

Seminario CLUSIT

La Sicurezza nei contratti ICT:

Cosa il Committente può ragionevolmente pretendere?

Cosa il Fornitore deve ragionevolmente garantire?

Auditorium SIA

Società Interbancaria per l'Automazione SpA

via Taramelli 26 Milano

Milano - 16 Giugno 2003



www.clusit.it

Abstract

L'obiettivo del Seminario è quello di esplorare le problematiche nell'ambito dei contratti di fornitura di prodotti e servizi di ICT Security.

Inizieremo con l'analisi degli aspetti contrattualistici e legali che caratterizzano il tema della Information Security nell'ambito delle forniture di ICT, dal concetto di Service Level Agreement alle disposizioni normative in materia di "Tutela del trattamento dei dati personali", fino all'analisi dei riferimenti proposti dallo standard ISO 17799/ BS 7799.

Successivamente daremo la parola ad alcuni Information Security Manager affinché illustrino le proprie esigenze in termini di requisiti per forniture di prodotti e servizi di ICT Security. Cercheremo di fare il punto, in particolare, dei requisiti contrattuali richiesti dagli Information Security Manager in funzione delle tipologie di prodotti e servizi che acquistano, e delle modalità previste per la verifica di tali requisiti in fase sia di aggiudicazione della fornitura che di esecuzione contrattuale.

Poi passeremo la parola ai Fornitori di servizi e prodotti di ICT Security per verificare come sia possibile da parte loro indirizzare i requisiti precedentemente illustrati dai Committenti e quali possano essere i vincoli al contorno.

Cercheremo di fare il punto, in particolare, su come vengono definiti, lato fornitore, i requisiti contrattuali per la fornitura di prodotti e servizi in ambito ICT security, e su come vengono forniti i riscontri al committente sia a livello tecnico che procedurale.

Infine si svolgerà una tavola rotonda fra i diversi convenuti nell'ambito della quale verrà dato spazio anche alle domande del pubblico. Nell'ambito della Tavola Rotonda sono previsti interventi anche da parte della SIA, relativamente agli specifici servizi di sicurezza e relativi requisiti contrattuali vigenti in ambito bancario. Inoltre è previsto anche il contributo di un rappresentante della Polizia Postale delle Telecomunicazioni che relazionerà sui requisiti tecnici richiesti per poter effettuare indagini investigative relative a presunti crimini informatici.

Programma

Orario	Titolo intervento	Relatore
9,00- 9,15	Registrazione partecipanti	
9,15 - 9,20	Saluto di Benvenuto a cura di SIA	
9,15- 9,30	Introduzione: Presentazione del CLUSIT e del programma del Seminario	Chairlady: Raffaella D'Alessandro Membro CD Clusit
9,30-10,45	Illustrazione della tematica della contrattualistica nella fornitura di prodotti e servizi ICT, individuazione e formalizzazione dei Service Level Agreement, aspetti legali	Luigi Vannutelli - Socio CLUSIT Andrea Monti - Socio CLUSIT
10,45-11,10	BS 7799 e contratti ICT	Vittorio Asnaghi Membro CD Clusit
11,10-11,30	Coffee Break	
11,30-12,15	Quali requisiti contrattuali nelle richieste di offerta per beni e servizi relativi alla ICT Security? Specificità del contesto Telecom Italia e/o Pirelli	Dr. Pierguido Iezzi Chief Security Officer Pirelli
12,30-13,00	Quali requisiti contrattuali nelle richieste di offerta per beni e servizi relativi alla ICT Security? Specificità del contesto Ministero Pubblica Istruzione	Ing. Alessandro Musumeci Direttore Generale Ministero P.I.
13,00-14,30	Pranzo	
14,30-15,15	Cosa puo' ragionevolmente garantire un fornitore di prodotti e servizi di Information Security? Focus sulla fornitura di Prodotti di ICT Security e nei servizi di EDP outsourcing	Mariangela Fagnani (IBM) Socio CLUSIT
15,15-16,00	Cosa puo' ragionevolmente garantire un fornitore di servizi internet in ambito Information Security? Focus sulla fornitura MSSP e Servizi SOC (I.net + esperienze BT)	Stefano Quintarelli (I.NET) Socio CLUSIT
16,00-16,20	Coffee Break	
16,20-18,00	Tavola Rotonda	Partecipano tutti i relatori intervenuti, SIA e la Polizia Postale <hr/> Conduce la Tavola Rotonda: Luigi Vannutelli Previste domande dal pubblico

SINTESI DEGLI INTERVENTI

ICT Security nei contratti

Abstract intervento Chairlady: Raffaella D'Alessandro, membro CD CLUSIT

Il tema della contrattualistica nell'ambito della fornitura di prodotti e servizi di ICT Security assume aspetti di natura interdisciplinare che richiedono l'indirizzamento e la risoluzione di problematiche ancora oggi assai complesse e non completamente definite e/o definibili.

