

Indice

1. **NUOVE CARICHE DEL CLUSIT**
2. **Internet e Minori, Internet e Valori - Quali strategie per la sicurezza della Rete**
3. **COMPUTER CRIME**
4. **Dalla Newsletter del MIT**
5. **DOCUMENTO CLUSIF: "La Riforma di BASILEA 2 - Una presentazione generale"**
6. **MASTER**
7. **SEMINARI CLUSIT DI GENNAIO**
8. **EVENTI SICUREZZA**

1. NUOVE CARICHE DEL CLUSIT

Durante l'assemblea elettiva di dicembre è stato rinnovato il direttivo del CLUSIT, nella stessa occasione è stato eletto il nuovo presidente. Dopo quattro anni di mandato il presidente Danilo Bruschi, tra i fondatori dell'associazione, ha passato il testimone: "Sono convinto che le cariche direttive debbano essere rinnovate per portare nuove idee e nuovi stimoli" ha dichiarato Bruschi nel discorso di apertura dell'assemblea, con il quale ha riepilogato il lavoro degli ultimi anni di mandato e spiegato le ragioni che lo hanno portato a non ricandidarsi. "In questi quattro anni il Clusit è cresciuto molto, oggi abbiamo superato i 400 iscritti, e abbiamo creato numerose relazioni sia con altre associazioni sia con le istituzioni. Abbiamo lavorato per diffondere una cultura della sicurezza informatica e ritengo che abbiamo raggiunto notevoli risultati. Ma gli orizzonti possibili sono tanti e un nuovo presidente, sostenuto da un direttivo dinamico, può dare un nuovo impulso. Continuerò ad essere vicino all'associazione e a dare il mio contributo scientifico." Su proposta del segretario generale, Paolo Giudice, l'assemblea all'unanimità ha nominato Danilo Bruschi, presidente onorario a vita.

L'assemblea ha poi votato il nuovo direttivo, riconfermando Raoul Chiesa, Raffaella D'Alessandro, Mariangela Fagnani, Giorgio Giudice, Paolo Giudice, Tommaso Mansutti, Massimiliano Manzetti, Roberto Mircoli, Gigi Tagliapietra, Claudio Telmon ed eleggendo per la prima volta Luca Marzegalli, Elio Molteni, Mattia Monga, Andrea Monti e Andrea Pasquinucci.

Tra i componenti del direttivo, l'assemblea ha eletto Gigi Tagliapietra, nuovo presidente del Clusit. Tagliapietra è da diversi anni nel Comitato Direttivo dell'Associazione. Si è occupato in modo particolare di tutela dei minori su Internet con il progetto Fata Turchina ed ha sostenuto il progetto e-Aware realizzato con l'Unione Europea. "Ho intenzione di continuare tutto ciò che di positivo è stato sin qui fatto e spero di contribuire con la mia ventennale esperienza personale di innovazione e gestione dell'Information Security" ha dichiarato Tagliapietra. "Continueremo il lavoro intrapreso con le associazioni di categoria e con gli organismi istituzionali per dare al Clusit maggior visibilità e peso politico. Continueremo a crescere in numero di soci e il mio operato, sostenuto dal direttivo, sarà nella direzione di coinvolgere ancora di più gli utenti. Ritengo anche che la costruzione di contenuti tecnici di qualità, come si è fatto con i convegni, i corsi, le certificazioni e i quaderni monografici, sia la strada maestra per generare valore per i soci e per il mercato."

2. Internet e Minori, Internet e Valori - Quali strategie per la sicurezza della Rete

Lo scorso 13 dicembre si è tenuto a Roma, nell'Aula Magna del Ministero delle Comunicazioni, il convegno "Internet e Minori, Internet e Valori - Quali strategie per la sicurezza della Rete?". Sono intervenuti, oltre all'On. Maurizio Gasparri, Ministro delle Comunicazioni ed a Danilo Bruschi, Presidente Comitato di Garanzia Internet e Minori:

Antonio Marziale, Presidente Osservatorio sui Diritti dei Minori

Marco Scarpati, Presidente ECPAT Italia

Roberta Bruzzone, Vice-presidente ICAA

Raffaele Corazzi, Stop-it, Save the Children

Donata Lodi, Direttore relazioni esterne Unicef
Ernesto Caffo, Presidente Telefono Azzurro
Gian Luca Petrillo, Consigliere per Internet del Ministro delle Comunicazioni
Salvatore Sica, Prof. Ordinario di Diritto Privato Comparato Università di Salerno
Michele Crudele, Direttore Associazione Centro ELIS Roma
Mons. Piero Monni, Osservatore permanente della Santa Sede presso l'O.M.T. (Nazioni Unite)
Alessandro Musumeci, Dir. Gen. del Servizio per l'Automazione Informatica e l'Innovazione Tecnologica, Miur
Domenico Vulpiani, Direttore del Servizio Polizia Postale e delle Comunicazioni
Paolo Vigevano, Consigliere del Ministro per l'Innovazione e le Tecnologie
Maria Burani Procaccini, Presidente Commissione Bicamerale Infanzia.

