# Indice



## 1. BUSINESS CONTINUITY IN AMBITO BANCARIO

Come noto, la scadenza del 31 dicembre si avvicina.

ANSSAIF ha svolto una indagine fra i suoi associati e qui di seguito sintetizziamo le principali risultanze.

Tutte le banche interpellate hanno adottato un approccio molto simile, anche nella realizzazione di soluzioni di dettaglio, sia per il coinvolgimento nei gruppi di elevati esperti del business e della "macchina operativa", nonché del senior management, sia per l'attività di condivisione delle problematiche e soluzioni svolta da ABI. Le banche maggiori e grandi sono in linea con i tempi e prevedono di presentare, entro le prossime settimane, ai rispettivi Consigli di Amministrazione la relazione sulle attività svolte, coerenti con gli impegni assunti ed approvati entro il 30 giugno 2005. La maggior parte delle banche invierà tali relazioni alla Banca d'Italia, per opportuna informazione.

Ciascuna relazione, in generale, ci risulta che riporterà:

- l'indice del Business Continuity Plan (fanno eccezione la maggior parte delle banche di interesse sistemico che invieranno l'intero BCP);
- l'indicazione delle soluzioni di mitigazione adottate, con l'esplicazione puntuale delle eventuali differenze adottate in corso d'opera, corredate dalla motivazione;
- le Società Controllate per le quali è stato redatto un BCP, avendo processi vitali o altamente critici, o coinvolte nella "filiera" di processi vitali o critici della Capogruppo;
- gli interventi eseguiti nei confronti degli Outsourcers coinvolti nei processi vitali ed altamente critici;
- una sintesi dei ruoli e responsabilità previsti per la gestione della Business Continuity e della Crisi, una volta a regime (dal 1° gennaio) e necessari per l'emanazione della normativa;
- l'approccio alla esecuzione dei test, che si intendono fare nel corso del 2007;
- l'indicazione sugli investimenti in formazione e sensibilizzazione alla continuità operativa, nei confronti del personale della banca;
- lo staffing, i sistemi e le infrastrutture necessarie per l'ufficio addetto alla gestione della Business Continuity;
- altre spese, di cui il CdA deve prendere atto ed approvare;
- altre informazioni peculiari della realtà aziendale in oggetto.

In tutti gli intermediari si è notata una evidente soddisfazione sul lavoro svolto e sui risultati raggiunti, malgrado la novità (e difficoltà!) che presenta l'individuazione di soluzioni di mitigazione dei rischi che siano "cost justified":

ciò in quanto si è in presenza di scenari caratterizzati da eventi rarissimi ma disastrosi.

In generale l'approccio è stato duplice: elevata tensione nella stesura e prova di opportune misure preventive, di emergenza e di ripristino, per i processi vitali, di sistema.

Negli altri casi (ossia, processi che diventano altamente critici nelle prime ore), valutazione attenta di possibili soluzioni di mitigazione alternative (backup reciproco fra strutture esistenti, ma molto distanti fra loro; outsourcing; contratti "open" di fornitura di attrezzature e sistemi; stipula di polizza assicurativa; ecc.) in modo da consentire di ottenere il recovery in breve tempo, ma con un'oculata attenzione ai costi.

Se a tutto questo si aggiunge che negli ultimi mesi molti processi di business o strutture organizzative sono cambiate, costringendo i gruppi di progetto a rapide analisi d'impatto e a modifiche tecniche, e, inoltre, che si stanno ripetendo i test di Disaster Recovery a livello aziendale e di sistema bancario, l'ottimismo è allora interpretabile come l'umore dello scalatore o del velista che oramai vede la meta agognata (indipendentemente se è arrivato primo o ultimo!).

Sarà interessante osservare come evolverà la continuità operativa nel 2007, ma ci auguriamo che l' "information sharing" fra gli intermediari e gli operatori di sistema continui, o addirittura si intensifichi, in modo che si trovino sempre le giuste soluzioni alle problematiche che man mano si incontreranno.