Tra i diversi aspetti che verranno trattati nell'ambito del seminario avremo modo di acquisire indicazioni relativamente alle problematiche di natura contrattuale, legale, di standardizzazione, di requisiti dell'utenza e di requisiti della fornitura.

Un insieme di esperienze ci consentiranno di capire meglio il problema soprattutto relativamente alla fornitura di Servizi di ICT Security, legati al crescente fenomeno del ricorso all'outsourcing.

Tutto ruota intorno alla definizione del cosiddetto "Security SLA", un "oggetto" ancora difficile da comprendere.

Quando sentiamo parlare di SLA (Service Level Agreement) in ambito ICT ci vengono in mente le tipiche classificazioni definite nei contratti di outsourcing, relative a metriche per la misurazione di performance hardware e di networking, come l'uptime e l'availability. Ma l'Information Security è soprattutto Business Risk Management, e di conseguenza la fornitura di prodotti e servizi di ICT security dovrebbe fare i conti con SLA orientati alla tutela del Business del cliente, piuttosto che a misurazioni di performance delle infrastrutture tecnologiche.

Questo approccio, che ci auguriamo possa presto vedere una consolidata prassi nell'ambito della fornitura di prodotti e servizi di ICT Security, dovrebbe partire dall'analisi dei Business Requirement ed, attraverso una attenta valutazione delle opzioni di Business Risk Management, dovrebbe consentire al cliente di definire:

Termini e Condizioni di copertura contrattuale: dovrebbero essere non troppo lunghi al fine di consentire una rinegoziazione in funzione delle evoluzioni tecnologiche e delle evoluzioni dei rischi di Business correlati.

Servizi coperti: possono cambiare nel tempo, o richiedere aggiornamenti in funzione di nuovi requisiti legali in materia di Information Security, o piuttosto in virtù di cambiamenti organizzativi e/o di strategia di Business.

Service Limits: la definizione di qualità del servizio (in termini di livelli di Security: integrità, riservatezza, disponibilità delle Informazioni) può variare da un concetto di Baseline ad uno di massima aspettativa di qualità da parte del cliente, e può essere commisurata a molteplici parametri, alcuni dei quali ampiamente variabili, come il numero di transazioni che ci si aspetta vengano gestite dal provider.

Metrics: è l'aspetto più difficile da definire, è generalmente espresso in termini percentuali e contiene indicazioni sulla misurabilità degli indicatori chiave. Rimane indubbiamente a carico del cliente la responsabilità nell'individuare tali indicatori e nell'assicurarsi di una loro corretta misurazione e reporting.

Penalties: non si tratta semplicemente di individuare condizioni al di sotto delle quali il cliente può rescindere il contratto, o il fornitore è tenuto a pagare penali, ma di valutare le responsabilità penali e civili che potrebbero insorgere da un mancato raggiungimento dei Security SLA e la possibilità di ripartire quindi tali responsabilità verso i soggetti "liable".

Reviews: sarebbe opportuno concordare a priori la frequenza, o l'occorrenza di eventi, sulla cui base entrambe le parti potranno proporre un aggiornamento del contratto di fornitura.

Change Controls: quando il fornitore dei servizi di ICT Security aggiorna la propria infrastruttura per rendere ai clienti un servizio più sicuro chi garantisce il cliente sulla competitività dei prezzi futuri? Bisognerebbe pensare anche a questo tipo di clausole.

E forse per definire adeguatamente gli SLA di Security sono ancora molte le clausole a cui pensare.

Fermo restando che rimane sicuramente in capo al cliente la responsabilità strategica di decidere se, cosa e come terziarizzare in materia di Information Security, la questione che appare evidente è che non basta individuare correttamente i Security SLA, ma altrettanto vitale è gestirli.

In organizzazioni grandi e distribuite territorialmente la gestione di una moltitudine di SLA, probabilmente forniti da una moltitudine di provider, genera l'esigenza di dedicare notevoli risorse al controllo di questi SLA.

Negli Stati Uniti pare che sempre più numerosi siano gli IT managers che cercano provider che tengano sotto controllo i propri SLA (erogati da altri provider), e probabilmente sta già nascendo un nuovo business poichè sembra che qualcuno stia già offrendo questi servizi.

Più la catena del servizio si allunga più la rete di responsabilità si infittisce e meno appare governabile la liability del Business Risk Management.

Avrà ragione Bruce Schneier quando afferma che alla fine si potrà semplicemente risolvere tutto con una copertura assicurativa?

Sicurezza e Contratti: Luigi Vannutelli – Andrea Monti

Le tematiche relative alla sicurezza hanno una rilevanza notevole in un gran numero di tipologie contrattuali nello scenario del business. Al di là dei contratti il cui oggetto sia la creazione e la gestione di sistemi di sicurezza, nei quali per definizione la tematica "Sicurezza" si pone come l'elemento portante del contratto stesso, vengono passati in rassegna alcuni tipi di contratti nei quali più frequentemente si presentano alle parti contraenti le tematiche attinenti alla sicurezza.

