



► RACCOLTA DEI NOTIZIARI
SETTIMANALI REDATTI DAL
GARANTE PER LA PROTEZIONE
DEI DATI PERSONALI..... 9



► CLUSIT INFORMA..... 11



► Newsletter AIPSI.....15
► Newsletter ANSSAIF.....18

○ FEBBRAIO | ○ 2007

IS Audit *focus*



La Newsletter di AIEA

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

Febbraio 2007

Il nuovo consiglio direttivo

Finite le operazioni di voto ed eletti i consiglieri per il triennio 2007-2009, il primo impegno è stato quello di eleggere le cariche associative, relative a:

- Presidente
- Vice Presidente 1
- Vice Presidente 2
- Segretario
- Tesoriere

Proseguendo quanto già avviato negli anni scorsi, ed in analogia a quanto già in uso presso ISACA, ad ogni consigliere è stato confermato/attribuito uno specifico ruolo. Le cariche ed i ruoli sono di seguito dettagliati.

Accanto alla definizione in italiano, sono riportate le definizioni in inglese, in analogia ai ruoli previsti da ISACA

Nome	Carica Associativa	Riferimento ISACA
BOLLI	Responsabile relazioni con Università'	Director Academic Relations
CECCARELLI	Responsabile "Percorsi formativi"	Education Chair
CELLINO	Tesoriere	Treasurer
DATTOLI	Percorsi formativi	Education Support
DELLEPIANE	Segretario	Secretary
GALLI	Responsabile relazioni con Associati	Director Membership
NARDUZZO	Vice Presidente - Responsabile IT Governance / COBIT	Vice president - Director IT Governance / COBIT
ONGETTA	Presidente	President
RODARO	Responsabile Certificazione CISA / CISM	Director CISA / CISM Certification
ROSA	Responsabile Comunicazione e promozione/ Edizione Newsletter	Director Marketing /Director Communications/Newsletter Editor
TOFFANIN	Vice Presidente Responsabile relazioni con i revisori	Vice President - Certified Publics Accountants Relations

Un augurio di buon lavoro a tutto il Consiglio!



Associazione Italiana
Information Systems Auditors





AIEA partecipa 1

IL 25 gennaio, il nostro Presidente ha partecipato all'evento "Identity e access management: un approccio organizzativo e metodologico", organizzato da AUSED. Il tema dell'evento è descritto qui di seguito:

La pervasività delle ICT e l'uso a volte incontrollato di queste tecnologie, pone seri problemi di sicurezza delle informazioni, sia quelle che interessano la sfera privata degli individui, sia quelle vitali per la continuità dei business aziendali. I rilievi statistici rilevano che l'uso fraudolento dei sistemi informativi è in maggior parte eseguito dall'interno delle organizzazioni. Le aziende sono, pertanto, impegnate non solo a proteggere il proprio patrimonio informativo da attacchi esterni, ma anche a garantire la sicurezza del sistema informativo, identificando con certezza gli utenti che interagiscono nei processi, attribuendo consapevoli autorizzazioni.

Con 'Identity e access management' (IAM) viene indicato il processo di impiego di policy, di regole organizzative e tecnologie indirizzate a gestire le informazioni riguardanti l'identificazione degli utilizzatori di un S.I. e le autorizzazioni agli accessi sia logici che fisici.

Per la presentazione e lo sviluppo di questi temi, Aused organizza un incontro così articolato:

1. L'approccio metodologico al progetto IAM;
2. L'impatto organizzativo;
3. Il work flow generativo rivolto alle risorse umane e ai processi.

AIEA partecipa 2

Alcuni soci (Francesco Ceccarelli e Natale Prampolini) hanno partecipato all'E-Security lab che si è svolto, a Milano, il 24 ed il 25 gennaio scorso.

La conferenza ha avuto come tema:

"Security Information Management, Identity Management e Threat Management per governare la sicurezza IT a tutela dell'impresa e nel rispetto delle leggi "

AIEA partecipa 3

Al via la seconda edizione del CISCO Expo: un appuntamento (Milano, 7 e 8 marzo) da non perdere nel corso del quale rappresentanti dell'industria e delle istituzioni si confronteranno sui temi della produttività, del cambiamento e dell'innovazione, in un Paese aggiornato al presente e pronto al futuro: L'Italia 2.0. Per maggiori informazioni sull'evento visitare il sito: www.ciscoexpo.it

AIEA ha patrocinato, insieme ad altre Associazioni, l'evento CISCO.

Hanno parlato di AIEA

ComputerWorld - 22 gennaio 2007: l'intera penultima pagina è stata dedicata ad AIEA, descrivendone missione ed attività. Di seguito, l'immagine dell'articolo dedicato ad AIEA.

