

Indice

1. **NUOVI SOCI**
2. **NUOVO RINVIO PER LA PRIVACY**
3. **TECNOLOGIE BIOMETRICHE E PUBBLICA AMMINISTRAZIONE**
4. **HOMELAND SECURITY**
5. **INFOSECURITY 2005: LE CONFERENZE**
6. **RETURN ON SECURITY INVESTEMENT**
7. **MEGATREND, RISCHI E SICUREZZA**
8. **SEMINARI CLUSIT DI NOVEMBRE**
9. **EVENTI SICUREZZA**

1. NUOVI SOCI

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

- ACTALIS (Milano),
- MG Engineering (Cinisello Balsamo),
- Nicole International (Roma).

2. NUOVO RINVIO PER LA PRIVACY

Nonostante la notizia non sia ancora stata ufficializzata, fonti ben informate ci confermano che venerdì scorso sarebbe stato approvato il decreto legge che proroga al 30 giugno 2005 il termine utile per presentare il Documento Programmatico sulla Sicurezza e per adottare le misure minime di sicurezza previste dal dlgs 196/2003.

3. TECNOLOGIE BIOMETRICHE E PUBBLICA AMMINISTRAZIONE

Il CNIPA (Comitato Nazionale per l'Informatica nella Pubblica Amministrazione) ha pubblicato on line le "Linee guida per le tecnologie biometriche". Il documento fornisce alle P.A. una panoramica sulle tecnologie attualmente disponibili e sulle loro applicazioni. Il documento è disponibile sul sito del CNIPA (<http://www.cnipa.gov.it/site/files/Linee%20guida%20tecnologie%20biometriche.pdf>).

4. HOMELAND SECURITY

Nei giorni 7 e 8 ottobre il CLUSIT ha partecipato a Ginevra ad un Forum che ha riunito 200 delegati in rappresentanza di 37 paesi.

Il Forum ha permesso di paragonare le diverse strategie adottate in materia di "Homeland Security" da Stati Uniti, Europa e resto del Mondo. È risultato evidente che l'approccio al problema è molto diverso, diversa la volontà politica e sicuramente diverso l'impegno economico. Nonostante queste differenze, sembra indispensabile giungere ad una convergenza delle strategie di Stati Uniti ed Europa. In questo processo di convergenza sarà indispensabile il coinvolgimento e la collaborazione internazionale del settore privato.

Il mercato mondiale della protezione contro il terrorismo è valutato in 100 miliardi di euro, quello della sicurezza ICT 50 miliardi di euro. Negli USA il dipartimento dell'Homeland Security, creato nel 2003, raggruppa 22 agenzie federali e 180.000 dipendenti, con un budget per il 2005 che supererà i 40 miliardi di dollari, di cui 1,1 dedicato alla ricerca, che vedrà coinvolti laboratori, università e imprese private. Secondo diversi esperti, il mercato della sicurezza, nonostante questo notevole impulso, non sarà completamente operativo prima di 7/8 anni. Probabilmente l'evoluzione imposta dagli americani porterà ad una "privatizzazione" della guerra al terrorismo ed aumenterà ulteriormente il dislivello tecnologico tra Stati Uniti ed Europa.

Per quanto riguarda la Sicurezza ICT, una strategia globale a livello mondiale è sicuramente indispensabile. Indipendentemente dalle tecnologie, come affermato anche da John Thompson (membro dell'US National Infrastructure Advisory Committee [NIAC], consigliere della Casa Bianca e Chairman e CEO di Symantec Corporation), le priorità a livello mondiale, per la lotta al cybercrime ed al cyberterrorismo saranno:

- 1) attività di Information Sharing
- 2) iniziative di Awareness
- 3) armonizzazione di leggi, norme e regolamenti nazionali, per permetterne l'applicazione a livello internazionale.

5. INFOSECURITY 2005: LE CONFERENZE

Sono state definite le principali tematiche che saranno trattate durante le conferenze di Infosecurity 2005.

LA SICUREZZA NEL MONDO BANCARIO

In questo convegno si cercheranno di descrivere le iniziative più significative intraprese o in corso d'opera, da parte del mondo bancario per proteggersi dall'insicurezza delle tecnologie dell'informazione e della comunicazione, tenendo particolarmente presente che Basilea 2 è sempre più presente e sempre meno futuro. Non si perderà quindi l'occasione per parlare di business continuity e disaster recovery, ma anche di nuove soluzioni sicure per l'home banking, e del passaggio dalla banda magnetica al microcircuito.

INFOSECURITY INCONTRA ENISA

Uno delle principali novità che ha caratterizzato il settore della sicurezza informatica lo scorso anno è stata sicuramente la creazione da parte della Commissione Europea, dell'Agenzia Europea per la Sicurezza Informatica. Infosecurity sarà occasione per un primo momento di incontro tra la comunità della sicurezza informatica italiana ed i rappresentanti dell'agenzia europea. Nell'ambito di questa tavola rotonda quindi si alterneranno i principali attori dell'agenzia europea che si confronteranno con tutti gli intervenuti all'evento, sulle principali iniziative che l'agenzia promuoverà a partire da quest'anno sul territorio europeo e nazionale.

LA SICUREZZA NELLE PMI

Solo negli ultimi anni la piccola e media impresa si è affacciata al mondo della sicurezza, che subito ha rivolto a questa importante componente del sistema produttivo nazionale una notevole attenzione. Questo convegno è mirato a descrivere, attraverso interventi di significativi rappresentanti del mondo della piccola e media impresa italiana da una parte e di fornitori di soluzioni dall'altra, lo stato della domanda e dell'offerta nel settore della sicurezza informatica per le PMI.

