,00 Domande e risposte e Chiusura dei lavori

Per iscriversi al convegno: www.edipi.com/conference/banca_aperta/registrazione.php

4. SMAU 2004

CLUSIT sarà alla prossima edizione di SMAU, che si terrà alla Fiera di Milano dal 21 al 25 ottobre.

Nello stand del CLUSIT sarà presente una "collettiva" costituita da alcune aziende socie: ADHERSIS, COLT TELECOM, CONFORTI, IKS, MIDASYS, PRES, PROGRAMATIC, SIOSISTEMI.

Durante le giornate di giovedì 21, venerdì 22 e lunedì 25, saremo disponibili per delle consulenze gratuite al **Padiglione 12, Stand B34**

5. DOCUMENT E CONTENT MANAGEMENT A INFOSECURITY 2005

Nell'ambito della prossima edizione di Infosecurity Italia, che si terrà alla Fiera di Milano dal 9 all'11 febbraio 2005, oltre a Storage Expo Italia che ha avuto un buon successo nello scorso febbraio, è prevista la presenza di una nuova area tematica,"Documation", che sarà dedicata all'information lifecycle management, presentando soluzioni di Document e Content Management.

"Documation" ha sponsorizzato uno studio, commissionato da AIDOC-Associazione Italiana Imprese Gestione Documenti e realizzato da SIRMI. Lo studio, che illustra lo scenario italiano del document e content management, vuole essere un punto di riferimento su cui costruire e misurare le attività delle aziende e le esigenze di questo mercato che condivide molteplici aspetti sia con la sicurezza IT che con lo storage management.

Lo studio, realizzato attraverso un'attività desk di individuazione dei principali operatori e delle diverse tipologie di offerte, traccia un quadro completo sul mercato italiano dei servizi e delle soluzioni per la gestione e l'archiviazione dei documenti inteso nella sua più vasta accezione: dalla gestione fisica del documento, e quindi da attività tipiche delle tematiche della logistica e della gestione di magazzini, fino a quelle più specificatamente correlate all'Information & Communication Technology.

Il dato più rilevante che risulta dal rapporto è che nel 2004 il comparto del document management muoverà un mercato di quasi 598 milioni di Euro e che nel 2005 supererà i 667 milioni di Euro, con tassi di crescita dell'11%.

6. COMPUTER CRIME

Insider Threat Study

Lo US Secret Service e il CERT hanno pubblicato uno studio dal titolo: Insider Threat Study: illicit cyber activity in the banking and finance sector.

L'indagine ha riguardato dei casi ampiamente documentati e, tra l'altro, sono stati intervistati anche alcuni degli autori.

Sono stati analizzati diversi casi di "incidents" causati da personale interno che intenzionalmente ha superato i controlli esistenti o ha abusato della propria autorità per compromettere, manipolare o accedere illegalmente a risorse informatiche od

informative, ai fini di ottenere, divulgare, cancellare, manomettere o aggiungere informazioni in modo illegale.

Riassumiamo, in estrema sintesi, i principali dati:

- Le perdite economiche segnalate dalle aziende variano da 168 a 691 milioni US$; il 30% dei sinistri ha superato i 500.000 $.

- Il 26% delle aziende colpite ha segnalato di aver avuto una perdita reputazionale, ma non l'ha quantificata.

- L'83% degli incidenti è iniziato all'interno dell'azienda ed il 70% è stato portato avanti durante l'orario di lavoro.

- Nell'87% dei casi sono stati usati comandi semplici ed autorizzati; infatti, solo il 13% degli atti criminali ha richiesto tecniche di spoofing o flooding, e, in gran parte, con la scrittura di linee di "codice".

- Il 70% dei criminali ha sfruttato o tentato di sfruttare vulnerabilità nelle applicazioni, processi o procedure.

- Il 61% ha sfruttato vulnerabilità esistenti nell'hardware, software o nella rete.

- Il 78% degli insiders è rappresentato da personale autorizzato ad accedere ai sistemi.