AIEA, per l'auditing dei sistemi informativi

Le iniziative 2007 dell'associazione italiana

AIEA è l'Associazione Italiana Information Systems Auditors. I soci sono attualmente circa 550, presenti in tutto il territorio italiano e operano sia in grandi aziende finanziarie, commerciali, industriali e di consulenza, sia in istituzioni pubbliche, sia come singoli professionisti. Gli stessi soci aderiscono a un codice etico, partecipano ai numerosi eventi, organizzati direttamente da AIEA o patrocinati da AIEA, in collaborazione con università o enti di studio e ricerca.

Molti soci sono parte attiva in gruppi di ricerca su temi diversi (sicurezza, certificazione, controllo...) che talora coinvolgono anche le autorità competenti.

AIEA è anche il primo capitolo europeo dell'ISACA - Information Systems Audit and Control Association -, associazione internazionale che promuove la cultura sulla governance e sull'auditing dei sistemi informativi e che certifica, sotto accreditamento ANSI-RAB (USA), le figure professionali dei CISA - Certified Information Systems Auditor - e dei CISM - Certified Information Security Manager.

Nel 2007 AIEA, proseguendo nell'attuazione di iniziative volte al processo di miglioramento, formazione e informazione dei propri associati, ha messo in calendario un percorso formativo che prevede numerose attività.

Nel primo semestre, in particolare, è prevista la seconda edizione del Corso Base IS Audit, che sarà tenuto a Roma nei giorni dal 12 al 16 febbraio 2007. Sempre a febbraio inizieranno i corsi Cobit, sia base che avanzato. Nelle settimane successive saranno avviati i corsi di preparazione all'esame CISA e CISM, che saranno tenuti a Milano, Torino e Roma.

Oltre a tali attività, AIEA ha iniziato l'organizzazione del convegno annuale, previsto nei giorni 24 e 25 maggio 2007.

Il convegno annuale è l'oc-

casione, per i soci, di incontro e di aggiornamento su quelli che sono la professione e gli scenari di riferimento. Relatori italiani ed esteri porteranno le loro testimonianze e i loro contributi nel difficile campo della governance e dell'auditing dei sistemi informativi.

Per maggiori informazioni sul percorso formativo: aiea@aiea.it [cwi]

A tutela della professione

AIEA esercita un ruolo di filtro e di tutela della professione di auditor IT, nella forma di un controllo del rispetto del codice di etica e dei requisiti minimi di esperienza e di continuità nella professione. L'associazione ritiene fondamentale che nelle imprese il processo di governo dell'IT sia regolamentato a livello di professione, al fine di identificare e qualificare gli operatori che possiedono i requisiti necessari. Per le società di consulenza e i professionisti, d'altra parte, è necessario un riconoscimento della professione che ufficializzi e renda pubblico il quadro delle caratteristiche per l'esercizio di incarichi di consulenza di direzione.

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 Corso CISA Milano	
5			Corso Base IS Audit Roma		Corso CISM Milano Corso CISM Roma Termine Corso CISA Milano	Workshop COBIT
6			Corso Base IS Audit Roma	Corso CISA Torino		
7			Corso Base IS Audit Roma	Corso CISA Torino		
8		Sessione di Studio Torino	Corso Base IS Audit Roma Sessione di Studio Roma			
9			Corso IS Audit Roma 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				Termine Corso CISA Roma Termine Corso CISA Torino	
13				Corso CISA Milano Corso CISA Roma		
14				Corso CISA Milano Corso CISA Roma		
15						
16			Corso CISA Milano			
17			Corso CISA Milano	Sessione di Studio Torino		
18					Corso CISM Milano Corso CISM Roma	
19				Sessione di Studio Milano Sessione di Studio Roma	Termine Corso CISM Milano Termine Corso CISM Roma	
20		Corso COBIT base Milano	Corso COBIT Avanzato Milano	Corso CISM Milano Corso CISM Roma Corso CISA Torino		
21		Corso COBIT base Milano	Corso COBIT Avanzato Milano	Corso CISM Milano Corso CISM Roma Corso CISA Torino		
22						
23			Corso CISA Roma Corso CISA Torino			
24			Corso CISA Roma Corso CISA Torino		XXI CONVEGNO	
25					XXI CONVEGNO	
26						
27		Sessione di Studio Milano		Corso CISA Roma		
28			Sessione di Studio Milano	Corso CISA Roma		Sessione di Studio Torino
29						
30			Corso CISA Milano			
31	Sessione di Studio Roma		Corso CISA Milano			



