



▶ RACCOLTA DEI NOTIZIARI  
SETTIMANALI REDATTI DAL  
GARANTE PER LA PROTEZIONE  
DEI DATI PERSONALI..... 5



▶ CLUSIT INFORMA.....8



▶ Newsletter ISACA.....15  
▶ Newsletter AiPSI.....17  
▶ Newsletter ANSAIFF.....21

○ GENNAIO

○ 2007

# ISAudit *focus*



## La Newsletter di AIEA

AIEA è dal 1979 il primo capitolo Europeo accreditato ISACA  
(Information Systems Audit and Control Association & Foundation)

Gennaio 2007

## Buon Anno ai nostri soci!

Quando leggerete questa newsletter, saranno già state ultimate le operazioni di conteggio e verifica delle votazioni per il rinnovo del Consiglio Direttivo.

Ringraziamo e salutiamo i Consiglieri uscenti e teniamoci pronti ad accogliere i Consiglieri di nuova nomina!

Siamo, dall'anno scorso, un Very Large Chapter ed abbiamo superato la quota di 550 soci. Quindi, ricordiamoci che solo con il supporto di tutti i soci, il Consiglio Direttivo riesce sia a rappresentare le necessità, che a proporre attività realmente significative per l'accrescimento professionale di ciascuno di noi.

Buon lavoro a tutti i soci!



Associazione Italiana  
Information Systems Auditors



Al servizio dei professionisti dell'IT Governance

Capitolo di Milano

## **AIEA partecipa**

IL 25 gennaio, il nostro Presidente parteciperà all'evento "Identity e access management: un approccio organizzativo e metodologico", organizzato da AUSED.



## **Hanno parlato di AIEA**

ICT Security n. 51 dicembre 2006 .... pagina 7 ..... in buona compagnia tra i partner scientifici ....

ComputerWorld 27 novembre 2006 ... pagina 12 ..... " In parallelo è stata avviata una collaborazione con AIEA (....) che promuove ..."

## **Notizie da altre Associazioni**

Abbiamo ricevuto, da Marco Misitano (**AIPSI**), la seguente mail:

Caro Socio,  
durante l'assemblea di oggi, Venerdì 15 Dicembre 2006 è stato eletto il Presidente ed il Consiglio Direttivo per il triennio 2007-2009.

Elio Molteni è stato confermato presidente di AIPSI

Il Comitato Direttivo è composto da:

Molteni Elio  
Misitano Marco  
Pasquinucci Andrea  
Telmon Claudio  
Pennasilico Alessio  
Mapelli Maurizio  
Zanero Stefano  
Giudice Giorgio  
Agrelli Massimo  
De Paoli Claudio

Cordialmente,  
Marco L. Misitano  
CISSP, CISA, CISM  
Communication Officer  
AIPSI - Associazione Italiana Professionisti Sicurezza Informatica  
Italian Chapter ISSA - Information Systems Security Association  
[www.aipsi.org](http://www.aipsi.org), [www.issa.org](http://www.issa.org)

Da Marco Gentili (**CNIPA**) abbiamo ricevuto la seguente comunicazione:

Carissimi,  
Vi invio una nuova classe di fornitura 3.3.3 Continuità operativa delle "Linee guida sulla qualità dei beni e servizi ICT per la definizione ed il governo dei contratti della PA".

3 3 3 COP ContinuitàOperativa - v1 0 18-12-06.doc

Il tema trattato è quello della Business continuity. La classe di fornitura è stata resa coerente con le riflessioni ed i documenti sviluppati dall'apposito gruppo di lavoro CNIPA coordinato da Rellini a cui molte società associate AiTech/Assinform hanno partecipato.

Voglio particolarmente ringraziare Luciano Boschetti dell'HP che si è prodigato operativamente assieme a Dario Biani nella stesura del testo. Un grazie anche ai colleghi Giancarlo Pontevolpe e Giovanni Rellini per la loro attenta opera di revisione.

Aggiungo poi la nuova versione 2.0 della classe di fornitura 1.3.1 Assistenza in remoto.

Si tratta di una maior release che ha recepito la norma UNI 11200 sui contact center, ha introdotto la distinzione tra inbound e outbound e ha profondamente revisionato gli indicatori di qualità.

Voglio particolarmente ringraziare Stefania Gaetani Boschetti della B2win che ci ha segnalato la norma e che, come rappresentante di ASSOCONTACT, si è occupata della riscrittura della classe di fornitura assieme a Dario Biani.



Prego AiTech/Assinform e ASSOCONTACT di diffondere i documenti a tutti gli associati, come al solito rimango in attesa di eventuali richieste di emendamento che potranno essere proposte dalle Associazioni afferenti alla Federazione Servizi Innovativi e Tecnologici di Confindustria.

A 2 anni dall'emissione delle Linee Guida le stesse sono contraddistinte da una dinamica elevata: sono state completamente revisionati tutti i manuali emessi ed estese le classi di fornitura. Altre imminenti novità vi saranno inviate prossimamente in tema di utilizzo contrattuale dei function point (revisione del manuale 2 sulle Strategie di acquisizione).

Nel 2007 inizieremo poi a lavorare su un nuovo manuale, l'ottavo, dedicato agli studi di fattibilità e su una revisione della classe di fornitura dedicata alla consulenza allo scopo di recepire recenti norme UNI 11066 11067 10771 in materia di Consulenza di Direzione.

Colgo l'occasione per fare a tutti gli auguri di Natale e di buone feste.

.....  
I documenti citati dal Dr. Gentili sono reperibili e scaricabili dal sito [www.cnipa.it](http://www.cnipa.it)

\*\*\*\*\*

#### **Le prossime attività di AIEA**

Di seguito pubblichiamo il calendario degli eventi 2007, già programmati.



# Calendario Eventi

## 1° SEMESTRE 2007

## 1° SEMESTRE 2007



Al servizio dei professionisti dell'IT Governance

Capitolo di Milano

	Gennaio	Febbraio	Marzo	Aprile	Maggio	Giugno
1						
2			Inizio Corso CISA Milano			
3			Corso CISA Milano			
4					Corso CISM Milano Corso CISM Roma	
5					Corso CISM Milano Corso CISM Roma	Workshop COBIT
6				Corso CISA Torino		
7				Corso CISA Torino		
8		Sessione di Studio Torino	Sessione di Studio Roma			
9			Sessione di Studio Milano Inizio Corso CISA Roma Inizio Corso CISA Torino			
10			Corso CISA Roma Corso CISA Torino			
11					Corso CISA Roma Corso CISA Torino	
12	Sessione di Studio Lugano	Corso Base IS Audit Roma			Termine Corso CISA Roma Termine Corso CISA Torino	
13		Corso Base IS Audit Roma		Corso CISA Milano Corso CISA Roma		
14		Corso Base IS Audit Roma		Corso CISA Milano Corso CISA Roma		
15		Corso Base IS Audit Roma				
16		Corso Base IS Audit Roma Sessione di Studio Milano	Corso CISA Milano			
17			Corso CISA Milano	Sessione di Studio Torino		
18					Corso CISM Milano Corso CISM Roma	
19				Sessione di Studio Roma	Termine Corso CISM Milano Termine Corso CISM Roma	
20		Corso COBIT base	Corso COBIT Avanzato	Sessione di Studio Milano Corso CISM Milano Corso CISM Roma Corso CISA Torino		
21		Corso COBIT base	Corso COBIT Avanzato	Corso CISM Milano Corso CISM Roma Corso CISA Torino		
22						
23			Corso CISA Roma Corso CISA Torino			
24			Corso CISA Roma Corso CISA Torino			
25						
26						
27				Corso CISA Milano Corso CISA Roma		
28				Termine Corso CISA Milano Corso CISA Roma		
29						
30			Corso CISA Milano			
31	Sessione di Studio Roma		Corso CISA Milano			

Associazione Italiana Information Systems Auditors

20141 Milano Via Valla, 16 Tel. +39/02/84742365 Fax. +39/02/700507644 E-mail: aiea@aiea.it P.IVA 10899720154 C.F. 97109000154

Luogo	Data	Note
Roma	31 gennaio	In collaborazione con ISCOM
Milano	16 febbraio	
Roma	8 marzo	Probabile tema: Basilea II
Milano	9 marzo	
Roma	19 aprile	
Milano	20 aprile	
Roma	4 ottobre	
Roma	8 novembre	
Roma	13 dicembre	
Torino	8 febbraio	
Torino	17 aprile	

**Percorsi formativi**

Il **Corso Base IS Audit** sarà ripetuto, a Roma, dal 12 al 16 febbraio 2007.  
Sul sito AIEA è disponibile la locandina completa del corso di Roma.