- Il 43% ha usato le sue credenziali di accesso e solo il 26% quelle di colleghi.

- Il 23% era impiegato in ruoli tecnici.

- Il 17% possedeva credenziali di system administrator / root.

- L'81% l'ha fatto per motivi di guadagno; di questi, il 27% si trovava in difficoltà economica.

- In diversi casi, criminali esterni hanno pagato personale interno per modificare dati.

In un caso, con elevato danno economico, l'autore della frode, intervistato, ha dichiarato: ciò può avvenire quando "la volpe viene messa a guardia del pollaio"!

Si riferiva al fatto che l'auditor, che avrebbe dovuto controllarlo, dipendeva dal suo stesso capo!

A 10 anni di distanza, Mark Leeson della famosa Barings (la banca che,come noto, aveva la regina Elisabetta come cliente, ed ora scomparsa dal mercato - la banca, s'intende) sembra non aver insegnato nulla!

Come diceva un relatore ad Infosecurity 2004, la tecnica per portare avanti il crimine non è cambiato, è cambiata la tecnologia: una volta si catturava la parola chiave "apriti Sesamo!" ascoltando nascosti, ed oggi? Non è molto diverso! Si cattura la parola chiave, "ascoltando" sul pc, osservando mentre si digita… E' quindi ovvia una prima conclusione: le misure di prevenzione che si devono instaurare (ricordiamo che la recente normativa della Vigilanza insiste sulle misure preventive, non solo di emergenza, a fronte di possibili scenari, inclusi gli atti di sabotaggio) non possono non essere pianificate congiuntamente da chi sa come potrebbero verificarsi degli eventi criminosi e da chi conosce le tecniche e tecnologie utilizzabili a tale scopo.

Un'altra considerazione: se un criminale esterno non trova complicità all'interno dell'azienda, ben difficilmente riesce a portare avanti una frode!

Bisogna, inoltre, sottolineare un altro fatto importante: gli esempi sopra citati, indicano che le frodi o i danni (ad esempio, per vendetta) sono stati eseguiti, nella gran maggioranza dei casi, sfruttando le vulnerabilità esistenti!

Ciò non può che sottolineare l'importanza di eseguire periodiche analisi dei rischi, onde individuare eventuali vulnerabilità, e di audit, anche a sorpresa.

Non ultimo, se chi si occupa di Sicurezza non fa tesoro di come vengono portate avanti gli atti criminali e non apporta, o suggerisce di apportare, le necessarie modifiche ed integrazioni ai processi aziendali, tutti gli investimenti in sicurezza diventano vani.

Tutto ciò premesso, qualche domanda è d'obbligo: quante risorse degli attuali uffici sicurezza ICT delle banche hanno una sufficiente esperienza amministrativo-contabile che permette loro di capire se esiste una vulnerabilità capace di essere sfruttata per possibili frodi contabili? Quanti audit di questo tipo vengono condotti annualmente? Quali sinergie esistono fra chi conosce la tecnologia e chi conosce come si portano avanti le frodi da parte delle bande criminali? Quanti modelli comportamentali vengono realizzati all'interno delle banche, in modo da poter anticipare eventuali comportamenti anomali di alcuni utenti?

Quali sinergie esistono fra Sicurezza ICT, Sicurezza fisica, ed internal auditing? Esistono?

Un'ultima domanda: che riflessioni sta facendo l'azienda che ha perso 691 milioni di dollari? Quali provvedimenti ha preso ora?

Phishing

L'ultimissima su questo tema è la disponibilità di un kit per il perfetto...produttore di attacchi di phishing!

C'è tutto l'occorrente per fare un sito web uguale in tutto e per tutto a quello i cui clienti si vuole ingannare.

Per maggiori informazioni (non per l'acquisto, però), consultare:

http://www.sophos.com/spaminfo/articles/diyphishing.html

Il nostro laboratorio sul Phishing segnala, infine, che la banca cinese OCBC ha comunicato alle Autorità di Singapore che è stata colpita con la tecnica di "phishing". Ai suoi clienti, infatti, è pervenuta una email nella quale si chiedeva di digitare per verifica il codice di conto e la password.