Calendario Eventi

2° SEMESTRE 2007

2° SEMESTRE 2007



Al servizio dei professionisti dell'IT Governance

Capitolo di Milano

	Settembre	Ottobre	Novembre	Dicembre
1				Termine Corso CISM Milano
2		Corso CISA Roma		
3		Sessione di Studio Milano Corso CISA Roma		
4		Sessione di Studio Roma		
5				
6				
7			Sessione di Studio Milano	
8			Sessione di Studio Roma	
9			Corso CISA Milano Corso CISA Roma	
10			Corso CISA Milano Corso CISA Roma	
11				
12		Corso CISA Milano		Sessione di Studio Milano
13		Corso CISA Milano	Sessione di Studio Veneto	Sessione di Studio Roma
14				
15				
16		Corso CISA Roma	Corso CISM Milano	
17		Corso CISA Roma	Corso CISM Milano	
18				
19		Inizio Corso CISM Milano		
20		Corso CISM Milano	Corso COBIT 4.0 avanzato Roma	
21	Inizio Corso CISA Roma		Corso COBIT 4.0 avanzato Roma	
22	Corso CISA Roma			
23		Corso COBIT 4.0 base Roma	Corso CISA Milano Corso CISA Roma	
24		Corso COBIT 4.0 base Roma	Termine Corso CISA Milano Termine Corso CISA Roma	
25		Sessione di Studio Torino		
26		Corso CISA Milano		
27		Corso CISA Milano		
28	Inizio Corso CISA Milano			
29	Corso CISA Milano			
30			Corso CISM Milano	
31				

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

Percorsi formativi

Il **Corso Base IS Audit** sarà tenuto a Roma, dal 5 al 9 marzo 2007.
Sul sito AIEA è disponibile la locandina completa del corso di Roma.



Relativamente al **Corso COBIT 4.0**, programmato a Milano, le date da ricordare sono:

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

A Roma, il **Corso COBIT 4.0** è in programma nelle seguenti date:

Corso COBIT 4.0 BASE: 23- 24 ottobre 2007
Corso COBIT 4.0 AVANZATO: 20- 21 novembre 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
CISA	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
CISM	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	

Ricordiamo che l'iscrizione all'esame CISA-CISM è possibile già dallo scorso 8 novembre 2006 e che l'early bird con i relativi benefici economici si è chiuso il 14.2 .2007

La data ultima per iscriversi è l'11 aprile 2007

Ricordiamo, anche, che la **data dell'esame è il 9 giugno 2007**

Per la **sessione invernale**, del prossimo dicembre 2007, le corrispondenti date sono:

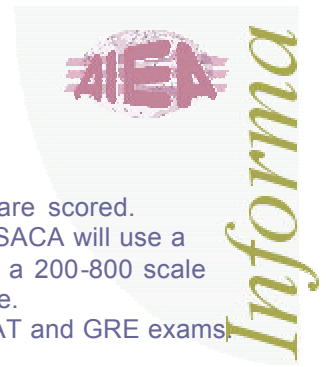
- Inizio iscrizioni: 15 agosto
- Data ultima per l'iscrizione: 26 settembre
- Esame 8 dicembre 2007

Il corso CISA/CISM, di preparazione all'esame di dicembre è programmato nei giorni:

	Domini	Sede di Milano	Sede di Roma
CISA	1 e 2	28 e 29 sett	21 e 22 sett
	3	12 e 13 ott	2 e 3 ott
	4	26 e 27 ott	16 e 17 ott
	5	9 e 10 nov	9 e 10 nov
	6 ed esame	23 e 24 nov	23 e 24 nov
CISM	1 e 2	19 e 20 ottobre	
	3 e 4	16 e 17 novembre	
	5 e test	30 novembre e 1 dicembre	

ISACA sta, in questi giorni, inviando i risultati dell'esame di dicembre 2006 CISA-CISM

Sollecitiamo tutti i soci interessati a verificare che i loro indirizzo e-mail, comunicato all'atto della iscrizione all'esame, sia uguale a quello attuale
Per evitare spamming, ISACA chiede di mettere nella white list : certification@isaca.org



Riportiamo le modifiche apportate, da ISACA, allo scoring dell'esame CISA-CISM:

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.

Riceviamo da ISACA

Ecco il testo di una mail ricevuta:

Sent: Monday, January 15, 2007 4:11 PM

Subject: CISA Item Writing Workshop

ATTENTION ALL CISA ITEM WRITERS – SUBMISSION DEADLINE 2 February, 2007

ISACA is proud to announce that the US Department of Defense (DoD) 8570.01-M “Information Assurance Workforce Improvement Program” manual names the CISA certification among those approved for DoD information assurance (IA) professionals.

Please visit www.isaca.org for details regarding this appointment.