Nei primi mesi del 2007 è programmato, a Milano, il **Corso COBIT**.

Le date da ricordare sono:

Corso **COBIT Base**: 20-21 febbraio 2007

Corso **COBIT Avanzato**: 20-21 marzo 2007

**Esame CISA e CISM di giugno 2007**

Di seguito riportiamo la pianificazione dei corsi, a Roma, a Milano e a Torino, che potrà essere utile ai soci, per meglio programmare le attività.

	Domini	Sede di Milano	Sede di Roma	Sede di Torino
<b>CISA</b>	1 e 2	2 e 3 marzo	9 e 10 marzo	9 e 10 marzo
	3	16 e 17 marzo	23 e 24 marzo	23 e 24 marzo
	4	30 e 31 marzo	13 e 14 aprile	6 e 7 aprile
	5	13 e 14 aprile	27 e 28 aprile	20 e 21 aprile
	6 ed esame	27 e 28 aprile	11 e 12 maggio	11 e 12 maggio
<b>CISM</b>	1 e 2	20 e 21 aprile	20 e 21 aprile	
	3 e 4	4 e 5 maggio	4 e 5 maggio	
	5 e test	18 e 19 maggio	18 e 19 maggio	

**Bibliografia**

E' on line il nuovo numero di InterLex ( <http://www.interlex.it> )

Vi informiamo che sul sito [www.cnipa.it](http://www.cnipa.it) sono disponibili molti documenti di interesse per i nostri soci. Ricordiamo, inoltre, che il CNIPA organizza incontri o seminari aperti anche ai soci AIEA



- PRIVACY. ADOZIONI E DIRITTO DI CRONACA
- CASO SWIFT: GRAVI DEFICIT INDIVIDUATI DAI GARANTI UE

## Privacy, adozioni e diritto di cronaca

Non si può pubblicare senza il consenso dei genitori la notizia che un minore è stato adottato

Non si può pubblicare, senza il consenso dei genitori, la notizia che un minore è stato adottato. Lo vietano la normativa sulla privacy, il codice deontologico dei giornalisti e la legge sulle adozioni.

Con un forte richiamo ai mezzi di informazione il Garante ha concluso l'esame della segnalazione di una persona che lamentava la pubblicazione della notizia relativa all'adozione, da parte sua, di un bambino. Come evidenziato in più occasioni, il Garante ha ribadito che le informazioni sullo stato di adozione sono oggetto di una speciale protezione. Per tutelare la personalità dell'adottato e la sua famiglia la legge, infatti, stabilisce che siano i genitori adottivi a decidere i modi e i tempi per informare il minore della sua condizione. E a garanzia degli interessati la normativa individua limiti rigorosi, anche penali, riguardo alla diffusione di questa informazione.

Inoltre, pur tenendo conto del delicato problema del bilanciamento tra diritto di cronaca e diritti dei cittadini, l'Autorità ha ribadito la necessità che i giornalisti rispettino con particolare rigore, quando scrivono di minori, la regola dell'essenzialità dell'informazione. Il codice deontologico prescrive infatti una forte tutela della personalità dei minori, giungendo ad affermare che il loro diritto alla riservatezza deve essere sempre considerato come primario rispetto al diritto di cronaca.

L'esigenza di una particolare cautela da parte del giornalista trova conferma anche in altre disposizioni del Codice della privacy, laddove si prevede che in caso di pubblicazione di sentenze o altri provvedimenti su riviste giuridiche siano omesse le generalità o altre informazioni che rendano identificabili i minori.

## Caso Swift: gravi deficit individuati dai Garanti Ue

Un grave deficit di trasparenza nei confronti della clientela, l'assenza di un'adeguata base giuridica per il trasferimento di dati personali ad autorità Usa, la mancata consultazione delle autorità di protezione dati: sono queste le principali critiche espresse dai Garanti europei rispetto al caso Swift - la Società per le Telecomunicazioni Finanziarie Interbancarie Mondiali con sede in Belgio - e all'inosservanza delle normative sulla protezione dei dati. I Garanti hanno invitato tutti i soggetti responsabili (Swift, Banche centrali, istituzioni bancarie e finanziarie) a porre rapidamente rimedio alla situazione attuale, onde evitare possibili sanzioni da parte delle autorità nazionali per la protezione dei dati. Swift è la società, con sede in Belgio, di cui si servono da decenni le banche ed i soggetti operanti nel settore finanziario di tutti i Paesi europei per i trasferimenti internazionali di valuta. Tali trasferimenti riguardano anche Paesi al di fuori dell'Ue, come gli Usa, con tutti i problemi che ciò comporta in termini di adeguato rispetto per i dati personali dei soggetti coinvolti (ad esempio, i soggetti che effettuano il pagamento, o i beneficiari del pagamento stesso). I Garanti europei, riuniti nel Gruppo di lavoro "Articolo 29", hanno affrontato questi problemi il 22 e 23 novembre scorso a Bruxelles dopo un'attenta analisi della documentazione e delle informazioni fatte pervenire da Swift, sollecitati anche da articoli di stampa comparsi negli ultimi mesi. In particolare, si trattava di capire in che modo avessero operato Swift e le istituzioni finanziarie che di Swift si servono rispetto alle richieste formulate da autorità federali Usa che, nel quadro della lotta contro le attività terroristiche, più volte avevano chiesto ed ottenuto da Swift di accedere ad informazioni contenute nelle transazioni finanziarie. L'analisi condotta dal Gruppo dei Garanti europei ha portato a stabilire che Swift e le istituzioni finanziarie sono contitolari del trattamento in questione, seppure per aspetti distinti. Entrambi hanno, pertanto, la responsabilità di assicurare il rispetto delle norme europee e nazionali in materia di protezione dei dati. Swift e le istituzioni finanziarie hanno violato le disposizioni della Direttiva 95/46 in materia di protezione dei dati personali, poiché non hanno

informato adeguatamente i clienti della possibilità che i loro dati fossero trasferiti negli Usa per le finalità sopra ricordate. In particolare, Swift ha proceduto a fornire le informazioni richieste dalle autorità Usa senza consultare le autorità nazionali di protezione dati né altri soggetti competenti, mentre le istituzioni finanziarie che di Swift si servono hanno omesso di vigilare adeguatamente sul rispetto delle norme di protezione dati da parte di Swift. I Garanti hanno sottolineato che il trasferimento dei dati personali dei clienti alle autorità federali Usa è stato effettuato senza alcun valido fondamento giuridico e con un grave deficit di trasparenza che non ha consentito il controllo indipendente da parte delle autorità europee per la protezione dei dati.