Tali tipologie di contratto possono essere riassunte sulla base di alcuni elementi costitutivi, quali, ad esempio, tutti i contratti nei quali sia previsto l'accesso in aree, fisiche o virtuali, del Committente da parte del Fornitore, quali contratti di manutenzione o di consulenza; contratti che prevedano una durata a medio / lungo termine, ed anche contratti la cui esecuzione comporti l'accesso a dati, informazioni o strutture del Committente che rivestano carattere di riservatezza e / o di segreto industriale.

Viene inoltre sviluppata la distinzione tra "Dati", intesi come sequenze alfanumeriche suscettibili di essere memorizzati in strumenti informatici, ed "Informazioni", intendendosi per tali un insieme aggregato di "Dati" che fornisce al soggetto che ne ha accesso una nozione in più. La differenza è rilevante per il diverso trattamento e la diversa attenzione che deve essere data da parte di chi stia negoziando un contratto. I "Dati" dovranno essere protetti contro possibili perdite, accessi indebiti, manipolazioni non autorizzate, ecc., da cui ne consegue che l'attenzione del negoziatore deve essere prevalentemente indirizzata alle specifiche tecniche che devono essere o attuate o comunque rispettate nella esecuzione del contratto. Diverso è invece il caso delle "Informazioni". Qui si deve partire dal presupposto necessario che le informazioni che devono essere protette, sono già, per definizione, in possesso o comunque accessibili da parte di coloro nei confronti dei quali tali protezioni debbano essere attuate. Si tratta quindi di porre delle regole valide ed efficaci nei confronti di comportamenti umani, con tutte le inevitabili difficoltà che la definizione di tali regole contrattuali comporta.

L'intervento verrà svolto dai due relatori in contemporanea ed in contraddittorio interattivo tra loro stessi.

BS 7799 e contratti ICT: Vittorio Asnaghi

Lo sforzo normativo nel campo dei sistemi di gestione della sicurezza delle informazioni è storicamente posteriore allo sforzo sui criteri per la valutazione della garanzia (TCSEC, ITSEC) e successivo allo sforzo per la definizione delle norme per la gestione dei sistemi di gestione della qualità (serie ISO 9000 e Vision 2000), di cui risente.

Storicamente, nel 1995 è stata pubblicata da BSI (ente di normazione britannico) una norma, la BS 7799, nota anche come Code Of Practice, che costituiva un insieme di buone regole di comportamento per la gestione della sicurezza delle informazioni in azienda, comprendendo in 10 capitoli una dettagliata serie di punti su cui concentrare l'attenzione della Direzione. Tale norma escludeva (e la sua versione attuale BS 7799 parte 1, altrimenti nota come ISO/IEC 17799, esclude ancora oggi) l'utilizzo in attività di verifiche di terza parte (certificazione).

Nel 1999 BSI pubblica la BS 7799 in due parti: la parte 1 analoga al vecchio Code of Practice e la parte 2 contenente dei requisiti oggetto di possibile verifica da terze parti. Nel Settembre 2002 è uscita l'ultima versione di questa norma, che comprende diverse modifiche relative all'esigenza di rendere evidente la continuità del processo di gestione della sicurezza delle informazioni. Il ciclo di vita del processo è suddiviso in quattro fasi: pianificazione del sistema di gestione (Plan), implementazione del sistema di gestione (Do), verifica del sistema di gestione (Check),

applicazione delle modifiche (Act). Il modello sottostante prevede che esista un ciclo continuo che attraversi queste quattro fasi, l'unica modalità che renda possibile il miglioramento ed un'evoluzione dell'organizzazione coerente con l'evoluzione della tecnologia e con i mutamenti delle esigenze dettate dal modello di business dell'Azienda.

Esistono in entrambe le due parti in cui è suddivisa la norma espliciti riferimenti agli aspetti di sicurezza delle informazioni indotti dall'outsourcing, parziale o totale. Tali riferimenti sono concentrati nel capitolo relativo all'organizzazione della sicurezza e sono differenziati per la semplice acquisizione di beni o servizi e il vero e proprio outsourcing. La norma è di tipo generalista, nel senso che deve adattarsi a tutti i modelli di Azienda e a tutte le tipologie di fornitura, per cui i requisiti sono espressi in forma generale e andranno calati nelle specifiche situazioni. Il relatore ritiene che, al di là dei requisiti connessi con la gestione delle terze parti che vengono esaminati nel dettaglio nell'intervento, il beneficio maggiore della norma sia quello di rendere possibile un linguaggio comune tra cliente e fornitore, per tutto ciò che concerne la sicurezza e la proprietà delle informazioni di entrambi.