Avviso ai soci 1

Per la stesura della Newsletter e per la predisposizione del notiziario InfoAIEA, stiamo cercando soci disposti a collaborare. L'idea è di mettere in piedi un “Comitato di redazione” che collabori alla messa a punto dei nostri due documenti. Chi fosse interessato è pregato rivolgersi in segreteria.

Bibliografia

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

Vi informiamo che sul sito 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



- FAX INDESIDERATI E PRIVACY
- USA: VERSO UN'AUTORITÀ FEDERALE PER LA PRIVACY

Fax indesiderati e privacy

Il Garante vieta ad una società l'uso della banca dati

Nuovo duro intervento del Garante contro l'invio di messaggi pubblicitari indesiderati. L'Autorità ha vietato l'uso di una banca dati ad un consorzio che pubblicizzava via fax servizi e iniziative a studi di consulenza per il settore del trasporto senza il consenso dei destinatari. La società sanzionata, che ha continuato questa attività illecita nonostante avesse dichiarato in fase istruttoria di averla cessata, non potrà più utilizzare i dati contenuti nel proprio data base. Al provvedimento di divieto si è giunti a seguito della segnalazione di alcuni studi di consulenza che lamentavano la ricezione di numerosi fax indesiderati. Segnalazione divenuta necessaria viste le ripetute e inutili richieste rivolte al consorzio affinché cessasse gli invii pubblicitari. Nel definire il procedimento il Garante ha ribadito i principi, più volte affermati, ai quali attenersi per un corretto uso dei dati personali nel settore del marketing telefonico. E' bene ricordare, infatti, che è possibile inviare fax o effettuare telefonate per effettuare ricerche di mercato, promozioni o comunicazioni commerciali, vendite dirette, pubblicità o altro materiale di carattere commerciale solo dopo aver ottenuto il preventivo e esplicito consenso del destinatario, anche se il numero telefonico compare in un elenco cosiddetto pubblico o viene reperito in Internet. L'intervento del Garante nei confronti del consorzio è solo l'ultimo di una lunga serie di iniziative, accertamenti, ispezioni, sanzioni amministrative avviate per contrastare il fenomeno delle comunicazioni pubblicitarie indesiderate. Sempre sul fronte fax indesiderati l'Autorità ha confermato un provvedimento di blocco di una banca dati di una società con oltre tre milioni di nominativi, disposto nel marzo 2006.

Usa: verso un'Autorità federale per la privacy

Il Congresso degli Usa ha approvato un disegno di legge che prevede l'istituzione di un'Autorità federale indipendente per la tutela della privacy e delle libertà civili, con il compito di vigilare sulle attività degli organismi federali collegate alla lotta al terrorismo. Il disegno di legge dovrà essere approvato anche dal Senato, ma si tratta comunque di un passo importante che potrebbe facilitare i rapporti transatlantici nel settore della protezione dei dati soprattutto rispetto alle attività di cooperazione giudiziaria e di polizia. Il disegno di legge approvato la scorsa settimana dal Congresso degli Stati Uniti (http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h1eh.txt.pdf) prevede alcune modifiche a disposizioni attualmente in vigore che sono finalizzate a contrastare il terrorismo internazionale; nell'ambito di questo pacchetto sono state inserite anche norme relative all'istituzione ed al potenziamento di un'Autorità indipendente (definita "Privacy and Civil Liberties Oversight Board") che dovrà garantire il rispetto della privacy e delle "libertà civili" previste dalla Costituzione americana da parte delle varie agenzie operanti nel campo della lotta al terrorismo. Questo organismo indipendente avrà cinque membri nominati dal Presidente su indicazione e con il consenso del Senato, in base alle rispettive qualifiche professionali, all'esperienza maturata nel settore della privacy e delle libertà civili, ai riconoscimenti pubblici ottenuti, senza riguardo all'affiliazione politica (ma con la garanzia che non più di tre appartengano allo stesso partito). I cinque membri rimarranno in carica per sei anni. Il Board avrà il potere, anche attraverso ordinanze ingiuntive (*subpoenas*), di chiedere a chiunque (compreso il Department for Homeland Security, che coordina le attività antiterrorismo ed è responsabile di numerosi programmi fra cui la gestione dei dati Pnr) di fornire informazioni, documentazione o altro materiale pertinente. Il Board dovrà riferire regolarmente al Congresso ed alle commissioni competenti (a intervalli non inferiori a sei mesi) sulle attività svolte, sulle risultanze delle indagini condotte,

su proposte o raccomandazioni in materia. Le relazioni semestrali saranno parzialmente rese pubbliche e vi sarà spazio anche per audizioni pubbliche.