I Garanti hanno invitato Swift e le istituzioni finanziarie ad adottare rapidamente tutte le misure necessarie, nei rispettivi ambiti, per porre rimedio alla situazione. In caso contrario, si sono riservati l'applicazione di tutte le sanzioni previste dalle norme nazionali in materia. Inoltre, anche le Banche centrali dei singoli Stati membri dovranno fare chiarezza sul proprio ruolo in quanto autorità di vigilanza rispetto all'operato di Swift.

Un grave deficit di trasparenza nei confronti della clientela, l'assenza di un'adeguata base giuridica per il trasferimento di dati personali ad autorità USA, la mancata consultazione delle autorità di protezione dati: sono queste le principali critiche espresse dai Garanti europei rispetto al caso Swift - la Società per le Telecomunicazioni Finanziarie Interbancarie Mondiali con sede in Belgio - e all'inosservanza delle normative sulla protezione dei dati. I Garanti hanno invitato tutti i soggetti responsabili (Swift, Banche centrali, istituzioni bancarie e finanziarie) a porre rapidamente rimedio alla situazione attuale, onde evitare possibili sanzioni da parte delle autorità nazionali per la protezione dei dati. Swift è la società, con sede in Belgio, di cui si servono da decenni le banche ed i soggetti operanti nel settore finanziario di tutti i Paesi europei per i trasferimenti internazionali di valuta. Tali trasferimenti riguardano anche Paesi al di fuori dell'Ue, come gli Usa, con tutti i problemi che ciò comporta in termini di adeguato rispetto per i dati personali dei soggetti coinvolti (ad esempio, i soggetti che effettuano il pagamento, o i beneficiari del pagamento stesso).

I Garanti europei, riuniti nel Gruppo di lavoro "Articolo 29", hanno affrontato questi problemi dopo un'attenta analisi della documentazione e delle informazioni fatte pervenire da Swift, sollecitati anche da articoli di stampa comparsi negli ultimi mesi. In particolare, si trattava di capire in che modo avessero operato Swift e le istituzioni finanziarie che di Swift si servono rispetto alle richieste formulate da autorità federali Usa che, nel quadro della lotta contro le attività terroristiche, più volte avevano chiesto ed ottenuto da Swift di accedere ad informazioni contenute nelle transazioni finanziarie. L'analisi condotta dal Gruppo dei Garanti europei ha portato a stabilire che Swift e le

istituzioni finanziarie sono contitolari del trattamento in questione, seppure per aspetti distinti. Entrambi hanno, pertanto, la responsabilità di assicurare il rispetto delle norme europee e nazionali in materia di protezione dei dati.

Swift e le istituzioni finanziarie hanno violato le disposizioni della Direttiva 95/46 in materia di protezione dei dati personali, poiché non hanno informato adeguatamente i clienti della possibilità che i loro dati fossero trasferiti negli Usa per le finalità sopra ricordate. In particolare, Swift ha proceduto a fornire le informazioni richieste dalle autorità Usa senza consultare le autorità nazionali di protezione dati né altri soggetti competenti, mentre le istituzioni finanziarie che di Swift si servono hanno omesso di vigilare adeguatamente sul rispetto delle norme di protezione dati da parte di Swift. I Garanti hanno sottolineato che il trasferimento dei dati personali dei clienti alle autorità federali Usa è stato effettuato senza alcun valido fondamento giuridico e con un grave deficit di trasparenza che non ha consentito il controllo indipendente da parte delle autorità europee per la protezione dei dati.

I Garanti hanno invitato Swift e le istituzioni finanziarie ad adottare rapidamente tutte le misure necessarie, nei rispettivi ambiti, per porre rimedio alla situazione. In caso contrario, si sono riservati l'applicazione di tutte le sanzioni previste dalle norme nazionali in materia. Inoltre, anche le Banche centrali dei singoli Stati membri dovranno fare chiarezza sul proprio ruolo in quanto autorità di vigilanza rispetto all'operato di Swift.

---

#### NEWSLETTER

del Garante per la protezione dei dati personali  
(Reg. al Trib. di Roma n.258 del 7/6/99).  
Direttore responsabile: Baldo Meo.  
Ha collaborato Antonio Caselli.

Direzione e redazione: Garante per la protezione dei dati personali, Piazza di Monte Citorio, n.121 - 00186 Roma.  
Tel: 06/69677713 - Fax: 06/69677755. Newsletter è



## COMUNICATO STAMPA

### **MAGGIORI GARANZIE SUL POSTO DI LAVORO: LE LINEE GUIDA DEL GARANTE PRIVACY**

No ad archivi centralizzati per i dati biometrici, dati sanitari conservati in fascicoli separati, cartellini identificativi a prova di privacy, lavoratori informati sui loro diritti. Il Garante ha definito, per la prima volta in un quadro unitario, misure ed accorgimenti per disciplinare la raccolta e l'uso dei dati personali nella gestione del rapporto di lavoro. Il provvedimento generale, relatore Mauro Paissan, è stato adottato anche in seguito a numerose istanze di lavoratori, organizzazioni sindacali e imprese. A questo provvedimento ne seguiranno altri che affronteranno specifiche tematiche, come l'uso delle e-mail e la navigazione in Internet. Queste in sintesi i punti principali delle linee guida.

#### **Principi generali**

Il datore di lavoro può trattare informazioni di carattere personale strettamente indispensabili per dare esecuzione al rapporto di lavoro. Deve individuare il personale che può trattare tali dati e assicurare idonee misure di sicurezza per proteggerli da indebite intrusioni o illecite divulgazioni.

Il lavoratore deve essere informato in modo puntuale sull'uso che verrà fatto dei suoi dati e gli deve essere consentito di esercitare agevolmente i diritti che la normativa sulla privacy gli riconosce (accesso ai dati, aggiornamento, rettifica, cancellazione etc). Entro 15 giorni dalla richiesta il datore di lavoro è tenuto a comunicare in modo chiaro tutte le informazioni in suo possesso

#### **Cartellini identificativi, Intranet, bacheche aziendali**

Nelle aziende private può essere eccessivo indicare sul cartellino identificativo del dipendente dati anagrafici o generalità: a seconda dei casi può bastare un codice identificativo o il solo nome o solo il ruolo professionale.

Senza consenso non si possono comunicare informazioni ad associazioni di datori di lavoro, di ex dipendenti o a conoscenti, familiari, parenti. Il consenso è necessario anche per pubblicare informazioni personali (foto, curricula) nella Intranet aziendale e a maggior ragione in Internet. Nella bacheca aziendale possono essere affissi solo ordini di servizio, turni lavorativi o feriali. Non si possono invece diffondere emolumenti percepiti, sanzioni disciplinari, assenze per malattia, adesione ad associazioni.

#### **Dati sanitari**

I dati sanitari vanno conservati in fascicoli separati. Il lavoratore assente per malattia è tenuto a consegnare al proprio ufficio un certificato senza la diagnosi ma con la sola indicazione dell'inizio e della durata presunta dell'infermità. Il datore di lavoro non può accedere alle cartelle sanitarie dei dipendenti sottoposti ad accertamenti dal medico del lavoro. Nel caso di denuncia di infortuni o malattie professionali all'Inail, il datore di lavoro deve limitarsi a comunicare solo le informazioni connesse alla patologia denunciata.

#### **Dati biometrici**

Non è lecito l'uso generalizzato e incontrollato di dati biometrici, specie se ricavati dalle impronte digitali. L'uso può essere giustificato solo in casi particolari, per presidiare, ad esempio, accessi ad "aree sensibili"(processi produttivi pericolosi, locali destinati a custodia di beni, documenti riservati). Anche quando l'uso è consentito non è ammessa la costituzione di banche dati centralizzate: è infatti sufficiente la memorizzazione su una smart card in uso esclusivo del dipendente.