Gli abstract degli interventi sono disponibili su

<http://www.comunicazioni.it/it/DocSupp/920/Convegno%2013%20Dicembre%202004-1.zip>

<http://www.comunicazioni.it/it/DocSupp/920/Convegno%2013%20Dicembre%202004-2.zip>

3. COMPUTER CRIME

Cyber Crime - Nuovo sistema di attacco.

Un nuovo sistema è stato messo in pratica: un attacco alle abitazioni, ai giochi dei ragazzi, creando un nuovo cavallo di Troia.

Infatti, attraverso un dispositivo non protetto, inserito in LAN (quale ad esempio, una Playstation o una Xbox) un hacker può diffondere dei programmi ad hoc per catturare utili informazioni dalla rete. Se poi un utente si collega alla rete aziendale dal pc di casa, l'ignoto hacker può entrare anche lui nella rete dell'azienda. Vediamo l'antefatto.

Tutto è iniziato con un disco "demo" di un nuovo gioco per la Playstation Sony: chi ha installato il programma, ha subito la cancellazione della memoria. Da questo episodio, che ha avuto solo degli ignari giocatori quali vittime, il passo, per azioni più mirate da parte di bande criminali, è assai breve.

Teniamo a mente che, quando si tratta di giochi, non c'è la stessa accortezza che si ha con un personal computer dove vi sono dati personali o aziendali.

Per maggiori informazioni sull'episodio citato, consultare la pagina:

<http://www.eweek.com/article2/0,1759,1735655,00.asp>

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

4. Dalla Newsletter del MIT

Nell'ambito del programma di studio sulla criminalità informatica, l'EURIM (European Information Society Group) e l'IPPR (Institute for Public Policy Research) hanno diffuso i dati di due nuovi studi: "Reducing Opportunities for E-Crime" e "The Reporting of Cybercrime". In sostanza i due documenti evidenziano da una parte la necessità di una collaborazione più efficace tra il mondo dell'industria e quello legislativo al fine di produrre un codice di comportamento e di tutela ad uso degli utenti e dall'altra l'esigenza di razionalizzare l'estrema varietà di organismi e strumenti preposti al monitoraggio del fenomeno e-crime.

Approfondimento:

http://rogerdarlington.co.uk/commswatch/permalink.php?id=1064_0_2_0

(Tratto dalla newsletter n.88 del Ministero per l'Innovazione e le tecnologie)

5. DOCUMENTO CLUSIF: "La Riforma di BASILEA 2 - Una presentazione generale"

I colleghi del CLUSIF hanno pubblicato un documento che traccia una panoramica generale sulle novità introdotte dalla riforma di Basilea 2.

Il gruppo di lavoro che ha elaborato il documento, ha analizzato i rischi connessi alla sicurezza ICT nell'ambito dei "Rischi Operativi" che devono essere presi in considerazione dalle banche e dalle aziende di intermediazione finanziaria in generale. Il documento, che è rivolto principalmente ai security manager del settore finanziario, è una sintesi semplificata, che aiuta ad individuare gli impatti della riforma di Basilea 2 e le responsabilità che ne derivano. Lo scopo è anche quello di aiutare la raccolta delle informazioni necessarie per il calcolo dei fondi di riserva delle banche.

Il documento offre comunque interessanti spunti di riflessione sull'importanza di una corretta presa in considerazione del Rischio Operativo anche da parte delle aziende degli altri settori.

Il documento è per ora disponibile solo in francese

<https://www.clusif.asso.fr/fr/production/ouvrages/pdf/ReformeBale2.pdf>

Stiamo ipotizzando una traduzione in italiano.

6. MASTER

Prende il via la 4a edizione del Master Universitario di I livello in Sicurezza delle Tecnologie dell'Informazione e della Comunicazione. Il master, che si svolgerà a Milano e avrà inizio il 31 gennaio 2005, è organizzato dal Dipartimento di Informatica e Comunicazione dell'Università degli Studi di Milano in partnership con il CEFRIEL, Centro di Eccellenza Ict del Politecnico di Milano e con il patrocinio di CLUSIT.

Dedicato a tutti coloro che sono in possesso di un diploma universitario, una laurea breve o una laurea in Informatica, Scienze dell'Informazione, Ingegneria, Matematica e Fisica, il master affronterà le tematiche di maggior interesse per la figura dell'Information Security Specialist, tra cui le tematiche di base tecniche, organizzative e legali. Obiettivo del programma di studi è, infatti, formare figure professionali che possiedano una buona conoscenza delle problematiche legate alla sicurezza delle reti telematiche e dei sistemi informativi, conoscano le metodologie più usate per progettare e realizzare sistemi informatici sicuri e abbiano sviluppato conoscenza e capacità di valutazione critica delle più diffuse soluzioni tecnologiche per la sicurezza informatica disponibili sul mercato.