Interessante è il fatto che il disegno di legge preveda la nomina di una sorta di “incaricati per la protezione dei dati” presso le singole agenzie federali ed i ministeri competenti (tesoro, sanità, giustizia, Homeland Security, Cia) che avranno il compito di vigilare sull’applicazione della normativa e sul rispetto della privacy – non soltanto per quanto riguarda l’introduzione e l’applicazione di norme in materia di lotta al terrorismo, ma anche rispetto alla prassi quotidiana delle agenzie e dei ministeri (che dovranno garantire ai singoli la possibilità di presentare ricorsi o segnalazioni per presunte violazioni della privacy o delle libertà civili). Viene affermato con chiarezza il principio per cui i poteri, anche speciali, concessi per garantire la sicurezza nazionale devono essere bilanciati nell’ottica di tutelare privacy e libertà civili. E’ indubbia la volontà del Congresso Usa di rafforzare i poteri di indagine e controllo poiché la tutela della privacy a livello federale verrebbe estesa a “chiunque” e non più soltanto ai diritti dei consumatori (che oggi ricadono nelle competenze della Federal Trade Commission) o dei pazienti (tutelati da legislazione federale ad-hoc che protegge i dati sanitari di degenti e pazienti).

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

Estratto della Newsletter di gennaio 2007

1. LA PROTEZIONE DI RETI E SISTEMI DI CONTROLLO ED AUTOMAZIONE NEGLI IMPIANTI DI PRODUZIONE

Proteggere i sistemi informatici e le informazioni da essi generate o elaborate è divenuto critico in ogni attività, è può esserlo ancora di più nel settore industriale e delle infrastrutture ove sono ampiamente utilizzati reti e sistemi di controllo e supervisione.

I danni che possono provocare incidenti ai sistemi di controllo a volte possono essere altamente pericolosi ed avere conseguenze molto gravi anche per l'impianto stesso, l'ambiente, persone e cose.

Pensiamo (solo per ipotesi, naturalmente) ai danni indotti da un incidente in una centrale nucleare, o alle conseguenze derivanti da un black-out elettrico, da un blocco delle comunicazioni telefoniche, in un aeroporto, oppure ad un problema in una fabbrica chimica, in raffineria o in un impianto di controllo di una diga, in un depuratore o in un acquedotto, e ancora in un nodo ferroviario, una fonderia o un ospedale.

I sistemi informatici, con l'avanzare della tecnologia, sono ormai ampiamente diffusi e controllano e supervisionano impianti ed edifici ovunque.

Bisogna anche pensare che proteggere un sistema di automazione di fabbrica o di controllo di processo spesso può anche essere più difficoltoso di altri sistemi, per vincoli tecnologici e operativi. Minacce e vulnerabilità alle quali sono esposti questi sistemi a volta sono addirittura sconosciute e molto diverse da quelle in cui tradizionalmente sono incorse banche ed aziende in genere. Spesso errori degli operatori, incuria, sabotaggio ed altro sono eventi che provengono dall'interno, ma la schiera dei malintenzionati può includere anche eventi ed agenti esterni (come riportato dalla stampa) e purtroppo anche terroristi (come appurato anche da CIA, FBI e dalla stessa Casa Bianca).

Come per tutte le attività che hanno rischi insiti, è necessario "pensarci prima".

Ci possono essere diversi approcci per affrontare il problema.

Le considerazioni dalle quali bisogna partire sono però le seguenti :

- un sistema non potrà mai essere sicuro al 100%
- un sistema "sicuro" ora, potrà non esserlo più domani o tra un'ora
- la sicurezza non è un prodotto confezionato, è un processo, un modo di pensare
- i problemi di sicurezza non si risolvono solo con la tecnologia
- i comportamenti delle persone sono la parte preponderante per rendere sicuro un sistema

Alcune norme ci possono aiutare a decidere quali sono le migliori politiche per la sicurezza dei sistemi e delle informazioni, a definire rischi, minacce e vulnerabilità e identificare quali sono i controlli e le contromisure da adottare.

Clusit ha deciso di approfondire il tema della protezione di reti e sistemi di controllo, promuovendo la pubblicazione di un Quaderno, che sarà scritto dal socio Enzo Maria Tieghi e potrà essere disponibile nel corso del prossimo mese di marzo.

2 . CYBERCRIME

Aumentano gli "spyware".

Avevamo ribadito, anche nella Newsletter di dicembre 2006, la nostra preoccupazione per un aumento di programmi "malvagi" (c.d."malware" e "spyware") sui personal computer dei Consumatori e di piccole aziende.