Chiaramente la richiesta non perveniva dalla banca.

Altra analoga segnalazione proviene dalla AL-South Trust e, per la prima volta, da due banche tedesche: Postbank AG e Deutsche Bank AG.

Per ulteriori informazioni:

www.channelnewsasia.com/stories/corporatenews/view/105416/1/.html

http://birmingham.bizjournals.com/birmingham/stories/2004/08/30/daily29.html

www.computerworld.com/softwaretopics/software/groupware/story/0,10801,95429,00.html

PDA

Una indagine commissionata dalla Pointsec Mobile Technologies ha riscontrato che i PDA, contenenti in genere dati riservati dell'azienda alla quale appartiene il possessore, non utilizzano tecniche di crittografia e ben un terzo non è protetto da password.

Ne possiamo concludere che, tra laptop e PDA, la riservatezza dei dati sta divenendo un'utopia, a meno di prendere rapidi provvedimenti.

Fra questi, vorremmo ricordare, vi è quello di produrre, approvare agli opportuni alti livelli, e diffondere a tutto il personale, le policy di sicurezza aziendali. E le policy devono contenere i riferimenti alla legislazione e normativa vigente: uomo avvertito...

Ribadiamo questo concetto perchè diverse indagini, in Italia ed all'estero, indicano che mediamente il 50% del personale delle aziende non conosce in quali rischi incorre se compie determinate azioni; è dimostrata l'ignoranza della legge!

Come è stato ampiamente documentato dalla prof.sa Bruzzone al convegno di Acaya, già durante un primo intervento informativo / formativo sulla protezione dei dati, in alcune aziende si sono avuti degli immediati benefici.

Per informazioni sulla citata indagine, riferirsi a:

http://www.theregister.co.uk/2004/09/01/pda_sec

***Fonte**: ANSSAIF - Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria*

7. INTERVENTO DELLA COMREG IRLANDESE

La ComReg, l'ente che è incaricato di controllare le comunicazioni telefoniche in Irlanda, bloccherà le chiamate telefoniche dirette verso 13 paesi, in gran parte piccole isole del Pacifico, per proteggere le vittime di un nuovo tipo di truffa su Internet.

La truffa è compiuta tramite un virus, che modifica, all'insaputa dell'utente, il numero di telefono utilizzato per contattare il proprio Internet Provider.

Nel corso del 2004 la ComReg ha ricevuto molte segnalazioni da parte di utenti, che avrebbero subito fino a 2.000 euro di spese telefoniche impreviste.

Il blocco delle telefonate comincerà il 4 ottobre e riguarda: Norfolk, Nauru, Sao Tome e Principe, le isole Cook, Tokelau, Diego Garcia, Wallis e Futuna, Tuvalu, le Comore, Kiribati, le isole Salomon, la Mauritania e la Polynesia francese.

Naturalmente, gli irlandesi che volessero veramente telefonare in uno di questi paesi, potranno ottenere lo sblocco delle linee su semplice segnalazione.

All'inizio di quest'anno, anche gli Internet Provider inglesi erano stati il bersaglio di questo tipo di truffa.

Non possiamo che complimentarci con la ComReg irlandese, per la sua iniziativa.

Ci sembra evidente che sono le Autorità competenti, più che i singoli utenti, a dover prendere le misure necessarie (anche se drastiche) per impedire questo genere di truffe.

8. SEMINARI DI OTTOBRE

SEMINARIO CISSP
MILANO 11-15 ottobre 2004

Ancora qualche posto disponibile per l'ultimo seminario del 2004 in Italia.

Tutte le informazioni su www.clusit.it/isc2. Per essere avvisati quando saranno disponibili le date di seminari ed esami 2005 iscriversi alla mailiglist: www.clusit.it/isc2/form_news_isc2.htm.

