Indice

1. NUOVI SOCI

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

- COLT Telecom (Milano),
- NEXTREM (Mirandola - MO),
- PERCORSI (Roma

2. LA SICUREZZA INFORMATICA NELLA P.A.

Il Comitato Tecnico Nazionale sulla Sicurezza Informatica nella Pubblica Amministrazione, di cui fa parte il nostro Presidente (Prof. Danilo Bruschi), ha pubblicato le "Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione" (http://www.innovazione.gov.it/ita/intervento/normativa/allegati/proposte_sicurezza_marzo04.pdf). In particolare, nella seconda parte del documento, il Comitato indica le attività più urgenti da intraprendere.

3. CRITTOGRAFIA QUANTISTICA

EFFETTUATA LA PRIMA TRANSAZIONE FINANZIARIA TRAMITE LA CRITTOGRAFIA QUANTISTICA

Il 21 Aprile 2004 a Vienna è stata realizzata la prima transazione finanziaria in cui la sicurezza delle comunicazioni informatiche è stata garantita dalla Crittografia Quantistica (la Press Release è disponibile a http://www.quantenkryptographie.at/rathaus_press.html). Il gruppo del Professor Zeilinger dell'Università di Vienna e la Seibersdorf Research hanno progettato e realizzato il sistema di Crittografia Quantistica. La transazione finanziaria è stata effettuata dal Sindaco di Vienna tra il Municipio e la Bank Austria Creditanstalt.

La Crittografia Quantistica è una nuova tecnologia che permette di creare e scambiare chiavi segrete da utilizzare poi per cifrare le comunicazioni, pertanto un nome più appropriato è "Quantum Key Distribution". Per generare e trasmettere le chiavi segrete, la Crittografia Quantistica sfrutta alcune delle principali leggi della Meccanica Quantistica, la quale formula le leggi fondamentali delle particelle elementari.

I sistemi attuali di Crittografia Quantistica si basano sul codificare un bit informatico in una proprietà di un singolo fotone, che è il costituente fondamentale della luce e delle radiazioni elettromagnetiche. La Meccanica Quantistica garantisce che se un fotone è intercettato da un attaccante nel suo tragitto tra le due parti che stanno generando la chiave segreta, alcune delle sue proprietà vengono modificate e l'attacco viene perciò rilevato. In altre parole la Meccanica Quantistica garantisce l'individuazione di qualunque tentativo di attacco al processo di generazione e scambio della chiave.

La Crittografia Quantistica è quindi un'alternativa all'uso dei protocolli a Chiave Pubblica, quali ad esempio il famoso RSA, per generare e scambiare le chiavi segrete. La differenza principale tra i protocolli a Chiave Pubblica e la Crittografia Quantistica è che quest'ultima non teme attacchi basati sulla potenza di calcolo degli elaboratori o sugli sviluppi di tecniche matematiche che permettono già oggi di rompere sistemi a Chiave Pubblica che adottano chiavi pubbliche/private troppo corte.

D'altra parte, la Crittografia Quantistica richiede oggi l'uso di singoli fotoni, e non è facile creare e rilevare singoli fotoni con le tecnologie odierne anche se lo sviluppo in questo campo è molto rapido. Inoltre è necessario avere a disposizione un'unica fibra ottica, il che limita la distanza di applicazione, ad oggi il massimo raggiunto è 150 chilometri. Anche in questo caso le tecniche sono in rapido sviluppo, e si prevede che in qualche anno saranno disponibili altre implementazioni della Crittografia Quantistica, anche via satellite, con la possibilità di copertura dell'intero globo terrestre.

Anche se lo studio in Università e laboratori di ricerca di questa tecnologia ha ormai più di 20 anni, solo verso la fine del 2003 sono comparsi sul mercato i primi due prototipi commerciali da parte di "MagiQ Technologies" (New York) e "id Quantique" (Ginevra). Inoltre altre aziende, quali NEC, Toshiba e Hewlett-Packard, stanno sviluppando propri sistemi di Crittografia Quantistica che presto appariranno sul mercato.

La Crittografia Quantistica ha già catturato l'interesse di governi, di militari ed agenzie di sicurezza, e di banche e istituzioni finanziarie.

Ad esempio, Visa International, l'azienda internazionale di carte di credito, sta sperimentando questa tecnologia, ed altre banche e istituzioni finanziare hanno annunciato il loro interesse. Infine l'Unione Europea ha finanziato un enorme progetto, iniziato il 1 Aprile 2004, per lo sviluppo sia della ricerca che della implementazione tecnologica e commerciale della Crittografia Quantistica (la Press Release è disponibile sul sito http://www.quantenkryptographie.at/ e la descrizione del progetto sul sito http://www.arcs.ac.at/quanteninfo/).

Il progetto ha un budget di 11,4 Milioni di Euro in 4 anni, vi partecipano 41 partner in 12 paesi europei, e per l'italia vi sono l'Università di Pavia, il CNR, la Scuola Normale Superiore di Pisa ed il Politecnico di Milano.

(Autore: Andrea Pasquinucci, membro del Comitato Tecnico Scientifico del CLUSIT)

4. I SEMINARI CLUSIT

Il CLUSIT, per rispondere alle continue richieste di formazione in ICT Security che provengono dai Soci e per adempiere ad uno dei suoi principali obiettivi istituzionali, ha deciso di organizzare una serie di Seminari specialistici, programmati da giugno 2004 a maggio 2005, che si terranno con cadenza mensile sia a Roma che a Milano.