In questo mese, che è trascorso, abbiamo avuto altri riscontri e, fra questi, abbiamo raccolto un'informazione riguardante un crescente interesse - da parte di varie fonti, certamente non lecite - nell'acquisto di software "malevolo". Dato che questa notizia è uscita dall'"underground", vuol dire che il sistema dei software "spioni" piace, e molto.

Ricordiamo che parliamo di un sistema consistente nel far memorizzare un software sui pc di ignari cittadini, ai fini di catturare utili informazioni dai file contenuti sui dischi e da quanto digitato sulla tastiera.

Se è vero che il sistema è nato per conoscere le abitudini e le preferenze dei Consumatori, è anche vero che è utilissimo ai criminali, e, perché no, ai terroristi.

E' già accaduto che alcuni computer, "innocenti", sono serviti per lanciare degli attacchi a siti di aziende nemiche, in quanto appartenenti ad ideologie, religioni, ecc. non condivise. Siccome una domanda crescente non può che far aumentare l'offerta, ci dobbiamo attendere una recrudescenza su questo campo.

Su questo tema, che meriterebbe ben più di quattro righe, dobbiamo segnalare alcuni articoli usciti questa settimana.

Il primo accenna alla presenza di pc "zombi", pronti quindi ad agire ad un comando da remoto. Su [quotidiano.net](http://qn.quotidiano.net) e su altri giornali si può trovare trattato questo tema:

<http://qn.quotidiano.net/chan/tecnologia:5454941:/2007/01/14:>

Il secondo, dal titolo "quando il virus diminuisce, phishing e spam festeggiano", tende a dare una spiegazione - supportata da dati - sul perché si è vista una diminuzione nella "cattiveria" di attacco dei virus.

MessageLabs lo giustifica, come dice il titolo, dalla necessità - per i criminali - di attirare i Consumatori nelle trappole connesse alle email con titoli allettanti o che sembrano provenire da aziende o Enti conosciuti, e con i quali si ha un rapporto cliente-fornitore.

Appunto le spam e le email di phishing.

Per maggiori informazioni:

www.vnunet.it/it/vnunet/article/2007/01/22/strategie-sempre-pi-complesse

A proposito di titoli allettanti, possiamo citare il recente caso - segnalato da Symantec - delle email riportanti il titolo "230 morti a causa della tempesta che ha colpito l'Europa".

Una volta aperto l'allegato (un videoclip), il computer viene infettato dal Trojan Peacomm, il quale cercherà di connettersi a un indirizzo remoto

ed usare il computer infetto per inviare un alto numero di messaggi spam.

Per maggiori informazioni consultare la pagina:

www.agi.it/oggi-in-italia/notizie/200701232034-cro-rt11289-art.html

La **Polizia di Stato** ha realizzato facili istruzioni per i Consumatori.

Suggeriamo di accedere al sito:

www.poliziadistato.it/pds/cittadino/consigli/internet.htm

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

3. INFOSECURITY ITALIA 2007

Dal 6 all'8 febbraio prossimo si terrà la settima edizione di Infosecurity Italia, alla Fiera di Milano. Anche quest'anno il CLUSIT ha contribuito in maniera significativa all'organizzazione della parte convegnistica.

Il programma definitivo dei convegni e delle iniziative collaterali Clusit è disponibile su www.clusit.it/infosecurity2007/infosecMI07.pdf

Tutti i convegni sono a partecipazione libera e gratuita.

Per partecipare ai seminari Clusit, gratuiti per i soci, è necessario seguire la procedura di registrazione su <https://edu.clusit.it/>.

Troverete tutte le informazioni utili su Infosecurity Italia 2007 all'indirizzo www.infosecurity.it/.

Durante i tre giorni della manifestazione, tutto lo staff del Clusit sarà presente allo Stand C29 (Pad. 17/2)

4. PREMIAZIONE DELLE MIGLIORI TESI IN SICUREZZA INFORMATICA

Il 7 febbraio alle 12.00 circa nell'ambito di Infosecurity, al termine del convegno di presentazione dell'Hacker's Profiling Project, verrà premiata la migliore tesi in Sicurezza Informatica. Il primo premio della seconda edizione di 'Innovare la sicurezza delle Informazioni' consiste in 2.000,00 euro. Il secondo classificato potrà invece partecipare gratuitamente ad un corso per Lead Auditor ISO IEC 27001 (BS7799:2) del valore di 1.600 € (oltre IVA). Inoltre i primi 5 classificati avranno l'adesione gratuita al Clusit per il 2007.

La valutazione delle tesi inviate è stata effettuata da una commissione composta da membri del comitato direttivo, dal comitato tecnico scientifico e da soci CLUSIT, sia del mondo accademico che industriale. Gli elaborati sono stati valutati per l'innovatività dell'argomento trattato, la complessità dell'attività svolta, il livello di conoscenza dimostrato e l'utilizzabilità dei risultati raggiunti.