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

## 2. CYBERCRIME

Considerazioni personali sugli "insider's" interni partendo dal presupposto che i dipendenti costituiscono: la minaccia più seria, la prima linea di difesa, la risorsa più pregiata.

Uno studio del servizio segreto USA e del CERT della Carnegie Mellon University descrive tratti e motivazioni più frequenti di un insider ostile interno. E questo perché è cambiata la percezione di una volta che considerava le minacce portate dall'esterno alla rete aziendale preminenti rispetto a ciò che potevano fare gli utenti interni: è ormai acclarato che gli attacchi portati da persone apparentemente fidate e in vario modo 'interne' all'azienda (dipendenti, consulenti, partner...) sono molto più dannosi, in proporzione, di quelli portati da hacker esterni on quanto un 'insider' è considerato affidabile, quindi meno controllato.

In Italia, non esistono molte ricerche sulla percezione esatta che le aziende italiane hanno del crimine informatico e del peso che gli insider hanno in questi fenomeni. Un'indagine IBM su circa 150 imprese nazionali ha mostrato che metà (51%) delle aziende italiane intervistate ritiene che le minacce alla sicurezza aziendale provengano oggi dall'interno delle rispettive organizzazioni. Di contro, questo pericolo è evidenziato dal 66% delle aziende a livello mondiale.

Buona parte (75%) dei responsabili IT italiani è poi convinta che il crimine organizzato dotato di competenze tecniche stia sostituendo la figura dell'hacker solitario e, in misura minore (50%) che una minaccia emergente proviene anche dai sistemi non protetti presenti nei Paesi in via di sviluppo.

**Sono tre le principali motivazioni che inducono un "interno" ad agire:**

- la curiosità e la sfida: molti insider non considerano affatto ciò che fanno come un attacco all'azienda, ma piuttosto come una sfida attraverso cui dimostrare competenze e pazienza. Gli attacchi più comuni portati per questo motivo comprendono il forzare account di posta, fare penetration

test non autorizzati o arrivare a informazioni sensibili come il salario del collega;

- la vendetta: e' la spinta degli insider che pensano di avere motivi di rivalsa nei confronti dell'azienda in generale o di qualche collega in particolare. Sono pericolosi perché hanno uno scopo preciso e forti motivazioni (tra i casi scoperti l'indagine ha rilevato che il 92% del campione agiva per vendetta);
- il guadagno: cresce il numero degli insider che rubano informazioni sensibili per conto di qualcuno esterno all'azienda.

**Gli attacchi più comuni rilevati:**

- Sabotaggio: distruzione fisica di parte dell'infrastruttura IT o dei sistemi collegati. Furto di informazioni o di beni: sottrazione di informazioni digitali, furto di documenti cartacei, furto di oggetti informativi fisici.
- Inserimento di *bad code*: bombe a tempo, ossia software programmato per danneggiare un sistema in un certo momento, e le bombe logiche, che si attivano non a tempo ma secondo determinate condizioni.
- Virus: il portatore di virus più pericoloso è sempre l'utente disattento, ma anche gli insider usano introdurre virus nelle loro imprese.
- Attacchi a livello di protocollo: DNS spoofing, TCP sequence, hijacking delle sessioni TCP/IP, Denial of Service...
- Attacchi a livello di sistema operativo - Sono portati soprattutto da parte di utenti tecnici e con privilegi di accesso, che sanno quali vulnerabilità ci sono nei loro sistemi e quali non sono state *patchate*.
- Social engineering - La buona vecchia *ingegneria sociale* è ancora un mezzo diffuso ed efficace per carpire le informazioni necessarie ad aumentare i propri livelli di autorizzazione in rete o per raggiungere altri dati importanti.

A. Caricato, ANSSAIF - www.anssaif.it

## 3. INFOSECURITY ITALIA 2007

**IL COMITATO SCIENTIFICO**

DANILO BRUSCHI, Professore Ordinario di Informatica presso il Dipartimento di Informatica e Comunicazione dell'Università degli Studi di Milano, Presidente Onorario Clusit.