Pierguido Iezzi

Un'azienda che vuole essere leader si trova oggi a doversi confrontare con la rapidità dei cambiamenti tecnologici e della problematica relativa al mantenimento del proprio vantaggio competitivo derivante da una riduzione sia dei costi che del time to market. Questo scenario costringe le organizzazioni ad essere più snelle ed a ricercare in outsourcing quei partners che si dimostrano in grado di supportare i cambiamenti e che diventano perciò veri e propri attori del vantaggio competitivo. Criticità derivanti da tali scelte si annoverano nel dover virtualmente gestire rapporti di interdipendenza con partners esterni i quali devono necessariamente garantire determinati requisiti di sicurezza volti a tutelare il successo dell'azienda.

Alessandro Musumeci

L'intervento verte sulle specificità nel settore dell'istruzione, dell'università e della ricerca, per quanto riguarda l'acquisizione di beni e servizi.

Verranno esaminate in sintesi le caratteristiche dei sistemi informativi attuali, i piani di sviluppo, e le caratteristiche dei principali contratti, in particolar modo per quanto riguarda i livelli di servizio e la loro verifica.

Verrà quindi dettagliato lo stato attuale dei vari contratti con particolare riguardo a quelli derivanti dalle convenzioni CONSIP e ai loro riflessi in termini di sicurezza e di garanzia del servizio.

Particolare attenzione verrà posta alla recente direttiva sugli esami di stato nella quale viene sperimentata per la prima volta una concreta collaborazione con la Polizia delle Comunicazioni.

Verrà infine illustrata l'evoluzione attesa in termini di livelli di servizio e di prestazioni contrattuali degli attuali contratti e le prospettive future di forniture nel settore dell'istruzione.

Mariangela Fagnani

Premessa

Vorrei iniziare questo intervento, che ha l'obiettivo di presentare quali sono le garanzie di sicurezza che un fornitore di servizi di outsourcing deve ragionevolmente offrire, con qualche considerazione sull'andamento del mercato dell'outsourcing e sul modello evolutivo di tali servizi, che ci permettono di comprendere come questi si ripercuotono sulle necessità di sicurezza delle aziende.

I trend di mercato che emergono da una ricerca presentata recentemente da Michael F. Corbett, Chairman e Executive director dell'Outsourcing Research Council, mostrano che nel periodo 1998-2003 la spesa globale per i servizi di outsourcing è passata da 2 a 5 trilioni di dollari e che nel prossimo futuro le aziende spenderanno mediamente un terzo del loro budget nell'outsourcing, non solo tecnologico, nella sua accezione più ampia.

Nel contesto di mercato odierno, caratterizzato da una competizione sempre più spinta, dalle incertezze dei mercati finanziari, dalle rapidissime evoluzioni della tecnologia, le aspettative dei clienti sono cambiate e cresciute perché richiedono all'outsourcing quella versatilità e flessibilità che permette loro di gestire il cambiamento in tutti i suoi aspetti e di rimanere competitivi sul mercato.

Stiamo assistendo negli ultimi anni al passaggio dalla fase di "IT transformation" , a quella di "Process Transformation", per arrivare al "Business Transformation", ovvero al ridisegno dei processi di business delle aziende che sfrutta le enormi potenzialità offerte dalla tecnologia per realizzare il "Business on demand".

E' evidente che in questo contesto i fornitori dei servizi di outsourcing si trovano sicuramente di fronte una grossa sfida da cui dipende anche la loro capacità di crescita in questo mercato: infatti non possono più limitarsi ad offrire degli efficienti servizi IT, ma devono avere la capacità di creare valore per il business dei clienti, per aiutarli a realizzare la "business resilience", ovvero:

- Permettere ai clienti la flessibilità necessaria per passare alla nuova generazione in termini di infrastruttura e applicazioni
- Ridurre i costi IT e migliorare il valore per gli azionisti
- Permettere ai clienti di focalizzarsi sulle loro competenze "core"
- Migliorare i livelli di servizio
- Variabilizzare i costi
- Poter avere a disposizione le competenze degli esperti a livello di settore, business e tecnologie.

Cosa significa questo cambiamento per la sicurezza informatica ???

Anche il concetto stesso di sicurezza che i fornitori devono garantire cambia in questo nuovo contesto, in quanto deve tener conto delle necessità tipiche del business del cliente, senza trascurare gli aspetti legati all'utilizzo delle nuove tecnologie che sono veicolo di nuovi rischi per l'integrità, la confidenzialità e la disponibilità dei dati e dei servizi offerti.

Naturalmente i servizi di sicurezza offerti dal provider sono strettamente correlati con le tipologie del servizio di outsourcing , quali:

- IT outsourcing services -data center
- Network outsourcing services
- NetworkWorkstation Management Services
- Managed Security Services
- Customer service center
- Trasformational outsourcing di processi quali CRM , Sicurezza (es. Security Operation Center)

e con gli ambienti gestiti (es. ambienti di sviluppo, ambienti di produzione, etc.), ma in questo intervento ci limitiamo a fare una analisi della globalità dei servizi di sicurezza che un fornitore dovrebbe offrire, indipendentemente dall'associazione con la tipologia del contratto.

