

## Indice

1. NUOVI SOCI
2. NOTE DA BRUXELLES
3. VITTORIA AL "CAPTURE THE FLAG"
4. PRIMA CONFERENZA NAZIONALE SERVIZI INNOVATIVI E TECNOLOGICI

### 1. NUOVI SOCI

Hanno aderito al Clusit:

- Ansaldo Segnalamento Ferroviario (Genova)
- K2Compliance (Pomezia - RM)
- Seven One Solution (ROMA)

### 2. NOTE DA BRUXELLES

Il 7 dicembre scorso si è tenuto a Bruxelles un seminario organizzato dalla Direzione Generale Information Society and Media della Commissione Europea dal titolo ***Raising security awareness and strengthening the trust of end-users in information society: policy challenges for the next decade*** a cui erano invitati, oltre ai rappresentanti dei governi dei paesi membri, esponenti del mondo accademico ed esperti di sicurezza a vari livelli.

Il **CLUSIT** era presente, nella persona del suo presidente, Gigi Tagliapietra, sia come organizzazione focalizzata alla sicurezza che come rappresentante del Dipartimento per l'innovazione e le tecnologie della Presidenza del Consiglio dei Ministri.

L'obiettivo dichiarato del seminario era quello di fornire indicazioni alla Commissione su quali passi compiere, all'interno dell'iniziativa i2010, per costruire una società dell'informazione che sia anche sicura.

Il seminario era diviso in tre sessioni di brainstorming

- **Tecnologia:** quali impatti ci si devono aspettare dalle nuove tecnologie rispetto alla privacy e alla fiducia degli utenti sia business che privati.
- **Dipendenza:** come le reti, intese come insieme di oggetti e servizi, siano sempre più determinanti per la vita sociale e come garantirne la continuità
- **Percezione:** quali fattori psicologici influiscono sulla fiducia, come trasformare la consapevolezza in fiducia, come misurare la fiducia e come bilanciare responsabilità e legalità.

Già nel titolo si colgono due aspetti importanti: l'attenzione si sposta sempre più dal tema "sicurezza" (che sottintende tecnologia) a quello della "fiducia" (che implica fattori emotivi e psicologici) e l'orizzonte

temporale deve essere quello di medio-lungo periodo, dieci anni, perchè le politiche di breve termine non possono sperare di fronteggiare le sfide che abbiamo di fronte a noi.

### **Lo scenario**

Le presentazioni di apertura del dr. Andrea Servida, responsabile dell'unità A3 della DG Information Society, e del prof. Michel Riguidel dell'Ecole Nationale Supérieure des Télécommunications di Parigi, hanno dipinto uno scenario contraddittorio.

Un livello ancora insufficiente di consapevolezza dei rischi e la conseguente limitata protezione dei sistemi (secondo un'indagine Eurostat solo il 30% degli utenti protegge i propri sistemi) a fronte di una crescente complessità e fragilità dell'infrastruttura: "Dobbiamo vedere i sistemi come 'inestricabili' e non più come sistemi 'complessi'" (Riguidel).

A fronte di una esigenza a breve di recuperare il ritardo accumulato è importante guardare al futuro con un'ottica completamente diversa rispetto al passato che faccia superare la dicotomia macchina-rete verso una visione molto più dinamica e olistica dei sistemi e delle relazioni che si instaurano tra i partecipanti.

La sicurezza del futuro sarà non un sistema monolitico ma la negoziazione di una serie di informazioni tra due entità (il singolo e l'ente o azienda) che vogliono dialogare, in cui la fiducia non sarà affidata integralmente a sistemi tecnologici ma anche a reti di referenza e trust reciproco di micro-comunità.

In più non dovremo pensare solamente alla sicurezza ma alla "sovranità" e alla "dignità" digitale come temi centrali per la costruzione di una società dell'informazione in cui i cittadini possano riconoscersi.