ANTONELLO BUSETTO, Direttore dei Rapporti Istituzionali di Federcomin (Confindustria).

ALFONSO FUGGETTA, Amministratore Delegato e Direttore Scientifico del Cefriel.

LUIGI MANCINI, Professore Ordinario di Informatica presso l'Università di Roma La Sapienza.

CLAUDIO MANGANELLI, Componente del CNIPA, è stato Presidente del Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle PA.

GIULIO OCCHINI, Presidente uscente e Direttore Generale AICA (Associazione Italiana per l'Informatica ed il Calcolo Automatico).

SILVANO ONGETTA, Presidente AIEA (Associazione Italiana Information Systems Auditors).

STEFANO QUINTARELLI, Presidente AIIP (Associazione Italiana Internet Provider), Socio Fondatore e membro del Comitato Direttivo del Clusit.

ERMINIO SEVESO, Direttore Organizzazione e Sistemi di BTicino, Presidente AUSED (Associazione Utilizzatori Sistemi e tecnologie dell'Informazione).

MICHELA TERRIBILE, Confcommercio - Settore Utilities e Telecomunicazioni.

DOMENICO VULPIANI, Direttore del Servizio Polizia Postale e delle Comunicazioni.

GIOVANNI ZICCARDI, Professore Associato di Informatica Giuridica e Informatica Giuridica Avanzata presso la Facoltà di Giurisprudenza dell'Universita' degli Studi di Milano.

## I CONVEGNI

### 6 Febbraio (Pomeriggio) CONVEGNO INFOSECURITY

IDENTITÀ DIGITALE: UNA SFIDA PER IL FUTURO

Ogni utente della rete possiede molteplici identità digitali, anche nell'ambito della stessa organizzazione. Ciò rende estremamente problematica e spesso inefficente la gestione delle identità digitali, sia per gli utenti che per gli amministratori di sistema. Il problema non è purtroppo di facile soluzione. Solo recentemente sono state messi a punto metodologie e prodotti che possono contribuire ad una soluzione radicale.

In questo convegno, alcuni rappresentanti delle Istituzioni e esperti del settore illustreranno le iniziative più significative in ambito nazionale.

Alcuni fornitori leader di mercato illustreranno alcuni esmpi reli in cui il problema è stato risolto con successo.

Nel corso del convegno si discuterà anche del problema del furto di identità digitale.

Chairman: GIGI TAGLIAPIETRA, Presidente CLUSIT

### 7 Febbraio (Giornata intera) CONVEGNO STORAGE/INFOSECURITY

TECNOLOGIE, NORME E STANDARD PER LA SICUREZZA DELLE INFORMAZIONI

È sempre più vasto il repertorio di norme e Standard in ambito Security che un'azienda è chiamata a soddisfare: Testo Unico sulla Privacy, Legge sulla Data Retention, Legge sul Diritto d'Autore, Legge sulla Pedofilia online, Basilea 2, norme ISO, Common Criteria, ecc. Il corretto uso di tecnologie di Storage e di Security possono facilitare notevolmente le attività che un'azienda deve intraprendere per far fronte a tali esigenze. Nell'ambito di questo convegno, alcuni massimi esperti in ambito legale e normativo esporranno lo stato dell'arte in materia; i fornitori leader di mercato illustreranno casi reali in cui le tecnologie hanno aiutato le aziende a raggiungere i livelli di conformità richiesti.

**MATTINO**

Chairman: MARCO GATTI (Giornalista Week.it)

**POMERIGGIO**

Chairman: GIGI BELTRAMI (Gionalista, Sole24Ore)

### 8 Febbraio (Mattino) CONVEGNO INFOSECURITY

LA SICUREZZA DELLE APPLICAZIONI WEB

Il web è ormai diventato l'ambito di riferimento per lo sviluppo di tutte le applicazioni di rete, quali ad esempio home banking, e-commerce, e-government, e-health, ecc. La stragrande maggioranza di tali applicazioni richiede spesso il. soddisfacimento di requisiti di sicurezza molto stringenti.