Servizi di sicurezza

Prima di addentrarci ad analizzare quali aspetti della sicurezza dovrebbero essere assicurati nella fornitura di outsourcing, vale la pena di sottolineare che nel contratto che regola il rapporto fra Cliente e Fornitore ci dovrà essere una parte dedicata alla sicurezza in cui saranno esplicitate in modo chiaro:

- le relative responsabilità, sia per gli aspetti di security che per quelli di privacy (rif. Legge 675/96)
- il contenuto e le caratteristiche dei servizi "base" inclusi nel contratto e di quelli "opzionali"
- i risultati attesi
- le modalità e i parametri di misurazione
- le modalità di billing.

Coerentemente con quanto espresso in premessa, il fornitore deve garantire la sicurezza "end-to-end", agendo sulle seguenti componenti:

- strategie e linee guida
- processi
- tecnologie

➤ personale

ed assicurando non soltanto un ambiente "sicuro" per il trattamento dei dati e dei processi del cliente, ma competenze e soluzioni che aiutino ad indirizzare le necessità specifiche delle diverse tipologie di business in cui operano i clienti.

Strategie e linee guida

Uno dei capisaldi della sicurezza è la presenza di un framework organizzativo e normativo condiviso da tutte le funzioni e strutture coinvolte nel servizio: le policy, gli standard, i processi e le procedure sono quindi essenziali affinché tutte le persone/strutture operino in sintonia e nel rispetto di quanto stabilito a livello contrattuale.

Il quadro organizzativo del fornitore di outsourcing deve prevedere l'assegnazione di compiti e responsabilità per quanto attiene gli aspetti di sicurezza; sia il quadro organizzativo che quello normativo potranno richiedere, per lo specifico cliente/contratto, modifiche e personalizzazioni che assicurino il recepimento del contenuto del contratto stesso ed eventuali legislazioni in materia.

Ruoli, responsabilità e procedure dovranno indirizzare sia la realizzazione delle misure di protezione, che l'amministrazione nel day-by-day, e la gestione di situazioni critiche (incidenti di sicurezza, disastri, etc.).

Non solo il fornitore dovrà assicurare quanto sopra nell'ambito del servizio base offerto, ma, nell'ottica di aiutare i propri clienti nel processo di evoluzione verso l'e-business on-demand, il vero valore aggiunto che potrà offrire sarà quello di mettere a disposizione dei clienti un supporto qualificato per definire ed impostare le strategie di sicurezza, i modelli organizzativi e linee guida coerenti con le strategie di business.

Processi

In un modello di "business on demand", che si basa su ambienti operativi e processi "on demand", i processi IT e i processi di business dovranno essere rivisti anche in ottica di sicurezza e questo è certamente il compito più difficile per i fornitori dei servizi outsourcing, in quanto richiede competenze molto qualificate e diversificate.

Tecnologie

Le soluzioni tecnologiche che il fornitore realizza avranno l'obiettivo di garantire:

- la sicurezza e la continuità delle infrastrutture condivise (rete, ambienti fisici, personale, etc.)
- il recepimento dei requisiti specifici del cliente, espressi nel contratto, in termini di protezione dei dati e di continuità del servizio.

Possiamo classificare le soluzioni tecnologiche secondo le seguenti categorie:

- sicurezza fisica delle aree e sistemi di protezione dei server e delle apparecchiature
- protezione dei confini della rete e delle connessioni esterne, segmentazione della rete interna
- sistemi di identificazione e autenticazione (alla rete, ai sistemi, alle applicazioni)
- protezione del software (di sistema e applicativo) e dei dati
- crittografia e firma digitale
- continuità delle operazioni, business recovery
- sistemi di controllo e monitoraggio della sicurezza (vulnerability scanning, intrusion detection, audit, etc.).

Personale

il personale gioca un ruolo fondamentale nella gestione della sicurezza e deve quindi conoscere nei dettagli cosa, quando e come debba essere fatto per garantire all'azienda ed al cliente il raggiungimento degli obiettivi fissati a livello contrattuale e quanto richiesto dalle leggi in vigore.

Approccio alla sicurezza nei servizi di outsourcing

Se finora abbiamo parlato di quali servizi un fornitore può ragionevolmente offrire, vediamo invece qual'è l'approccio che dovrebbe essere seguito nella presa in carico e nella gestione di un nuovo cliente/servizio; tale approccio si estrinseca in un processo per fasi:

Assessment and Design (assessment delle misure di sicurezza pre-outsourcing, analisi dei requisiti del cliente, gap analisi rispetto al servizio base offerto dal fornitore, definizione del Piano di sicurezza da realizzare, delle responsabilità e dei livelli di servizio attesi)

Implement (realizzazione delle soluzioni tecnologiche, organizzative e di processo)

Run (amministrazione degli aspetti di sicurezza, auditing e controllo, reporting al cliente sul livello di sicurezza).