I Seminari CLUSIT sono rivolti a personale già introdotto nell'ICT Security e/o comunque coinvolto nelle procedure organizzative e o tecniche inerenti l'ICT Security, che vuole approfondire argomenti specifici di attualità o relativi a tecniche innovative.

I seminari avranno una durata di mezza giornata e si svolgeranno di pomeriggio. Saranno ammessi fino ad un massimo di 25/30 partecipanti per ogni seminario.

I seminari saranno tenuti da esperti del mondo Accademico e Professionisti del settore e permetteranno di ottenere Crediti di Formazione per il mantenimento di certificazioni quali CISSP, SSCP, CISA, CISM.

I soci CLUSIT avranno diritto ad un certo numero di seminari gratuiti e potranno partecipare ai successivi, con un costo estremamente ridotto.

I primi Seminari tratteranno di "Principi di Crittografia", "Voice-over-IP", "Il documento elettronico", "Crittografia Quantistica", "Wi-Fi", "RFID", "Sicurezza VLAN e LAN", "Tecniche biometriche", "DRM".

Il programma dettagliato dei seminari sarà a breve disponibile sul sito web dell'associazione.

5. CONVEGNO CLUSIT / ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI MILANO

L'ordine degli Ingegneri della provincia di Milano e il CLUSIT, in collaborazione con CEFRIEL, Cisco Systems e il Politecnico di Milano hanno organizzato la seconda edizione del seminario sulla sicurezza dei sistemi informativi ed aspetti legali, quest'anno intitolato "Tutelare l'azienda gestendo efficacemente la sicurezza informatica: dalle implicazioni tecniche alle responsabilità legali".

Il seminario previsto per il 4 giugno 2004 presso il Politecnico di Milano (aula S-01 - Piazza Leonardo da Vinci 32) si propone, anche attraverso lo studio di un caso concreto, di considerare gli aspetti tecnologici, gestionali, organizzativi e di conformità legale legati alla sicurezza dei sistemi informativi aziendali. L'agenda del seminario, è disponibile su http://www.clusit.it/eventi/ording_04_06_04.pdf.

La partecipazione è gratuita, previa registrazione.

6. LE AZIENDE BRITANNICHE E GLI ATTACCHI INFORMATICI

LONDRA (Reuters) - Il Dipartimento del Commercio e dell'Industria (DTI) ha indicato nel suo rapporto annuale che le maggiori imprese britanniche hanno subito attacchi da pirati, virus informatici ed altre forme di intrusione nelle proprie reti, col ritmo di un incidente alla settimana nel corso del 2003.

Il documento del DTI indica che più dei due terzi delle società inglesi hanno segnalato degli incidenti informatici nel corso dell'anno.

Lo studio del DTI sulle vulnerabilità di sicurezza informatica è stato pubblicato proprio quando un gruppo di legislatori stanno lavorando alla riforma dell'unica legge nazionale esistente in materia di cybercrime. Si tratta di una legge di quattordici anni fa, che molti giudicano ormai inadeguata per far fronte alla criminalità informatica dei nostri giorni.

La polizia inglese ha recentemente indicato che il cybercrime costa ogni anno alle aziende britanniche centinaia di milioni, forse di miliardi, di lire sterline.

Il DTI ritiene che le aziende sono in parte responsabili della situazione in quanto, benchè siano sempre più numerose le società che adottano delle politiche di sicurezza informatica, gli investimenti delle imprese in questo settore sono assolutamente sottodimensionati.

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

4 maggio 2004, Settimo Milanese
Seminario AIPSA sulla Sicurezza delle Reti

4 maggio 2--4, Roma
"Giornata di lavoro sullo spam", organizzata dall'Autorità Garante per la protezione dei dati personali con la collaborazione di Internet Society (Italy Chapter)

6 maggio 2004, Padova - Webbit
"Sicurezza ed etica nella tutela dei dati personali". SEMINARIO CLUSIT

8 maggio 2004, Monza (MI)
Esame di certificazione CISSP

12-14 maggio 2004, Roma
Internet/Intranet: TCP/IP Network Security

14 maggio 2004, Castellanza (VA) - Università Cattaneo - LIUC
"La sicurezza dei dati e la privacy in internet"

19-21 maggio 2004, Cortona
XVIII Convegno Nazionale di Information Systems Auditing, organizzato dall'AIEA

21 maggio 2004, Lecce
Il rischio "accettato"

24-28 maggio 2004, Milano
Mastercourse Security Manager

4 giugno 2004, Politecnico di Milano

"Tutelare l'azienda gestendo efficacemente la sicurezza informatica: dalle implicazioni tecniche alle responsabilità legali"

2° Seminario sulla sicurezza informatica, organizzato dall'Ordine degli Ingegneri della Provincia di Milano e da CLUSIT, in collaborazione con CEFRIEL, Cisco Systems e Politecnico di Milano.

7-11 giugno, Roma

Seminario di preparazione all'esame CISSP

16-17 giugno 2004, Ginevra (CH)

CISO Executive Summit

22 giugno 2004, Milano

SEMINARIO CLUSIT - "Principi di crittografia"

23 giugno 2004, Milano

Web Security, 4ª edizione

10 luglio 2004, Roma

Esame di certificazione CISSP

13 luglio 2004, Roma

SEMINARIO CLUSIT - "Principi di crittografia"

Per cancellarsi dalla mailing-list inviare un messaggio (vuoto) a:
clusit-newsletter-unsubscribe@news.clusit.it
riceverete una email alla quale rispondere per confermare la cancellazione.

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