Scopo del presente convegno è illustrare le metodologie e le tecnologie oggi presenti sul mercato per la realizzazione o la messa in sicurezza di applicazioni web.

Alcuni fornitori illustreranno le tecniche utilizzate in casi concreti.

Chairman: JOY MARINO

Keynote speaker: DAVE WICHERS

*Dave Wichers is the COO and cofounder of Aspect, where he is responsible for running daily operations of the company. Prior to founding Aspect, Dave started and ran the application security practice at Exodus Communications, which provided a full suite of application security consulting services to Fortune 500 and other commercial companies starting in1998.*

*Dave has focused on information security during his entire career, starting in 1988. His information security background spans the entire security engineering lifecycle, including software development, system security requirements, security architectures, secure designs, security policies, models, and system testing.*

*He has supported the design and development of trusted operating systems, trusted databases, secure routers, multilevel secure guards, and large integrated systems for a wide variety of customers, including NSA, DoD, and Fortune 500 vendors and end customers.*

*Dave is a primary author of the OWASP Top 10 Web Application Security Vulnerabilities and is the OWASP Conferences Chair. He was also a primary contributor to the group responsible for creating ISO 21827, the Systems Security Engineering Capability Maturity Model (SSE-CMM).*

*Dave earned a B.S. summa cum laude in Computer Systems Engineering from Arizona State University and an M.S. summa cum laude in Computer Science from the University of California at Davis. Dave holds both CISSP and CISM certifications.*

## I SEMINARI CLUSIT EDUCATION

**6 febbraio - 14.00/18.00**

"I rischi del Trusted Computing"

Docente: Claudio Telmon (membro CD e CTS Clusit)

Abstract: Il Trusted Computing, la cui più famosa implementazione è quella proposta dal Trusted Computing Group, comincia a essere implementato in alcuni dei computer in commercio. Il Trusted Computing promette nuove funzionalità di sicurezza, ma è stato criticato anche per diversi rischi che porterebbe con sè. Il seminario cerca di fornire alcuni elementi per valutare sia l'efficacia in termini di sicurezza, sia i rischi di questa tecnologia.

**8 febbraio - 10.00/18.00**

"Il Social Engineering e la sua applicazione nel penetration testing professionale: tecniche di attacco, strategie per difendersi in contesti aziendali, case-study ed esercitazioni pratiche".

Docenti: Raoul Chiesa (OPST, OPSA), Andrea Ghirardini (CISSP)

Abstract: Questo seminario, della durata di una intera giornata, analizzera' nel dettaglio la tecnica del Social Engineering e la sua applicazione nell'esecuzione professionale di verifiche di sicurezza, azioni di penetration testing ed ethical hacking. I due docenti, forti di dieci anni di esperienza in questo delicato settore, illustreranno alla platea le basi fondamentali dell'ingegneria sociale, per passare poi all'analisi approfondita di alcuni attacchi specifici, fornendo e dettagliando casi di studio realmente avvenuti. La seconda parte della giornata vertera' sulle

corrette strategie da adottare in azienda per difendersi da questa tipologia di attacchi, generalmente di difficile rilevazione, e si concludera' con delle esercitazioni teoriche e pratiche, selezionando alcuni volontari tra il pubblico.

### LA PRESENTAZIONE DEL PROGETTO HPP

7 febbraio - 14.00/16.30

Presentazione del progetto HPP

**Un nuovo approccio al Cybercrime: il progetto HPP - Hacker's Profiling Project**

- Introduzione al progetto HPP e presentazione dei risultati 2005-2006
  Relatori: Raoul Chiesa, Alessio Pennasilico, D.ssa Elisa Bortolani
- Presentazione del libro "HPP"
  Relatore: Fabio Brivio, Apogeo Editore
- Tavola Rotonda sull'evoluzione del cybercrime ed il profiling degli hackers

Ospiti:

Raoul Chiesa, CLUSIT/ISECOM, HPP Project Manager

Alessio Pennasilico, CLUSIT/AIPSI, HPP Core Team

D.ssa Elisa Bortolani, Psicologa, HPP Core Team

Matteo Curtoni e Maura Parolini, scrittori ed esperti di true-crime.