Tra le sfide più serie vi è quella della comprensione dei tempi diversi dei diversi fattori in gioco (la vita media di un sistema di sicurezza era stimato in 10 anni mentre le generazioni di attacchi mutano ogni 3) e il fatto che la distinzione tra mondo reale e virtuale si assottiglia sempre più e dovremo aspettarci nei prossimi 5 anni virus e malware che causeranno la morte di persone (si pensi a un pacemaker connesso alla rete sanitaria per monitoraggio che viene messo fuori uso da un virus).

Di certo la tecnologia pone quesiti importanti e non solo perchè parliamo di RFID ma perchè dovremo pensare a come securizzare il nanomondo e gli oggetti infinitamente piccoli o come securizzare i futuri computer quantici che non sono "digitali".

Dovremo infine accettare il fatto che non tutto sarà controllabile e sicuro e che "infosfere", di cui noi non avremo e non potremo avere il controllo, appartengono al nostro futuro.

### **Il dibattito**

Dalla discussione sono emersi spunti molto interessanti.

Janne Uusilehto, responsabile product security di NOKIA, ha fatto notare come nel 2015 si prevede siano 5 miliardi le persone "always connected" e un livello di traffico moltiplicato per 100 volte rispetto a quello attuale e ha ricordato che "La tecnologia non protegge le persone ma offre strumenti alle persone che vogliono proteggersi".

Ha sottolineato inoltre che se è vero che il grande tema è quello della alfabetizzazione di massa dei cittadini e degli utenti, non bisogna

dimenticare che occorre preparare e formare in modo preciso anche tutta una nuova generazione di tecnici, che oggi non sono in grado di sviluppare software sicuri fin dall'inizio.

Gerald Spindler dell' Università di Gottingen ha ricordato che servono norme che introducano "minimum security standards" (oggi presenti solo per i prodotti medicali) e che la direttiva europea sulla responsabilità di prodotto non include il software come "prodotto". Gli ha fatto eco Kornelia Kutterer della European Consumer Association condividendo l'idea delle regole minime di sicurezza ma ha sottolineato che bisogna anche definire chi garantisce l'imposizione e il rispetto di queste norme e per di più la Commissione Europea dovrebbe essere molto più precisa quando usa termini come pirateria, sicurezza, cybercrimine che oggi assimilano gli utenti ai terroristi.

### **Il tema della fiducia**

Angela Sasse Professor of Human-Centered Technologies all' University College di Londra ha sviluppato il tema della "fiducia" che era il punto chiave del seminario.

Ne ha dato innanzitutto una definizione: Fiducia come volontà di essere vulnerabile basandosi su positive aspettative sulle azioni degli altri.

La fiducia è cognitiva (razionale) o immediata (pre-cognitiva) ad esempio con i familiari e si sviluppa nella lettura di segnali che spesso mancano nel mondo virtuale e rappresenta una scorciatoia per un approccio analitico alla valutazione costi-rischi-benefici.

Dopo le prime interazioni in un ambiente di fiducia, l'utente trasforma la fiducia in affidabilità e abbassa la percezione della vulnerabilità (vedi il phishing), non si tratta quindi di manipolare la richiesta di fiducia (mettere un viso sorridente sulla pagina web) ma di aiutare gli utenti a comportamenti positivi in cui "La tecnologia consente agli utenti di prendere la giusta decisione in termini di fiducia".

L'interazione deve dare incentivi che premiano comportamenti corretti e fornire segnali che gli utenti possono leggere: servono SINTOMI (es. prodotti di relazione fiduciaria) e non semplicemente SIMBOLI.

Compito delle istituzioni è quindi anche quello di ridurre le situazioni di "incertezza" e un possibile percorso da seguire è quello di sostenere comunità di utenti che costruiscono legami di fiducia e che poi si autoregolano.