Penso risulti evidente che, pur essendo l'approccio sopra illustrato valido qualunque sia il contenuto del servizio gestito, le caratteristiche dello stesso richiedono, anche per gli aspetti di sicurezza, competenze e soluzioni mirate che possano permettere ai clienti di raggiungere i propri obiettivi di "business on demand". Si pensi ad esempio alla gestione in outsourcing delle Certification Authority, dei processi della pubblica amministrazione, della sanità, con tutte le loro specificità in termini di privacy e sicurezza.

Dr. Sergio Staro – Vice Questore Aggiunto della Polizia di Stato, funzionario della Divisione Investigativa sui Crimini Informatici del Servizio Polizia Postale e delle Comunicazioni.

La criminalità informatica è in forte e costante espansione in tutto il mondo e anche l'Italia non sembra immune dalle conseguenze di tale espansione.

Nel nostro Paese, infatti, si è registrato un aumento degli incidenti di natura colposa e degli episodi dolosi; sono cresciuti gli attacchi da parte degli *insiders* e dei cosiddetti *hacker* alle aziende, i pedofili sembrano aver trovato sul web una nuova opportunità per soddisfare le loro perversioni sessuali, la duplicazione abusiva del *software* fa registrare un incremento costante, i gruppi terroristici utilizzano il mezzo telematico per attività di proselitismo, organizzazione logistica e rivendicazione degli attentati.

Anche sul fronte della violazione della *privacy* si registrano sempre più spesso azioni condotte da soggetti risoluti che sfruttano il mezzo tecnologico per finalità commerciali al limite del legale (si pensi, ad esempio, all'introduzione di *cookies* all'insaputa del navigatore, alla modifica dei *browser*, all'invio/ricezione di messaggi pubblicitari di posta elettronica non richiesti e non graditi).

Negli ultimi anni, l'importanza del fenomeno è quindi cresciuta notevolmente, facendo registrare sia delle evoluzioni di vecchi reati che la nascita di azioni delittuose nuove, ai danni sia di soggetti singoli che della collettività intera. Le condotte delittuose connesse alle nuove tecnologie consentono generalmente grandi guadagni con costi molto bassi e implicano oltretutto un modesto rischio di essere scoperti e assoggettati a sanzioni penali severe.

Le infrastrutture informatiche e delle telecomunicazioni sono così diventate un elemento critico delle nostre economie, possibile obiettivo di comportamenti criminali, che possono costituire un pericolo per gli investimenti e per le attività degli operatori del settore, nonché per la sicurezza e per la fiducia dei cittadini nella società dell'informazione.

In Italia il Servizio di Polizia Postale e delle Comunicazioni già da tempo è stato deputato al contrasto dei crimini informatici ed opera attraverso una struttura centrale, 19 Compartimenti nelle principali città italiane e 76 sezioni distaccate. Il personale investigativo è altamente specializzato e svolge attività di prevenzione e repressione di tutte le forme di computer crime: hacking, pirateria del *software*, pedofilia *on-line*, truffe e frodi, riciclaggio, cyberterrorismo, eccetera.

L'attività operativa nell'ambito del *computer crime* ha fatto nascere l'esigenza di ricorrere, nel settore dell'investigazione, a figure professionali nuove e altamente specializzate che operano in collegamento stretto con i fornitori di connettività e le compagnie telefoniche. Il personale della Polizia Postale e delle Comunicazioni svolge infatti un percorso di formazione specialistica sia all'interno della struttura che presso realtà esterne aziendali e universitarie.

Attualmente l'attività investigativa ha portato eccezionali risultati soprattutto nel campo del contrasto alla pedofilia *on-line* laddove la normativa attuale consente l'attività sotto copertura al personale della Polizia di Stato. Nel quadro del contrasto a tale forma di reato, negli ultimi tre anni sono state effettuate più di 1000 denunce di soggetti, sono stati eseguiti oltre 120 arresti, 5000 cittadini stranieri sono stati segnalati ai rispettivi organismi di Polizia esteri, più di 90.000 siti web sono stati monitorati e segnalati (solo due residenti su *server* italiani e subito chiusi). Importanti risultati sono stati ottenuti anche nel campo della prevenzione di attacchi a siti istituzionali o di aziende di interesse strategico, come in occasione dell'ultimo G8 tenutosi a Genova, nel corso del quale il Servizio ha individuato e neutralizzato più di 200 attacchi provenienti da comunità di *hackers* italiane e straniere.

L'ambito dove maggiormente la Polizia delle Comunicazioni sta cercando di incrementare l'attività investigativa e preventiva è quello delle aziende. In tale settore ancora permane, infatti, una scarsa propensione alla denuncia in caso di computer crime a causa, prevalentemente, della paura della perdita di immagine aziendale che può seguire alla dichiarata vulnerabilità del sistema. Frequenti incontri con i responsabili della sicurezza aziendale e una capillare azione di sensibilizzazione sono in corso da tempo per tentare di ovviare a questo stato di cose.