Il numero dei partecipanti quest'anno è aumentato del 18% rispetto alla precedente edizione e si è ampliato anche il numero degli atenei di provenienza, con cinque nuovi inserimenti. Le tesi che hanno partecipato al premio provengono da Politecnico di Torino, Ca' Foscari di Venezia Università Cattolica, sede di Brescia, Università degli Studi di Milano Statale, Università degli Studi di Torino, Università di Cagliari, Università degli Studi di Firenze, Università di Padova, Università degli Studi di Modena e Reggio Emilia, Roma Tre, Politecnico di Milano, Università di Bologna, Università dell'Aquila, Università degli Studi

dell'Insubria, Varese, La Sapienza di Roma, Politecnico delle Marche, Università degli Studi di Siena, Università degli studi di Milano Bicocca, Università degli Studi di Messina.

Il premio è stato sponsorizzato da:



ed è concepito come un'occasione di scambio tra mondo produttivo e mondo scientifico, tra studenti e mondo del lavoro.

5. NOTIZIE DAI SOCI

Il progetto internazionale OWASP ha recentemente pubblicato la nuova Testing Guide v2 che rappresenta una metodologia per l'audit di sicurezza degli applicativi web.

Tale documento è il risultato di uno sforzo di quasi 4 anni da parte della comunità OWASP con il contributo di oltre 50 professionisti di tutto il mondo.

Il progetto è stato affidato a Matteo Meucci (Fondatore e Chair del capitolo italiano del progetto) che grazie al supporto di altri 10 membri italiani è riuscito a spostare il baricentro di un progetto internazionale dagli Stati Uniti all'Italia.

La guida rappresenta la prima metodologia per la verifica di sicurezza degli applicativi ed è liberamente distribuita on-line con lo scopo di diventare lo standard "de-facto" nel mondo della web security industry.

E' possibile prendere visione della nuova guida direttamente on-line:
www.owasp.org/index.php/OWASP_Testing_Guide_v2_Table_of_Content

oppure leggerla in formato pdf o doc:
www.owasp.org/index.php/Testing_Guide

CLUSIT
ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA*
Dipartimento di Informatica e Comunicazione
Università degli Studi di Milano
Via Comelico 39 - 20135 MILANO - cell. 347.2319285

* associazione senza fini di lucro, costituita il 4 luglio 2000

© 2007 Clusit - Vietata la riproduzione
Clausola di esclusione della responsabilità e informazioni relative al
Copyright: www.clusit.it/disclaimer.htm

~~~~~

**ESTRATTO DALLA NEWSLETTER AIPSI DI GENNAIO 2007:**

-----

## Eventi con la partecipazione di AIPSI ##

-----

- IDC Security Conference, Milano, 21 e 22 Febbraio 2007

AIPSI e' lieta di annunciare la propria partecipazione ad IDC Security Conference - Sicurezza 2.0: Security in a convergent world, che si terrà a Milano presso il Milan Marriott Hotel il 21 e 22 Febbraio 2007.

Marco Misitano, Communication Officer della Associazione sara' il chairman della sessione "Sicurezza nelle comunicazioni integrate, reti innovative e requisiti di sicurezza"

Attraverso Sessioni plenarie e parallele, tavole rotonde, keynote speakers di livello internazionale e il confronto con le aziende, i Partecipanti di Security Conference 2007 potranno cogliere indirizzi, trend, indicazioni necessari per portare le loro organizzazioni agli standard qualitativi richiesti dalle iniziative di IT.

AIPSI inoltre e' fra le associazioni patrocinanti dell'evento.

Per maggiori informazioni:

<http://www.idc.com/italy/events/security07/security07.jsp>

- CiscoExpo (Milano, 7 e 8 Marzo 2007)

AIPSI sara' fra le associazioni che aderiscono a CiscoExpo. La manifestazione si svolgera' a Milano i giorni 7 ed 8 marzo 2007. AIPSI sara' presente con una propria area espositiva, dove potrete richiedere qualsiasi informazione.

Durante la manifestazione, AIPSI terra' uno dei propri "Security Talk Show " con rinfresco finale, aperto a tutti. Un'eccellente occasione per conoscersi, scambiare opinioni e... per un brindisi al tardo pomeriggio. Vi invitiamo a passare a trovarci ed a segnalare l'opportunita' ai vostri conoscenti e collaboratori. Informazioni piu' dettagliate nella prossima newsletter e presto anche su:

[www.ciscoexpo.it](http://www.ciscoexpo.it) e [www.aipsi.org](http://www.aipsi.org).

Per adesso tenete a mente la data del 7 ed 8 marzo!

-----

## ISSA News ##

-----

- ISSA Webcast

ISSA's latest On Demand Webcast "What is Deep Network Forensics?" is available now at <http://viavid.net/dce.aspx?sid=000039E3>

I Webcast di ISSA sono disponibili su

<http://www.issa.org/current-webcast.html> a partire dalla data indicata.

- ISSA Journal

AIPSI, Associazione Italiana Professionisti di Sicurezza Informatica

Estratto dalla Newsletter AIPSI numero 8, 16 Febbraio 2007

Disponibile in PDF all'indirizzo

[http://www.aipsi.org/newsletter/Aipsi\\_NewsLetter-8-2007\\_2.pdf](http://www.aipsi.org/newsletter/Aipsi_NewsLetter-8-2007_2.pdf)