Il master si articola in una parte didattica, in aula e in laboratorio, per un totale di 500 ore e un tirocinio formativo di 300 ore da effettuarsi presso aziende e organizzazioni esterne. 25 è il numero massimo di posti disponibili. Per l'ammissione al corso, è previsto un colloquio individuale volto a valutare competenze e motivazioni del candidato. Le prove di selezione si terranno nei giorni 13 e 14 gennaio 2005 alle ore 9.30, presso il CEFRIEL.

Il contributo d'iscrizione è pari € 6.000,00 + Iva. Sono, inoltre, previste borse di studio a copertura parziale della quota ed è possibile anche accedere a finanziamenti agevolati presso gli Istituti di credito convenzionati.

Per ulteriori informazioni: Dott.ssa Roberta Letorio - Via Fucini n. 2, 20133 Milano tel 02.23954253 fax 02. 23954254 e-mail: roberta.letorio@cefriel.it

Visto il gradimento ed il successo riscosso e le numerose domande di iscrizione pervenute, il Dipartimento di Informatica dell'Università di Roma "La Sapienza" ha istituito la II Edizione del Master di I livello in "Sicurezza dei Sistemi e delle Reti informatiche per l'impresa e la Pubblica Amministrazione" (scadenza presentazione domande: 21 febbraio 2005). Il corso è rivolto soprattutto a coloro che già operano nel settore informatico, presso aziende private o la Pubblica Amministrazione ed intendono completare e potenziare la loro formazione, senza interrompere la propria attività lavorativa e si svolge prevalentemente nei giorni di venerdì e sabato. Il Master è aperto, previa selezione, a tutti i possessori di una Laurea (almeno di primo livello) in Informatica, Fisica, Ingegneria, Matematica, Statistica, nonché i possessori di una Laurea in altre discipline, che abbiano una comprovata esperienza lavorativa pluriennale nel campo dell'informatica.

Per ulteriori informazioni: <http://security.di.uniroma1.it/master/>

E-mail: mastersicurezza@di.uniroma1.it

7. SEMINARI CLUSIT DI GENNAIO

**SEMINARIO CLUSIT Reti WiFi
ROMA 18 gennaio 2005**

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 gratuita*

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 legati all'uso una rete WiFi

Accesso ed utilizzo illegale della rete aziendale
Fuga ed intercettazione di informazioni 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 architettureali:
Ridondanza degli elementi
802.1x Metodi a confronto (Sicurezza versus complessità)
Alternative all'802.1x: metodi a confronto:
Cifatura (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 Cifatura 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: Centro di formazione Percorsi Srl - Viale Manzoni 22

**SEMINARIO CLUSIT Tecniche biometriche
MILANO 25 gennaio 2005**

Sono aperte le iscrizioni.

Il modulo per registrarsi: www.clusit.it/edu/reg_sem_form_2004.pdf

Per i Soci Clusit la partecipazione è gratuita*

PROGRAMMA

1- Introduzione ai sistemi biometrici

Definizioni, modalità di riconoscimento, tipologie di applicazioni, misura delle prestazioni
Panorama delle caratteristiche biometriche, parametri di valutazione
Tecnologie biometriche (con particolare riferimento a volto e impronta digitale)

2- Progettare un sistema biometrico

Studio di fattibilità e pianificazione
Aspetti tecnologici
Aspetti organizzativi
Sistemi biometrici e privacy

3- Valutazione delle prestazioni di un sistema biometrico

Come eseguire la valutazione
Valutazione di algoritmi per il riconoscimento di impronte digitali
Valutazione di algoritmi per il riconoscimento del volto

4- Sistemi biometrici basati su impronte digitali: aspetti implementativi

Perché le impronte digitali
Caratteristiche dei lettori di impronte, prestazioni
Enroll: caratteristiche dei template, criticità, soglia di riconoscimento
Riconoscimento: gestione del dispositivo, utenti problematici, verifica e identificazione

5- Applicazioni

Sicurezza logica: logon a sistemi, accesso a risorse critiche, esempi
Scanner stand alone: firma digitale
Cenni sulla sicurezza fisica
Considerazioni sulla privacy

6- Impronte e SmartCard

Gli standard, i vantaggi e i limiti
Match on card

7- Sistemi di sviluppo

Un esempio: FX3 SDK

Agenda:

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

Docenti: Raffaele Cappelli, Andrea Patrignani

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

8. 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"