PRESENTAZIONE DEI RELATORI

Raffaella D'Alessandro

Membro Comitato Direttivo CLUSIT

Senior Manager Ernst & Young – Technology and Security Risk Services

Laureata in Economia e Commercio sviluppa il proprio percorso professionale in ambito Information Technology occupandosi di programmazione software e di networking presso la Olivetti Systems & Networks. Dopo diversi anni di esperienze tecniche di progettazione, a partire dal 1990 si dedica alle attività di Information Security partecipando alla realizzazione di progetti di integrazione tecnologica di Security Solutions per importanti clienti italiani nell'area Pubblica Amministrazione, Banche, Telco. A partire dal 1997 continua il percorso di specializzazione in Information Security indirizzandosi verso attività di natura consulenziale presso primarie società di consulenza.

Ha ottenuto la qualifica di Lead Auditor BS 7799 del British Standard Institute.

Da molti anni è impegnata in attività associative fornendo importanti contributi di studio e divulgazione sui temi della Information Security.

Andrea Monti – Avvocato

Andrea Monti esercita la professione di avvocato e si occupa di diritto delle telecomunicazioni e delle nuove tecnologie. Fra i suoi clienti annovera software house internazionali, operatori telefonici, internet provider, società internazionali di consulenza, gruppi bancari, gruppi editoriali e case editrici. Ha collaborato e collabora con diverse università.

Dal 2001 è docente di teoria dei sistemi informatici applicati alla didattica del diritto presso la Scuola di specializzazione per l'insegnamento secondario delle università di Chieti e Teramo. È stato componente del comitato scientifico del Master in sicurezza informatica organizzato dal dipartimento di scienze dell'informazione dell'università statale di Milano.

Ha svolto regolarmente attività di formazione per le forze di polizia. Ha tenuto lezioni presso l'Istituto Superiore della Polizia di Stato, il CNA dell'Arma dei Carabinieri e il Centro Addestramento Polizia Postale di Genova.

Scrive di rete e di legge per svariate riviste come PC Professionale, Linux&C, ICT Security, WebMarketing Tools, Interlex e collabora come free lance con il quotidiano Puntocom. Ha scritto per l'editore Apogeo insieme a Stefano Chiccarelli il libro "Spaghetti Hacker" e "Segreti, spie, codici cifrati" con Enrico Zimuel e Corrado Giustozzi.

Sempre per Apogeo ha curato la traduzione italiana del libro di Alan Cooper "The inmates are running the asylum" edito con il titolo "Il disagio tecnologico". Per Hops editore, insieme a Alessia Ambrosini, ha scritto "Trademark online".

Fin dal 1995 è stato relatore in numerosi convegni italiani (in particolare nelle due ultime edizioni della Italian Cyberspace Law Conference) e internazionali fra i quali il Computer Freedom and Privacy 2000 svoltosi a Toronto (CA), l'Internet Rights Workshop svoltosi nel 2001 a Praga, la British Society of Criminology 2002 Conference tenutasi alla Keele University, UK, la Bileta 2003 Conference alla Queen Mary University di Londra e la CTOSE Conference 2003 all'università di Namur (BE).

Sostiene i diritti civili e la libertà di espressione ed è attivamente coinvolto nell'associazione ALCEI

Luigi Vannutelli – Consulente Contratti ICT

Dopo una formazione di base giuridica in Diritto Commerciale Comparato (Italia – USA) , ha iniziato l'attività nel settore dell'esportazione di prodotti siderurgici. Passato subito dopo in IBM ha svolto attività di Professional sull'intero arco della contrattualistica informatica. Ha partecipato in IBM Europe alla task force che ha condotto, con successo, la difesa della stessa nel procedimento antitrust promosso dalla Cee. L'ultima posizione rivestita in questa azienda è stata quella di Contract Negotiation Manager per i contratti in Outsourcing.

Dal 1994 svolge attività professionale indipendente come consulente; è autore di numerosi articoli in riviste del settore informatico e coautore del libro: "Outsourcing nelle tecnologie dell'Informazione" . E' socio del CLUSIT, associazione italiana per la sicurezza informatica. (e-mail: luigi.vannutelli@sercit.com).

Vittorio Asnaghi – Consulente ICT Security

Laureato in ingegneria elettronica, si è occupato fino al 1990 di sviluppo di software di base presso i laboratori di Honeywell e Olivetti, in Italia e negli Stati Uniti. Dal 1990 a 1993 è stato direttore R&D di ESA Software. Dal 1993 la sicurezza delle informazioni è alla base delle sue attività professionali: ha realizzato in Italia il primo Centro di Valutazione indipendente per la sicurezza informatica e partecipato a progetti internazionali per la Difesa. Dal 2003 è libero professionista. Socio fondatore di CLUSIT, è attualmente membro del comitato direttivo e scrive regolarmente per la rivista ICT Security.

Pierguido Iezzi – Security Manager Gruppo Pirelli

Nato il 09/12/1970, laureato in Scienze dell'Informazione, ex ufficiale dell'Esercito Italiano proveniente dai corsi dell'Accademia Militare di Modena. Negli ultimi anni ha ricoperto incarichi in qualità di Information Security Manager per il Gruppo Pirelli e Responsabile della IT Security per Telecom Italia SpA. Dal 2003, è Responsabile della Direzione Security del Gruppo Pirelli.