LA TUTELA DEI DIRITTI D'AUTORE IN RETE

Si tratta di uno dei temi principalmente discussi a livello internazionale, ma anche nel nostro paese dove recentemente è stata introdotta una legge per regolamentare il tema della tutela dei diritti d'autore in rete. Il tema ha risvolti sia tecnologici che giuridici. Nell'ambito di questo convegno, ci si concentrerà su questi ultimi, mettendo a confronto alcuni dei principali attori che hanno animato, la primavera scorsa, il dibattito sulla legge Urbani nel nostro paese, accompagnati da testimonianze internazionali, a sostegno delle diverse tesi.

LE CERTIFICAZIONI DI SICUREZZA

Da poco meno di un anno operano nel nostro paese gli organismi per certificare da una parte prodotti e dall'altra processi, legati alla sicurezza ICT. Nonostante i due percorsi di certificazione e le certificazioni in sé siano estremamente diverse, c'è ancora molta confusione sul tema e molto spesso ci si chiede: Quali sono le differenze tra questi vari enti? Qual è la differenza tra la certificazione di un prodotto e di un processo? Come si ottiene una certificazione? Chi è preposto a controllare i processi di certificazione? Queste sono alcune delle domande a cui i relatori di questo convegno cercheranno di dare una risposta esauriente.

6. RETURN ON SECURITY INVESTEMENT

I colleghi del CLUSIF hanno pubblicato un documento che intende dimostrare il valore aggiunto degli investimenti in sicurezza informatica. Il gruppo di lavoro che ha elaborato il documento, ha cercato di formalizzare alcune considerazioni di base che permettano di giustificare il valore della sicurezza IT ed il suo importante contributo al corretto funzionamento delle attività aziendali. Non vengono fornite formule per il calcolo del ROSI, ma si evidenziano argomentazioni utili per tutti coloro che desiderano dimostrare la necessità di investimenti in sicurezza informatica in fase di definizione di budget.

Il documento è per ora disponibile solo in francese
(<https://www.clusif.asso.fr/fr/production/ouvrages/pdf/RoSI.pdf>).

7. MEGATREND, RISCHI E SICUREZZA

Segnaliamo un libro interessante, scritto dal Prof. Augusto Leggio, uno dei nostri soci fondatori:

"MEGATREND, RISCHI E SICUREZZA:

Per comprendere il mondo di oggi con la Teoria del Caos."

Il libro è edito da Franco Angeli Editore e sarà nelle librerie nel corso del mese di novembre.

Di fronte al profluvio di notizie politiche, economiche e sociali che i mezzi di comunicazione di massa riversano su di noi, l'autore propone di integrare la comprensione dei fatti con un approccio scientifico innovativo, derivato dall'osservazione di quanto accade naturalmente in fisica, chimica e biologia, noto agli addetti ai lavori come "Teoria del caos" o Teoria della complessità".

Lo studio dell'interconnessione tra i macrofenomeni tendenziali e dei relativi rischi (esaurimento delle risorse naturali, degrado dell'ambiente, globalizzazione, corruzione, criminalità organizzata, terrorismo, ecc.), porta l'autore a denunciare comportamenti erronei, derivanti da ideologie, interessi e ignoranza, che possono condurre l'umanità ad una instabilità e insicurezza crescenti e ad una iniqua e pericolosa esasperazione delle disuguaglianze.

Egli indica una via stretta, che può consentire l'attenuazione delle minacce incombenti e lo sviluppo di un futuro più sicuro, sereno ed equo. Su questa via, una pietra miliare è costituita dal ruolo autonomo, degno dei suoi valori e della sua storia, dell'Unione Europea, più responsabilizzata dalla recente approvazione della Carta costituzionale, e sostenitrice di un modello sociale dove capitalismo e solidarietà possono trovare un naturale punto di equilibrio.

Un libro nuovo, diverso, che arricchisce e fa riflettere sulla responsabilità di ciascuno nel costruire nel modo migliore l'avvenire di tutti coloro che ci seguiranno.

Augusto Leggio, socio fondatore CLUSIT, ha contribuito all'innovazione di alcune delle maggiori infrastrutture critiche del nostro paese, quali Banca d'Italia, Telecom Italia e Poste Italiane. Per conto del governo, ha diretto il Comitato 2000, creato per gestire i rischi legati al passaggio dal 1999 al 2000. È consulente per il controllo strategico di grandi amministrazioni e autore di testi sull'ICT e sul ruolo che questa ha assunto nel mondo moderno. Il suo indirizzo di posta elettronica è: augusto.leggio@email.it

8. SEMINARI DI NOVEMBRE

**SEMINARIO CLUSIT Documento Elettronico
ROMA 16 novembre 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 gratuita*

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: Centro di formazione Percorsi Srl - Viale Manzoni 22

**SEMINARIO CLUSIT Crittografia Quantistica
MILANO 23 novembre 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 gratuita*

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: 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)

8-12 novembre 2004, Milano
Mastercourse Security Manager

15 novembre 2004, Milano
"Nuove tecnologie: regole e mercato"

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

18 novembre 2004, Fiera di Milano
Convegno Assintel a "Sicurezza 2004"

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"

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

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

© 2004 Clusit - Vietata la riproduzione

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