## ETICA DELLA SICUREZZA

### **Etica della sicurezza.**

La soluzione è un modello collaborativo che esca dai confini dell'azienda.

Dall'epoca "cavalleresca" degli hacker alla ricerca del gesto élatante, siamo passati alla criminalità organizzata che vede nella rete un campo d'azione particolarmente allettante. Alla vulnerabilità per gli attacchi si associa una vulnerabilità dovuta alla complessità di un vero e proprio ecosistema fatto di milioni di macchine e milioni di utenti con l'aggiunta della totale mobilità. È difendibile un sistema simile? Quali sono i principi della sicurezza che rimangono validi e quali i miti da sfatare? Quali cambiamenti dopo l'11 settembre e, soprattutto, quali strategie adottare per difendere il valore dell'informazione? Sappiamo per certo che l'informazione è un bene prezioso e che potrà essere difeso solo con uno sforzo collaborativo che superi l'egoismo dei singoli e consideri la rete un patrimonio comune.

Con la diffusione pervasiva di sistemi informativi in rete, il tema della sicurezza informatica, da materia esoterica per addetti ai lavori è diventata argomento di interesse comune e fonte di giusta preoccupazione dei singoli individui oltre che di aziende ed enti pubblici. A fronte di una situazione in continuo mutamento, ci sono aspetti legati alla sicurezza delle informazioni che non sono cambiati e che vale la pena di conoscere, come è bene sfatare alcuni concetti che sono del tutto infondati.

Il bisogno di sicurezza è un bisogno primario che viene subito dopo il soddisfacimento dei bisogni fisiologici, è la condizione necessaria perché si possano stabilire relazioni con gli altri perché in un ambiente "insicuro" non siamo a nostro agio e le emozioni hanno il sopravvento sulla ragione. Viviamo in un mondo di incertezze, incertezze che sono cresciute e mutate con le trasformazioni sociali e chiediamo all'informatica certezze che non abbiamo nella nostra vita quotidiana. I computer sono sempre più affidabili e sicuri ma l'ecosistema in cui interagiscono li pone in una condizione di pericolo costante. Il mondo dell'informatica, presentato come il mondo binario degli 1 e degli 0 in cui non esistono sfumature, ingenera inoltre una forte aspettativa di certezza e di prevedibilità nella convinzione del totale dominio dell'uomo sulla macchina. Ricordo che il padre della cibernetica italiana Silvio Ceccato parlando del computer lo chiamava "l'idiota fulmineo" perché se istruito dall'uomo a fare una cosa sbagliata la faceva comunque e sempre a velocità straordinaria.

Dobbiamo innanzitutto accettare serenamente il primo principio: la sicurezza non esiste. Non potremo mai essere sicuri al 100% così come non possiamo aspettarci di vivere in eterno o di essere sempre in buona salute. La sicurezza deve conciliare aspetti tra loro conflittuali: le reti vogliono far comunicare liberamente e velocemente persone e imprese, la sicurezza vuole chiudere e controllare tutto. Se è vero che non esiste in assoluto, la sicurezza è la ricerca di un equilibrio dinamico, cioè sempre in movimento, tra apertura e chiusura, tra improvvisazione e regole, tra costi e danni.

Il secondo principio dice che la sicurezza è un'emozione: non è una condizione oggettiva uguale per tutti ma fa entrare in gioco importantissimi fattori emotivi e di vissuto personale, che a parità di situazione portano ad azioni molto diverse fra loro. La sicurezza riguarda quindi i comportamenti e non solo le tecnologie e richiede una forte coerenza nell'interazione fra i due: che senso ha una porta blindata se lascio la chiave

nella toppa? Che senso ha una password lasciata in chiaro sul tavolo? Il terzo principio dice che la sicurezza è la gestione di un rischio e in sostanza riassume i primi due: dobbiamo scegliere fino a che punto "sentirci" sicuri e quanto investire economicamente, in rinunce, in regole, in prodotti, per raggiungere questa condizione emotiva e oltre tale soglia accettare il rischio.

La sicurezza dovrebbe quindi ridurre il rischio in termini accettabili o sostenibili economicamente dall'impresa, per poi lasciare il "rischio residuo" al mondo delle assicurazioni. Qual'è, sempre parlando di principi, il più grande nemico della sicurezza? È l'abitudine. Dopo un attentato i controlli sono rigorosissimi e diventa particolarmente sicuro viaggiare, anche se logisticamente più problematico, mentre a distanza di qualche mese, quando l'allarme rientra e i controlli si attenuano, sale proporzionalmente il rischio di subire un nuovo attacco. La sicurezza vive di routines e controlli, pensate al check che fanno i piloti prima di tutti i decolli, ma guai se vengono fatti distrattamente e senza la consapevolezza di compiere un gesto importante per la propria vita e quella degli altri. Da queste considerazioni deriva il pilastro principale su cui poggia la sicurezza: il backup, la copia di sicurezza, il sistema d'emergenza.

Se si parte dall'assunto che non esiste la sicurezza assoluta non ci si deve domandare cosa fare SE avremo un guasto o un incidente, bensì cosa fare DATO CHE prima o poi avremo un guasto o un incidente.

Il brano è tratto dal saggio "Etica della sicurezza" di Gigi Tagliapietra, pubblicato integralmente sul secondo volume di Nòva24 Review, il bimestrale di ricerca, innovazione e creatività del Sole 24 ORE. Per ulteriori informazioni: [www.ilsole24ore.com/nova](http://www.ilsole24ore.com/nova).

## CYBERCRIME

Perché non ci sono più attacchi massicci di virus?

Vi ricordate i tempi di NIMDA, CODE RED, GAOBOT, e così via? Perché non si bloccano più le aziende? Perché milioni di computer non si fermano più, tutti assieme, un dato giorno? Ci sono tanti virus, tanti computer ogni giorno si bloccano, ma non è un attacco preoccupante. Almeno come in passato.

I giornali ne parlano poco. I possessori di computer dormono sonni tranquilli. Sono convinti di essere protetti. Lo sono veramente? Hanno l'ultima versione dell'antivirus? Siamo certi?

Una nostra indagine ha rivelato che su 100 utenti che hanno a casa il personal computer, tutti hanno un antivirus, ma solo il 45% si ricorda di quando ha scaricato l'ultimo aggiornamento! Il 5% è caduto dalle nuvole ed ha chiesto addirittura spiegazioni!

Hanno tutti un personal firewall attivato? Sono state inserite delle regole per impedire l'uscita dal pc di informazioni personali? Il 75% ha risposto di no.

Allora una domanda viene spontanea: non è che questa apparente "tranquillità" sta progressivamente indebolendo le difese? Non delle aziende, ma bensì di coloro che utilizzano il computer a casa, dove tengono dati personali e da dove fanno transazioni su Internet.

Abbiamo accennato tempo fa alla nostra preoccupazione: non si sta preparando un attacco massiccio? Correggiamo la domanda: non è che criminali (non trascurando i terroristi) stanno installando "trojans" sui computer e da lì si preparano a prelevare dati o ad attaccare le aziende? Milioni di computer potrebbero diventare dei temibili nemici.

Ecco allora l'invito nuovamente ai media: sensibilizzate, nel dovuto modo, i consumatori.

Come il Cliente aggiunge l'olio al motore per evitare di perdere l'auto ed i soldi, così aggiunga sicurezza al computer.

Ne basta poca: quella suggerita dal venditore o dal negoziante sotto casa. Nulla di più.

Noi chiaramente siamo sempre disponibili a fornire informazioni ed aiuto.