Prof. Silvio Ciappi, Cattedra di Criminologia all'Università di Firenze (in attesa di conferma)

### PREMIO TESI

7 febbraio - 16.30/18.00

Premiazione della Seconda Edizione del Premio **Innovare la sicurezza delle Informazioni** e presentazione delle migliori tesi.

## 4. IL NUOVO COMITATO DIRETTIVO DEL CLUSIT

Nel corso dell'assemblea generale del 30 novembre, si è proceduto all'elezione del nuovo Comitato Direttivo e del Presidente del Clusit.

Sono stati eletti:

- **Gigi Tagliapietra** - *Presidente*
- Luca Bechelli
- Raoul Chiesa
- Mauro Cicognini
- Mariangela Fagnani
- Giorgio Giudice
- Paolo Giudice
- Tomaso Mansutti
- Massimiliano Manzetti
- Luca Marzegalli
- Roberto Mircoli
- Mattia Monga
- Andrea Monti
- Stefano Quintarelli
- Claudio Telmon

## 5. SESSIONE DI STUDIO AIEA-CLUSIT

AIEA e CLUSIT presentano i risultati del Gruppo di ricerca **L'Outsourcing IT: best practice e Auditing** in una sessione di studio che avrà luogo a Milano, il 12 dicembre 2006 alle ore 14.00, presso la sede della Banca Popolare di Milano, via Massaua 6 - Milano.

A tutti i presenti, sarà consegnata una copia del volume scritto dal Gruppo di ricerca, nel quale sono raccolte *alcune best practice pertinenti alla professione dell'IS Auditor quando essa sia esercitata per la revisione di realtà nelle quali il Sistema Informativo, o anche la sola gestione dell'infrastruttura IT, siano stati esternalizzati*.

Per partecipare alla Sessione di Studio è necessario compilare l'apposita scheda di iscrizione che dovrà pervenire alla Segreteria Clusit per fax o email, entro il 4 dicembre. I soci delle associazioni che aderiscono al Clusit possono partecipare alla sessione di studio e dovranno -nella compilazione della scheda di iscrizione- barrare la casella "Invitato CLUSIT".

L'invito e l'agenda della Sessione di Studio, l'abstract del volume **L'Outsourcing IT: best practice e Auditing** e la scheda di registrazione sono disponibili su: www.clusit.it/eventi/061212_aieaclusit.pdf

## 6. NOTIZIE DAI SOCI

Il socio Giovanni Bassetti ci segnala l'uscita di un suo romanzo, un thriller basato sull'hacking ed internet:

www.prospettivaeditrice.it/libri/schedeautori/bassetti1.htm

Avevamo già segnalato l'imminente fusione di Federcomin e FITA. Ora è nata **Confindustria Servizi Innovativi** e si tratta di un messaggio forte, da parte di Confindustria, significativo per l'intero comparto.

Ricordiamo che la sola Federcomin rappresenta circa un migliaio di aziende che fatturano complessivamente circa 80 miliardi di euro.

Oltre a Clusit, le associazioni che aderiscono a Federcomin sono:

Asstel (Associazione delle imprese esercenti servizi di telecomunicazioni), AITech-Assinform (Associazione Italiana per l'Information Technology), Aiip (Associazione Italiana Internet Providers), Asas (Associazione delle imprese per i servizi, le applicazioni e le tecnologie ICT per lo spazio), Assocertificatori (Associazione dei ncertificatori di firma digitale), Assoticket (Associazione tra i produttori di sistemi fiscali per biglietteria), Fedoweb (Federazione Operatori Web), FRT (Federazione Radio Televisioni), RNA (Radio Nazionali Associate).

**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