Su questo tema è intervenuta Albena Spasova, responsabile dell' ufficio legale di eBay, per la quale il 100% del business di eBay dipende dalla fiducia: se un utente ha una esperienza negativa non torna più. La risposta è una iniziativa decisa e costante che si basa certo sulla tecnologia, ma soprattutto sulla completa trasparenza con gli utenti, informazioni continue e accurate, un servizio h24 per rispondere alle potenziali frodi, un software gratuito che garantisce l'autenticità del sito eBay. In sostanza non UNA risposta ma un insieme di azioni coordinate e focalizzate.

### **Due commenti degni di nota:**

"Un mondo con l'identificazione univoca di singoli oggetti e persone è estremamente pericoloso, dobbiamo pensare a forme di proxy che

mettano delle generalizzazioni tra noi e la rete garantendo la protezione dell'identità e nel contempo la partecipazione responsabile." (Riguidel)

"Dobbiamo sviluppare forme di ragionamento non lineare: le cinture di sicurezza riducono gli incidenti? No, riducono i morti, è vero, li dimezzano. Ma il numero totale dei morti in Inghilterra non è diminuito perchè sono aumentati gli incidenti, anche perchè, siccome la gente si sente più sicura, viaggia più veloce e corre maggiori rischi." (Sasse)

### **Come misurare la fiducia**

Già dal prossimo anno la Commissione Europea collaborerà con Eurostat per sviluppare sistemi che misurino il livello di fiducia degli utenti nei sistemi informativi, per poter valutare in termini concreti l'efficacia delle iniziative che vengono messe in campo.

E' un terreno difficile, come ha sottolineato Tobias Husing, ricercatore di Empirica, una società Tedesca che ha già collaborato con la DG su questo tema, perchè nelle indagini sulla sicurezza per gli utenti finali, la gran parte degli intervistati non è nemmeno in grado di capire la domanda.

Innovativo non è solo il terreno d'indagine ma devono essere innovati anche gli strumenti di misura e devono venire correlati indicatori anche marginali ma che possano aiutare a capire se il cambiamento di fiducia induce cambiamenti nei comportamenti. Qualunque analisi statistica classica non funziona per misurare la fiducia: serve un "benchmarking analitico" che analizzi in dettaglio anche micro-indicatori.

### **Due punti di vista significativi**

Sono stati presentati nel dibattito finale due punti di vista significativi da parte di istituzioni governative.

Ferenc Suba, Presidente del PTA, una emanazione del CERT ungherese, che ha scelto la via della costruzione di una fondazione di tipo privatistico che garantisce rapidità ed efficienza nell'azione quotidiana mantenendo il ruolo governativo di guida e orientamento ma evitando la farraginosità tipica delle pubbliche amministrazioni.

Il rappresentante del Governo Greco (Ministero delle Finanze) ha sostenuto che non si tratta di costituire nuove authorities ma di far interagire i player attuali (providers, operatori di telecomunicazioni, associazioni) e di unificarne i linguaggi e gli sforzi coordinandone le iniziative, favorendo l'interscambio di esperienze e la condivisione delle best practices.

Un richiamo alla collaborazione tra attori, istituzioni e paesi come chiave per la soluzione alle sfide della sicurezza del prossimo decennio.

## **3. VITTORIA AL "CAPTURE THE FLAG"**

Sono i **Chocolate Makers** dell'Università degli Studi di Milano i vincitori dell'edizione 2007 del torneo internazionale a squadre "Capture the Flag" organizzato dall'Università di Santa Barbara, in California.

"Una grande soddisfazione per una piccola squadra come la nostra che nel 2005 aveva già vinto una competizione analoga, anche se minore,

promossa dall'Università di Aachen, in Germania" - dice Roberto Paleari, uno degli 8 membri dei **Chocolate** che hanno sfidato gli altri 34 team provenienti in massima parte da Stati Uniti e Germania ma anche da Russia, India, Austria e Argentina. Settima classificata l'altra squadra italiana: "TheTower of Hanoi" del Politecnico di Milano, che aveva invece vinto l'edizione 2004.