*Anthony Cecil Wright, Presidente ANSSAIF - [www.anssaif.it](http://www.anssaif.it)*

## INFOSECURITY ITALIA 2007

Riportiamo il programma aggiornato al 31.12.2006 dei convegni che abbiamo contribuito ad organizzare nell'ambito di Infosecurity Milano (6-8 febbraio).

### **6 Febbraio Pomeriggio**

#### **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 inefficiente 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 reali 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**

#### **Relatori:**

- GIOVANNI MANCA - Responsabile Ufficio Standard e tecnologie d'identificazione del CNIPA

#### **L'identità digitale nell'e-government europeo**

In Italia ed Europa l'e-government continua la sua evoluzione per offrire servizi ai cittadini e alle imprese. In Italia proseguono le esperienze della Carta d'Identità Elettronica e della Carta Nazionale dei Servizi per l'accesso ai servizi in rete della PA. Ma il "cittadino europeo" quante identità digitali dovrà avere? Quale sarà la situazione nei prossimi mesi ed anni? Quale è il futuro della ECC (European Citizen Card)?

- LORENZO GRILLO - Country Manager VeriSign Italy

### **Un approccio integrato al furto di identità. L'esperienza CREDEM**

L'Internet Banking ha raggiunto un alto livello di qualità e gli utenti di servizi online stanno crescendo, anche se le frodi online continuano ad aumentare. CREDEM ha seguito l'approccio integrato di VeriSign, per fornire ai clienti, durante le loro attività di online banking, un alto livello di protezione delle proprie credenziali e delle informazioni personali contro i furti di identità

- GIOVANNI ANASTASI - ICT Manager Arthis

### **Gestire in sicurezza l'accesso ai dati e ai sistemi IT**

Sarà presentata l'esperienza di Arthis, che ha scelto la soluzione ORACLE Identity Management Suite per accrescere i propri livelli di sicurezza in termini di accesso ai dati e ai sistemi IT da parte degli utenti interni ed esterni. Arthis, fondata dal Gruppo Rinascente e da Accenture, gestisce tutte le funzioni di back office della grande distribuzione, dai servizi di account al reporting finanziario, consentendo al gruppo di aumentare l'efficienza operativa e nel contempo di operare in conformità al dlgs 196/03 sulla privacy.

- DOMENICO VULPIANI - Direttore Servizio Polizia Postale e delle Comunicazioni

### **Il furto di identità digitale**

Il furto di identità digitale è sicuramente la minaccia emergente che sta caratterizzando quest'ultimo periodo di evoluzione della rete e delle forme di attacco informatico. In questo intervento si delineeranno i contorni di questa forma di attacco rifacendosi a casi reali riscontrati a livello nazionale ed internazionale.

- CASE STUDY (in fase di definizione)
- CASE STUDY (in fase di definizione)

### **STORAGE/INFOSECURITY 7 Febbraio**

#### **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 - Direttore Responsabile WEEK.it**

**Relatori:**

ISAudit  
 *focus*

- GIOVANNI ZICCARDI - Università degli Studi di Milano
- CASE STUDY a cura di ISS
- CASE STUDY a cura di NetApp
- FRANCO GUIDA - Fondazione Ugo Bordoni - Vice-Direttore dell'Organismo di Certificazione della Sicurezza Informatica (OCSI)
- CASE STUDY a cura di ACHAB

#### **POMERIGGIO**

**Chairman: GIGI BELTRAME - Responsabile ICT & tech solutions - il Sole 24 Ore**

#### **Relatori:**

- ANDREA MONTI - Socio fondatore e membro del CD Clusit

#### **Privacy, informazioni segrete in aziende e ICT: problemi e soluzioni**

Lo scopo di questo intervento è fornire indicazioni chiare e concrete su come tutelare gli asset immateriali dell'impresa, nel rispetto della legge ma, soprattutto, di quello degli azionisti. Sempre più spesso la sicurezza ICT in azienda è identificata con la "messa a norma" della normativa sui dati personali. In realtà la protezione degli asset immateriali dell'azienda è un argomento ben più ampio e complesso.

Questo, anche per via di leggi - come il codice della proprietà industriale - tanto importanti quanto trascurate e a causa di recenti sentenze che hanno tracciato, finalmente, degli indirizzi chiari sui poteri di controllo delle imprese sull'uso delle risorse di comunicazione da parte dei dipendenti.

- CASE STUDY a cura di EMC
- CASE STUDY a cura di DELL
- PAOLO MACCARRONE - MIP School of Management del Politecnico di Milano
- CASE STUDY in fase di definizione
- CASE STUDY in fase di definizione

#### **INFOSECURITY 8 Febbraio Mattino**

#### **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**

#### **Relatori:**

- DAVE WICHERS keynote speaker

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 in 1998.

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.

- CASE STUDY a cura di ONE ANS
- CASE STUDY in fase di definizione
- CASE STUDY in fase di definizione

## SEMINARI CLUSIT 2007

È in fase di definizione il calendario 2007 dei seminari Clusit.

Segnaliamo che è in funzione un nuovo sistema che gestisce le registrazioni ai seminari Clusit online.

### **Registrazione**

Le registrazioni ai seminari d'ora in avanti avvera' solo online, dopo essersi registrati come utente (non saranno piu' accettate le registrazioni con fax).

La registrazione sarà immediatamente confermata dopo l'invio.

La conferma di partecipazione sarà inviata la settimana precedente il seminario all'indirizzo e-mail indicato.

### **Prerequisiti**

- Per usufruire del diritto di partecipazione gratuita ai seminari il Socio deve essere in regola con la quota sociale per l'anno in corso.

- Le Aziende associate, possono inviare un numero massimo di tre delegati per ciascun seminario.
- Per iscriversi in seguito ad un invito o ad una convenzione indicare il Codice Convenzione o Invito di 5 caratteri di cui si e' in possesso.
- Sono accettate fino a 3 iscrizioni di studenti a titolo gratuito per ogni seminario. Sarà considerato valido ai fini dell'iscrizione l'ordine d'arrivo delle registrazioni. Uno stesso studente può partecipare gratuitamente fino a 3 seminari nel corso di un anno solare. Lo studente dopo ogni registrazione deve inviare il certificato di frequenza rilasciato dall'Università per fax al numero 02.700440.496 o la scansione per email a: [edu@clusit.it](mailto:edu@clusit.it). In caso di mancato invio entro i 5 giorni successivi, la registrazione sarà cancellata. Non sono accettati altri tipi di documenti quale libretto, ricevute di pagamento, ecc.; *non sara' data risposta a richieste di ogni forma di deroga.*

#### **Cancellazione**

In qualunque momento è possibile cancellare la registrazione inviando un messaggio a [edu@clusit.it](mailto:edu@clusit.it), per dare così la possibilità di partecipare ad altri Soci.

#### **Riprese video e/o audio**

E' possibile che per alcuni seminari sia predisposta la registrazione video e/o audio allo scopo di rendere il materiale fruibile sul web o con altri mezzi di diffusione.

Su <https://edu.clusit.it> sono disponibili maggiori informazioni e sono aperte le iscrizioni ai primi 2 seminari, che si terranno in ambito Infosecurity Milano, nei giorni 6 e 8 febbraio.

Coloro che si iscrivono ai seminari di febbraio, possono richiedere a [info@clusit.it](mailto:info@clusit.it) un invito valido per l'ingresso gratuito a Infosecurity Italia.

# ExpressLine

A Monthly Newsletter for the Leadership of ISACA®



Informa

## Certification Update

### CISA and CISM Exam Highlights

The results of the December 2006 exam will be released in early February. The candidates will receive an e-mail result only if they consented to item 25 on the registration form and the exam fee has been paid in full. Please remind candidates to keep their record updated to ensure that current e-mail and postal addresses are available for result correspondence. To prevent the e-mail result notification from being directed to a spam folder, candidates should add [certification@isaca.org](mailto:certification@isaca.org) to their address book, white list or safe-senders list. To ensure the confidentiality of scores, exam results will not be reported by telephone or fax.