SEMINARIO CLUSIT Voice-over-IP
ROMA 12 ottobre

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

Introduzione alla VoIP

Considerazioni su QoS

Protocolli Voce:

- H.323
- SIP
- Gateway decomposition

Considerazioni di sicurezza:

- Address translation
- Firewall
- Cifratura IPSec e cifratura alternativa
- Rischi, minacce e vulnerabilitá generiche

Considerazioni sul deployment, disponibilitá, integrazione, gestione e monitoraggio:

- Convergenza ed IP Telephony: scenari e ruoli tecnologici
- Architetture disponibili: pro e contro
- IP Telephony: i punti di controllo
- Percorsi e problematiche della migrazione

Conslusioni, Q&A

Agenda:

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

Docenti: Stefano Bodini, Marco Misitano

Luogo: Centro di formazione Percorsi Srl - Viale Manzoni 22

SEMINARIO CLUSIT Documento Elettronico
MILANO 19 ottobre 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. Definizioni e normative; uso del documento elettronico nelle aziende

1.1 Dal documento cartaceo al documento informatico: brevi cenni

1.2 Cosa è il documento informatico: il D.P.R. 445/2000.

1.3 La validità legale del documento informatico

1.4 Il documento informatico sottoscritto: l'impatto delle normative comunitarie sulla disciplina nazionale

2. Il documento elettronico nella Pubblica Amministrazione, nei servizi al cittadino e alle imprese; stato attuale

2.1 L'evoluzione della tecnologia nei rapporti tra il cittadino/impresa e la Pubblica Amministrazione

2.2 Documenti amministrativi e atti pubblici

2.3 Copie di atti e documenti pubblici

2.4 Cenni alla disciplina della carta d'identità elettronica e del protocollo informatico

3. Problemi tecnici: i formati dei documenti elettronici

3.1 Open Source e P.A.:formati proprietari e non proprietari

3.2 Vantaggi derivanti dall'utilizzo di programmi open source

3.3 Il decreto del Ministro per l'Innovazione e le Tecnologie del 31 ottobre 2002 sull'open source nella pubblica amministrazione

3.4 Immodificabilità del documento elettronico: attenzione ai contenuti attivi

4. Impatto dell'evoluzione normativa sui processi, sull'attività e sui processi aziendali

4.1 Integrazione del documento elettronico nei flussi documentali

4.2 L'archiviazione e la conservazione digitale dei documenti

4.3 Originale e copia nel mondo digitale

4.4 La fattura elettronica

4.5 Brevi cenni sulla privacy e sulla sicurezza dei dati

Agenda:

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

Docenti: Gabriele Faggioli, Daniela Rocca

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)

7-8 ottobre 2004, Milano

IBM Global Security Conference III

7-8 ottobre 2004, Ginevra

"Homeland Security Forum - The United States, Europe and Beyond: New Challenges for Institutions and the Private Sector"

11-15 ottobre 2004, Milano

Seminario di preparazione all'esame CISSP

12 ottobre 2004, Roma

SEMINARIO CLUSIT - "Voice-over-IP"

13 ottobre 2004, Milano
"Facciamo il punto sulla sicurezza"

14 ottobre 2004, Milano
"La banca aperta - Business continuity e sicurezza nella banca multicanale"
Conferenza organizzata da AZIENDA BANCA (edipi), in collaborazione con ANSSAIF e CLUSIT

19 ottobre 2004, Milano
SEMINARIO CLUSIT - "Documento Elettronico"

21-25 ottobre, Fiera di Milano
SMAU

8-12 novembre 2004, Milano
Mastercourse Security Manager

16 novembre 2004, Roma
SEMINARIO CLUSIT - "Documento Elettronico"

18 novembre 2004, Roma
"Facciamo il punto sulla sicurezza"

20 novembre 2004, Milano
Esame CISSP

23 novembre 2004, Milano
SEMINARIO CLUSIT - "Crittografia Quantistica"

24-25 novembre 2004, Paris
Le Salon de la Sécurité Informatique

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

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

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