La gara di sicurezza informatica, nata nel 2003, vede la partecipazione internazionale di squadre di studenti che si affrontano difendendo l'integrità e il funzionamento di un dato

numero di servizi in rete, su piattaforma Linux o Windows, mentre cercano di sabotare quelli degli avversari. "Una sorta di versione virtuale di *bandiera* - spiega Paleari - dove le bandierine si conquistano individuando e riparando la vulnerabilità di file che dovrebbero invece risultare inaccessibili".

A garanzia di un comportamento etico, ogni anno sono ammesse a partecipare alla competizione solo le squadre che fanno capo a un'istituzione scolastica.

Per saperne di più: [www.cs.ucsb.edu/~vigna/CTF/](http://www.cs.ucsb.edu/~vigna/CTF/)

#### **4 . PRIMA CONFERENZA NAZIONALE SERVIZI INNOVATIVI E TECNOLOGICI**

I Servizi innovativi insieme alle Tecnologie dell'informazione e della comunicazione consentono di raggiungere obiettivi irrinunciabili dal punto di vista sia dell'efficacia che dell'efficienza, ottimizzando la performance di imprese e Pubbliche amministrazioni.

Nello sviluppo dell'Economia dei Servizi innovativi il nostro Paese segna un ritardo a causa di diversi fattori che ci impediscono di crescere ed essere competitivi al pari dei nostri partner europei.

L'innovazione è un sistema complesso, perché i soggetti coinvolti sono molteplici e gli strumenti per diffonderla innumerevoli.

L'innovazione è valore, perché costituisce la chiave per la crescita stessa della società, e questo crea sviluppo.

L'economia dell'innovazione trova nell'iniziativa imprenditoriale, nelle tecnologie e nei Servizi innovativi i fattori propulsivi, essenziali per imprimere al nostro sistema produttivo la necessaria accelerazione nella sfida globale.

Per riflettere sul ruolo dei Servizi innovativi e tecnologici come volano di crescita per l'economia del Paese e per dare visibilità alle dimensioni del settore, Confindustria Servizi Innovativi e Tecnologici organizza la "1a Conferenza Nazionale dei Servizi Innovativi e Tecnologici" che sarà occasione per discutere di modelli e strumenti per la crescita e di come "rimettere in corsa" il nostro Paese.

La Conferenza si terrà il 4 febbraio 2008, a Milano, presso l'Auditorium di Assolombarda, con inizio lavori alle ore 9 e conclusioni alle ore 14 circa.

Interverranno a questo importante appuntamento autorità ed esperti. Tra i contributi già confermati, il saluto di apertura del Presidente Assolombarda, Diana Bracco e le relazioni di Nando Pagnoncelli e Antonio Catricalà che introdurranno la sessione dedicata agli interventi dei Presidenti delle principali Rappresentanze dei Servizi di Confindustria.

Seguiranno la relazione del Presidente di Confindustria Servizi Innovativi e Tecnologici, Alberto Tripi, e l'intervento del Presidente di Confindustria, Luca Cordero di Montezemolo.

Il Ministro dello Sviluppo Economico, Pier Luigi Bersani, chiuderà i lavori.

La partecipazione alla Conferenza è gratuita, ma è obbligatoria l'iscrizione che potrà essere effettuata, a partire dal 10 gennaio tramite il sito [www.conferenzanazionalesestivi.org](http://www.conferenzanazionalesestivi.org) nel quale saranno pubblicati anche aggiornamenti sul programma, documentazione e ogni altra informazione utile.

Ai partecipanti alla Conferenza sarà consegnata copia del Primo Rapporto sui Servizi Innovativi in Italia.

---

**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

**© 2007 Clusit - Vietata la riproduzione**

Clausola di esclusione della responsabilità e informazioni relative al

Copyright: [www.clusit.it/disclaimer.htm](http://www.clusit.it/disclaimer.htm)