Once the exam results have been released, processing time for the hundreds of applications that will be received in the certification department is six to eight weeks. Please advise exam passers from previous administrations who are ready to submit their applications to send them as soon as possible to beat the rush.

Registration for the June 2007 Certified Information Systems Auditor™ (CISA®) and Certified Information

Security Manager® (CISM®) exams began on 8 November. The early registration deadline is 14 February 2007.

Candidates may view or print a copy of the CISA or CISM Bulletin of Information for the June 2007 exams at [www.isaca.org/cisaboi](http://www.isaca.org/cisaboi) and [www.isaca.org/cismboi](http://www.isaca.org/cismboi).

### CISA and CISM Scoring Change

ISACA's CISA and CISM certification boards recently approved changing the way exams are scored. To alleviate confusion found with the previous scoring method and to provide greater clarity, ISACA will use a 200-800 point scale with a passing point of 450 beginning with the June 2007 exams. Using a 200-800 scale will increase the range of scores and eliminate the perception that the score is a percentage. This scoring method is used by several testing organizations, including the well-respected SAT and GRE exams.

### 2005 CISA Audit

The audit of documentation for 2005 CPE activities continues. Please direct member questions to the certification department at [certification@isaca.org](mailto:certification@isaca.org) or +1.847.253.1545, ext. 471 or 403. ■

Please note that to substantiate CISA/CISM CPE credits claimed for exposure draft review under the category "contributions to the IS audit and control profession" (10-hour annual limitation), you should keep a copy of your comments as no formal certificate is awarded.

The Standards Board has issued IS Auditing Guideline G36 Biometric Controls, which is effective for IS audits commencing after 1 February 2007. ■

### Bookstore Update

Inform your members of the newest ITGI/ISACA research and the latest peer-reviewed books at the ISACA Bookstore, including:

IT Control Objectives for Sarbanes-Oxley, 2nd Edition\*

Audit Planning: A Risk-Based Approach

Audit and Trace Log Management: Consolidation and Analysis

Fraud Auditing and Forensic Accounting, 3rd Edition

Information Security: Design, Implementation, Measurement and Compliance

Implementing Database Security and Auditing

Security, Audit and Control Features Oracle E-Business Suite: A Technical and Risk

Management Guide, 2nd Edition\*

IS Audit  
focus

# ExpressLine

A Monthly Newsletter for the Leadership of ISACA®



Anti-Hacker Tool Kit, 3rd Edition

Business Continuity and Disaster Recovery for InfoSec Managers

2007 CISA study aids\*, [www.isaca.org/cisabooks](http://www.isaca.org/cisabooks)

2007 CISM study aids\*, [www.isaca.org/cismbooks](http://www.isaca.org/cismbooks)

\*Published by ISACA/ITGI

Visit the ISACA web site ([www.isaca.org/bookstore](http://www.isaca.org/bookstore)) and take advantage of secure online ordering, or contact the Bookstore at [bookstore@isaca.org](mailto:bookstore@isaca.org) or +1.847.253.1545, ext. 401 or 478. ■

## News Briefs

### Journal Update

The Information Systems Control Journal is seeking articles for volume 3, 2007, to be issued in May 2007. The copy deadline for drafts for volume 3 is 23 January 2007, and the theme is Top IT Problems. For more information, please view the 2007 editorial calendar at [www.isaca.org/journal](http://www.isaca.org/journal) or e-mail [jhaggiorgiou@isaca.org](mailto:jhaggiorgiou@isaca.org). ■

### Attachments to this issue...

- § Conference/Training Week Update
- § Research Update
- § Nominations and Participation Update
- § K-NET Facts



## AIPSI, Associazione Italiana Professionisti di Sicurezza Informatica

ESTRATTO DELLA NEWSLETTER AIPSI N.RO 6 del 16 DICEMBRE 2006

---  
## In Primo Piano ##  
---

- Elezioni del nuovo Comitato Direttivo e del Presidente

Il 15 Dicembre 2006 si sono svolte le elezioni del Consiglio Direttivo e del Presidente che saranno in carica dal 1 Gennaio 2007 al 31 Dicembre 2009. I risultati delle elezioni sono:

Presidente Eletto (42 voti validi su 42 espressi)

\* Elio Molteni (27 voti)

Consiglieri Eletti (48 voti validi su 48 espressi)

- \* Elio Molteni (37 voti)
- \* Marco Misitano (34 voti)
- \* Andrea Pasquinucci (31 voti)
- \* Claudio Telmon (30 voti)
- \* Alessio Pennasilico (29 voti)
- \* Maurizio Mapelli (28 voti)
- \* Stefano Zanero (28 voti)
- \* Giorgio Giudice (27 voti)
- \* Massimo Agrelli (23 voti)
- \* Claudio De Paoli (19 voti)

Le piu' vive congratulazioni ai nuovi eletti con un augurio di buon lavoro per i prossimi 3 anni.

Infine un ringraziamento alla commissione elettorale per il lavoro svolto.

---  
## Attivita' Locali e dell'Associazione ##  
---

- Certificazione AIPSI - Successo dei corsi di preparazione LoCSI

Il 11/12/2006 a Milano e 14/12/2006 a Roma si sono tenuti i primi corsi di preparazione alla Certificazione LoCSI di AIPSI. I corsi hanno ricevuto un grandissimo apprezzamento da parte dei partecipanti il che fa ben sperare per la prima sessione d'esame prevista per il 13/01/2007 e per le future edizioni dei corsi. Vi aspettiamo pertanto numerosi all'esame!

Ulteriori informazioni e materiale didattico per la certificazione AIPSI a questo link: <http://www.aipsi.org/certificazione/>

---  
## Eventi con la partecipazione di AIPSI ##  
---

- e-Security Lab 2007





## AIPSI, Associazione Italiana Professionisti di Sicurezza Informatica

AIPSI Partecipa come supporto ad e-Security Lab 2007, che avrà luogo il 24 e 25 gennaio 2007 (<http://www.bci-italia.com/eseconomy07.asp>).

Due sono gli interventi di moderazione a cura di AIPSI:

- \* Security Risk Management: Suite e Appliance di Threat & Vulnerability Management. Confronto/dibattito - Moderatore Stefano Zanero - AIPSI
- \* SCADA (Supervisory Control And Data Acquisition), i sistemi per il monitoraggio elettronico dei sistemi fisici: gestirne i rischi per la sicurezza derivanti dall'interconnessione globale in rete IP dei sistemi - Moderatore Maurizio Mapelli - AIPSI

- Jekpot business 24x7

AIPSI partecipa a BUSINESS 24-7 (Milano, 30-31 gennaio 2007; [www.jekpot.com/pagine/b247.htm](http://www.jekpot.com/pagine/b247.htm)), conferenza gratuita su Business Continuity, Service Oriented Architecture e Virtualization con un intervento del Socio e membro del CD Andrea Pasquinucci. All'evento è associato il tutorial a pagamento "Business Continuity & Disaster Recovery Plan" con sconto del 10% per i soci AIPSI, indicando il numero di tessera nel form di registrazione.