Alessandro Musumeci – Dir. Gen. Sistemi Informativi Min. Istruzione

Nato a Roma il 16 aprile 1956. Laureato nel 1980 in Ingegneria Meccanica, indirizzo automazione, presso l'Università degli Studi di Roma.

Ha maturato esperienze sia in società di rilevanza nazionale (SOGEI, Informatica & Telecomunicazioni, Gruppo COS) che in ambito internazionale (Cap Gemini, Andersen Consulting) maturando esperienze sia in ambiente bancario (nella Direzione Sistemi del Banco di S.Spirito) che nell'ambito della Pubblica Amministrazione (in Cap Gemini e in Andersen Consulting).

Dirigente dal 1989 ha ricoperto incarichi sia come responsabile tecnologico (per esempio dal 1990 al 1995 come manager delle metodologie e dell'Ingegneria del Software presso l'Andersen Consulting di Roma) che come coordinatore per la realizzazione di complesse procedure (ad esempio per conto dell'Università di Napoli o del Ministero della Giustizia), dirigendo organizzazioni complesse (fino ad 850 specialisti nella consulenza e nell'Information Technology) ubicate sia in ambito nazionale che internazionale.

Attualmente e' il consigliere per le politiche di innovazione tecnologica del Ministro dell'Istruzione, dell'Università e della Ricerca, Letizia Moratti, e Direttore Generale dei Sistemi Informativi dello stesso Ministero.

E' inoltre Docente di Sistemi Informativi presso il Diploma di Laurea in Ingegneria Informatica presso l'Università di Roma "La Sapienza" e ha svolto corsi presso l'Università di Roma "Tor Vergata" e nell'Università di Cagliari nell'ambito dell'Ingegneria del Software.

Giornalista pubblicitista dal 1991 ha pubblicato oltre 400 articoli nell'ambito dell'Information Technology sulle principali riviste di settore.

Ha inoltre pubblicato nel 2003 per l'editrice La Scuola il volume "E-Government e Scuola" con la prefazione del Ministro Letizia Moratti.

Nel corso dell'anno 2000 è stato Direttore Responsabile della rivista Idee & Traguardi.

Infine e' stato membro nel 1999 della commissione AIPA-ASSINFORM-ANASIN per la definizione delle "Linee Guida per la sicurezza nei sistemi informativi della Pubblica Amministrazione" ed è attualmente membro della commissione per il software "OpenSource" nella Pubblica Amministrazione, istituita il 31 ottobre 2002 dal Ministero per l'Innovazione e le Tecnologie e membro del Consiglio Superiore delle Comunicazioni, insediato il 28 marzo 2003.

Mariangela Fagnani – Security Leader South Region IBM

E' laureata in Matematica presso l'Universita' degli Studi di Milano: dal 1981 lavora in IBM dove ha ricoperto diversi ruoli, nell'area dello sviluppo applicativo e delle Operations.

Da 10 anni circa si occupa di Sicurezza Informatica, dapprima nella direzione Strategic Outsourcing e successivamente dal 1998 nella direzione Business Innovation Services (ora Business Consulting Services), divenendo punto di riferimento sia per le Funzioni interne che per i clienti. Dal 2001 ha assunto la responsabilità di Security & Privacy Practice Leader per la South Region. Ha maturato diverse esperienze, all'interno della IBM e presso i clienti pubblici e privati, nell'analisi dei rischi di sicurezza, nel disegno di architetture per la protezione dei sistemi e delle reti (Internet in particolare), nella loro realizzazione e controllo, nella definizione degli aspetti organizzativi e normativi, in particolare nell'applicazione della legge 675/96 e regolamenti successivi inerenti la Data Privacy. Sul tema specifico della Data Privacy ha condotto nell'anno 2000 una serie di seminari presso le Associazioni Industriali Territoriali.

Ha partecipato come relatrice sul tema della Sicurezza Informatica in molteplici convegni e istituti di formazione.

Stefano Quintarelli – Dir. Commerciale I.NET

Nato a Negrar (Verona) il 14 giugno 1965.

Diplomato al St. Charles College, Bogotà (Colombia).

Ha svolto attività di ricerca presso il Dipartimento di Scienze dell'informazione dell'Università degli Studi di Milano.

Nel 1992 ha lavorato come consulente per diverse aziende (Olivetti, IBM, Apple, ENI, PLADA, P&G, etc.).

Nel 1993 ha fondato e diretto SIDA Informatica, società specializzata nella Computer Security.

Nel 1994 ha fondato ed è stato General Manager di Educom, società specializzata nello sviluppo di applicazioni ipermediali e web-based.

Nel 1994 è stato socio fondatore di I.NET S.p.A.

Dal 1994 è direttore commerciale di I.NET S.p.A.