- AIPSI ad Infosecurity StorageExpo-Trackability

La nostra associazione, oltre ad uno stand dedicato, disporrà di un proprio spazio convegni nell'ambito della manifestazione che si terrà a Milano dal 6 all'8 Febbraio 2007 ([www.infosecurity.it](http://www.infosecurity.it)). Il programma della manifestazione, ancora in fase di approvazione finale, comprende oltre ai temi classici di Infosecurity e StorageExpo, anche la Trackability. Un'area dedicata alla sanità (Health & ICT) rappresenta un'ulteriore novità per l'edizione del 2007. AIPSI, nel nuovo ruolo di Partner Scientifico di Infosecurity collabora, inoltre, con gli enti organizzatori (Fiera Milano International e Reed Exhibitions) nella definizione del programma.

Maggiori dettagli verranno comunicati appena disponibili.

-----  
## Area Soci ed opportunità per i Soci ##  
-----

- Pubblicazioni

Ricordiamo ai soci che è possibile pubblicare articoli sia sul sito AIPSI che, in inglese, su ISSA Journal (contattate <[editor@aipsi.org](mailto:editor@aipsi.org)>).

Gli articoli di ISSA Journal sono disponibili on-line in PDF sul sito di ISSA ed anche nell'area soci del sito di AIPSI.

- Eventi

- Sikurezza.org

Le mailing list italiane di riferimento per la discussione di argomenti in sicurezza informatica sono quelle di Sikurezza.org ([www.sikurezza.org](http://www.sikurezza.org)). In particolare suggeriamo a tutti di iscriversi o consultare via web le liste [ml@sikurezza.org](mailto:ml@sikurezza.org) per le questioni tecniche, e [lex@sikurezza.org](mailto:lex@sikurezza.org) per quelle legali/giuridiche.

L'iscrizione è possibile dal sito web di Sikurezza. Se avete qualche domanda, anche inusuale, in sicurezza informatica è molto facile che possiate ricevere la risposta dai partecipanti a queste liste.





## AIPSI, Associazione Italiana Professionisti di Sicurezza Informatica

Se inviate un messaggio alle liste di Sicurezza, vi preghiamo di aggiungere alla vostra firma anche la dizione "Socio AIPSI".

- Corsi Auditor/Lead auditor ISO 27001:05 dell'ISMS User Group Italia

ISMS IUG Italy ha perfezionato un accordo con STR Srl di San Marino per la fruizione di corsi auditor/lead auditor ISO 27001:05. L'accordo e' stato raggiunto per i corsi accreditati IRCA e RICEC, ed altri corsi di STR Srl.

E' stato raggiunto un accordo con ISMS IUG Italy per ottenere sconti considerevoli anche per i soci AIPSI. I soci interessati possono contattare [info@aipsi.org](mailto:info@aipsi.org) per informazioni.

-----  
## ISSA News ##  
-----

- 2006 ISSA International Awards - Call for Nominations Closing December 31, 2006

The calendar year 2006 ISSA International Awards Committee is now accepting nominations. Write up short descriptions of the achievements of those you believe deserve to be recognized and get them in now. Nominations have begun and all documentation for every nomination must be completed and submitted before December 31, 2006. Please take the time now to honor the people and chapters that make this organization great. If you don't nominate them, we cannot honor them!

Awards include Hall of Fame, Honor Roll, Security Professional of the Year, Chapter Communications Program and many others.

To get all the details and learn how to place a nomination:

<http://www.issa.org/2006awardnom.html>

- Members Only Feature: Print your own Membership Card

In response to member feedback, we have developed a new feature, allowing members to download and print their membership card on demand. Now, if your card gets lost, or you need to show proof of membership for a chapter meeting or any other industry event, your membership card is readily available. Just go online, click, print and laminate. To check out this new feature, go to the members only section using the link below: <http://www.issa.org/members/members.html>

-----  
## Varie ##

>> -----

- DDL Mastella sul riordino delle professioni

Una importante novita' legislativa e' stata recentemente presentata, il DDL Mastella sul riordino delle professioni scaricabile ad esempio da [http://www.ilsole24ore.com/art/SoleOnLine4/Norme%20e%20Tributi/2006/12/n011206\\_cdm\\_professioni.shtml](http://www.ilsole24ore.com/art/SoleOnLine4/Norme%20e%20Tributi/2006/12/n011206_cdm_professioni.shtml)





## AIPSI, Associazione Italiana Professionisti di Sicurezza Informatica

Questo DDL, se trasformato in legge, potrebbe avere delle notevoli conseguenze sulle attività dei professionisti, inclusi i professionisti in sicurezza informatica, e sulle associazioni di professionisti quale AIPSI e per il futuro della certificazione LoCSi di AIPSI. Una discussione al riguardo è già in atto nella mailing list riservata ai soci.

Vista l'importanza dell'argomento, tutti i soci sono invitati ad informarsi e partecipare alla discussione.

### La Business Continuity si occupa solo di disastri?

In un recente Seminario, mi sono state fatte delle domande interessanti sulla Business Continuity.

Avevo accennato che abbiamo or ora terminato, con l'approvazione del Business Continuity Plan da parte del CdA, quanto previsto dalla normativa della Banca d'Italia, ossia l'impianto di misure di continuità finalizzate alla mitigazione dei danni derivanti da eventi catastrofici che possano colpire i processi vitali e altamente critici della banca o di sue controparti rilevanti.

Affermazioni o domande del tipo: "avete quindi terminato", "siete pronti ad affrontare i disastri", "la Business Continuity tratta solo di eventi di coda?", mi hanno fatto molto riflettere. L'affermazione "avete terminato", mi ha fatto pensare per un attimo a quanto fu studiato all'epoca del passaggio all'anno 2000 e all'euro. Furono studiati e predisposti dei piani di emergenza, in caso qualcosa fosse andato a male. Quell'esperienza, validissima, di pianificazione a tavolino di cosa fare in caso di interruzione di un processo aziendale critico, è stato un momento fondamentale, ma è poi terminata, non è proseguita, non è entrata, come dice l'amico Perazzo, nel "DNA delle persone".

Una funzione di Business Continuity, opportunamente collocata, doveva nascere allora (le eventuali eccezioni non fanno che confermare la regola) e diventare pienamente operativa. Per trovare un lavoro così sistematico, di mitigazione del rischio, elaborato congiuntamente dai responsabili dei processi operativi e di business e dalle funzioni di supporto (ICT, Logistica, Sicurezza, ecc.), ci si deve riferire all'attuale progetto, nato a seguito dei noti tragici fatti e sulla base di linee guida emanate dalla Banca Centrale.

Mi domando: quante volte in azienda un piano di mitigazione di un rischio inatteso avrebbe potuto salvare l'immagine della banca ed evitare la perdita di importanti clienti? Mi ricordo di un collega che mi accennava alle conseguenze derivanti dall'interruzione del sistema informativo nel momento di massimo picco nella raccolta delle richieste per un'OPA. Così pure di quella volta che una filiale, non avendo il collegamento TP con il sistema centrale, dovette chiamare la Forza Pubblica per placare gli animi dei dipendenti di un'azienda. In questo caso non fu assunta nessuna azione di emergenza, perché nessuno aveva intenzione di assumersi il rischio di pagare.

"Abbiamo terminato?" Chiaramente no. Inizia ora la fase ciclica di manutenzione dell'impianto. Guai a fermarsi. Perché l'azienda non si ferma (per fortuna).

"La Business Continuity si occupa solo di eventi estremamente rari?"

In questo momento sì. La preoccupazione, lo ricordiamo, è che, a fronte di un disastro ampio e di lunga durata, possano continuare ad operare processi vitali quali il sistema degli incassi e pagamenti, i regolamenti fra banche, ecc.

Di conseguenza, i progetti or ora terminati hanno tenuto conto del fatto che si fronteggiano eventi eccezionali e, quindi, livelli di servizio altrettanto eccezionali possono essere accettati. In casi quali il 9/11, la solidarietà a livello locale, istituzionale, nazionale ed internazionale è stata tale da compensare l'imprevedibilità dell'evento.

Ma la domanda se la "business continuity in azienda si occupa solo di disastri", fa riflettere. Ora che è stata instaurata la funzione di BCM, dotata di idonee risorse, sponsorizzata dal Vertice aziendale, e si è creato un ciclo di gestione e sviluppo, perché non pensare anche ad una sua utilità, che potremmo chiamare "quotidiana", cioè rivolta agli incidenti che hanno una probabilità di accadimento, ossia misurabili? Perché non prevenire interruzioni quali quelle esemplificate in precedenza, stilando dei piani e formalizzando le azioni di mitigazione del rischio e di accettazione di quello residuo?

Come beneficio si avrebbe un ufficio al di sopra delle parti che potrebbe riportare al top management delle proposte operative. Non ultimo, pensiamoci bene, la business continuity vedrebbe nei "process owners" un forte sponsor, specialmente ora che tutti ne hanno apprezzato la qualità e pragmaticità di approccio.

Mi risulta che qualche realtà aziendale abbia già iniziato a procedere in tal senso.

ANSSAIF potrebbe quindi chiamare queste realtà ed i soci ad un seminario da tenersi all'inizio dell'anno per approfondire questa tematica (indicativamente a metà febbraio).

Invito pertanto tutti a fornirci, entro la prima settimana di gennaio, la propria disponibilità ad intervenire con la propria esperienza e le proprie idee al seminario. A.C. Wright

### Considerazioni personali sugli insider's interni - Parte seconda

Abbiamo già detto che 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, specialmente se si tratta di insider interni.

Di contro, nei contesti lavorativi più moderni e sviluppati la valutazione dello "human factor" ha già da diversi anni un ruolo chiave nelle procedure di sicurezza. L'obiettivo in tali ambiti è quello di convincere le persone, al di là delle prescrizioni, ad attuare un comportamento sicuro, facendo leva anche sulla loro sfera motivazionale.

Sul versante della sicurezza informatica e della prevenzione del crimine i fattori maggiormente indagati sono connessi alla percezione del rischio di attacco (per la valutazione delle vulnerabilità dei sistemi di sicurezza legate al fattore umano). Da tali ricerche è emerso che il rispetto di una procedura di sicurezza da parte delle persone si basa su una serie di schemi cognitivi ed atteggiamenti che costituiscono la percezione di rischio.

Oltre a tali fattori occorre ovviamente considerare anche le condizioni di ergonomia della procedura e l'entità del rallentamento del processo lavorativo (alcune misure di sicurezza molto lunghe e complesse possono rappresentare un fastidio eccessivo per l'operatore). Ogni misura di sicurezza da rispettare costituisce infatti spesso una nuova dinamica da inserire nel processo di lavoro, in pratica una nuovo compito che l'operatore deve aggiungere al suo normale lavoro e tale inserimento deve essere "digerito" da tutti.

Normalmente le fasi critiche nell'applicazione di una operazione di security informatica sono due: la prima fase si manifesta all'inizio, con l'introduzione della nuova prescrizione, quando le persone devono abituarsi alla novità e devono quindi superare le fisiologiche rigidità all'innovazione; la seconda fase critica si manifesta invece dopo un certo periodo di tempo, quando l'abitudine alla routine e l'assenza di incidenti che "legittimano" la misura precedentemente adottata abbassano l'attenzione e inducono al non rispetto della procedura di sicurezza in questione.

Per tale motivo, ANSSAIF, partendo dal presupposto che dietro ad ogni tecnologia di sicurezza c'è una persona che deve utilizzarla, ritiene che anche la psicologia umana sia un fattore che deve essere considerato da chi progetta e gestisce la sicurezza informatica.

Ecco quindi il perché della collaborazione con il socio ICAA (International Crime Analysis Association), finalizzato a predisporre ed utilizzare strumenti predisposti allo scopo con l'obiettivo di misurare i livelli di "preparazione psicologica" rispetto alla sicurezza informatica all'interno delle aziende utilizzando appositi strumenti. Uno di questi è il PRA (Psychological Risk Assessment), strumento realizzato dall'ICAA che valuta il livello di percezione del rischio di attacco informatico (interno ed esterno) e la diffusione di atteggiamenti e comportamenti potenzialmente facilitanti gli attacchi.

La somministrazione di questo strumento è preceduta da una fase di osservazione dell'organizzazione al fine di individuare alcune esigenze specifiche. I ricercatori effettuano, prima dell'intervento, un breve colloquio con la dirigenza aziendale e con i responsabili della sicurezza per rilevare alcuni possibili "punti deboli" da misurare. I questionari utilizzati vengono somministrati ad un campione rappresentativo dell'azienda (di ampiezza variabile) e sono assolutamente anonimi. In aggiunta ai questionari vengono impiegate delle brevi interviste semistrutturate ai responsabili della sicurezza. Lo strumento PRA consente di evidenziare aree di rischio per quanto riguarda il fattore umano nell'ambito del processo di sicurezza informatica delle organizzazioni pubbliche e private. Il tempo di somministrazione dello strumento è estremamente breve (circa 20 minuti) e l'analisi dei dati ottenuti consente la realizzazione di un report molto efficace sullo stato della sicurezza della specifica organizzazione legato al "fattore umano" e di progettare un intervento correttivo basato su elementi di rischio realmente presenti nello specifico contesto di intervento.

Chi fosse interessato ad approfondire l'argomento può scrivere a [antonio.caricato@anssaif.it](mailto:antonio.caricato@anssaif.it) (A. Caricato - ANSSAIF)

### **Perché non ci sono più attacchi massicci di virus?**

Vi ricordate i tempi di NIMDA, CODE RED, GAOBOT, e così via? Perché non si bloccano più le aziende? Perché milioni di computer non si fermano più, tutti assieme, un dato giorno? Ci sono tanti virus, tanti computer ogni giorno si bloccano, ma non è un attacco preoccupante. Almeno come in passato.

I giornali ne parlano poco. I possessori di computer dormono sonni tranquilli. Sono convinti di essere protetti. Lo sono veramente? Hanno l'ultima versione dell'antivirus? Siamo certi?

Una nostra indagine ha rivelato che su 100 utenti che hanno a casa il personal computer, tutti hanno un antivirus, ma solo il 45% si ricorda di quando ha scaricato l'ultimo aggiornamento! Il 5% è caduto dalle nuvole ed ha chiesto addirittura spiegazioni!

Hanno tutti un personal firewall attivato? Sono state inserite delle regole per impedire l'uscita dal pc di informazioni personali? Il 75% ha risposto di no.

Allora una domanda viene spontanea: non è che questa apparente "tranquillità" sta progressivamente indebolendo le difese? Non delle aziende, ma bensì di coloro che utilizzano il computer a casa, dove tengono dati personali e da dove

## ESTRATTO DELLA NEWSLETTER ANSSAIF



fanno transazioni su Internet.

Abbiamo accennato tempo fa alla nostra preoccupazione: non si sta preparando un attacco massiccio? Correggiamo la domanda: non è che criminali (non trascurando i terroristi) stanno installando "trojans" sui computer e da lì si preparano a prelevare dati o ad attaccare le aziende? Milioni di computer potrebbero diventare dei temibili nemici.

Ecco allora l'invito nuovamente ai *media*: sensibilizzate, nel dovuto modo, i consumatori.

Come il Cliente aggiunge l'olio al motore per evitare di perdere l'auto ed i soldi, così aggiunga sicurezza al computer.

Ne basta poca: quella suggerita dal venditore o dal negoziante sotto casa. Nulla di più.

Noi chiaramente siamo sempre disponibili a fornire informazioni ed aiuto.