~~~~~

--
In Primo Piano ##

--

- Security Talk il 7 Marzo 2007 a CiscoExpo

Security Talk: Le certificazioni professionali in sicurezza informatica
Il 7 Marzo, all'interno della manifestazione Cisco Expo, AIPSI terrà uno
Dei suoi security Talk Show. Un Moderatore esplorerà un punto di vista sulle
certificazioni indipendenti, sulle certificazioni rilasciate dai vendor,
sulla offerta universitaria ed il punto di vista di chi si occupa di selezione
del personale. Quattro opinioni a confronto, una forte interazione del
pubblico, per un frizzante momento di confronto ed orientamento con il
tradizionale aperitivo finale, saranno gli ingredienti di questa puntata della
consolidata formula di incontro fra soci e non solo.

Il Security Talk sarà infatti all'interno della manifestazione Cisco
Expo, AIPSI ringrazia Cisco per l'ospitalità e la massima autonomia concessa
all'associazione.

Maggiori dettagli su www.aipsi.org!

--
Eventi con la partecipazione di AIPSI ##

--

- Incontro di studio "Tecnologia e attività di indagine dal
cyberterrorismo alla computer forensics", Varenna (Lecco), 16 febbraio 2007, Villa
Monastero

La Camera Informatica Lariana in collaborazione con VP TECH e NOVA
SYSTEMS ROMA e con il Patrocinio di IISFA - "International Information Systems
Forensics Association"-

Italian Chapter, Camera Penale di Como e Lecco, UAE Union des Avocats
Européen, CSDPE Centro Studi Diritto Penale Europeo, organizza a Varenna, il
prossimo 16 febbraio nella prestigiosa location di Villa Monastero, un incontro
di studio con i maggiori esperti del settore sul delicato rapporto tra
tecnologia e attività di indagine.

Intervento di Stefano Zanero, socio AIPSI

<http://www.iisfa.it/images/Varenna2007/VolantinoVarenna2007.pdf>

- BlackHat DC 2007, 26 Febbraio 2007, Washington D.C.

Si svolgerà allo Sheraton Crystal City, Washington DC, dal 26 Febbraio
al 1° marzo, BlackHat 2007.

Il socio Stefano Zanero terrà un talk il 1° marzo:

"360° Anomaly Based Unsupervised Intrusion Detection"

<http://www.blackhat.com/html/bh-dc-07/bh-dc-07-index.html>

<http://www.blackhat.com/html/bh-dc-07/bh-dc-07-speakers.html#Zanero>

I soci AIPSI/ISSA hanno diritto ad uno sconto di 100 Euro se si
registrano online. Chi fosse interessato troverà nell'area soci/sistema
documentale del sito AIPSI le indicazioni su come ottenere lo sconto.

--
ISSA News ##

--

- The Secure IT 2007 conference, Sacramento, March 27-29
Come to the Secure IT 2007 conference in Sacramento, March 27-29, to learn from experts and colleagues the latest in technology and network security. The 2007 conference will focus on: law, policy and compliance, network control, authentication and encryption, new trends in curriculum development, and the emerging threat-vulnerabilities in web applications.
<http://www.secureitconf.com/>

- Next ISSA CISO Forum in Las Vegas, March 29-30
Enabling Your Business - Think Strategically, Act Tactically.
This is the theme of the next ISSA CISO Executive Membership Forum, to be held in Las Vegas at the MGM Grand, March 29-30. This forum will focus on the steps CISOs can take today to better integrate with business initiatives and create a better long term environment for information security. If you or your boss are interested in attending:
<http://ciso.issa.org/>

- ISSA Webcast
ISSA's Latest Webcast: Security Controls to Ensure Compliance - The Next Phase: Controls Automation & Monitoring
<http://www.issa.org/current-webcast.html#ca012307>

I Webcast di ISSA sono disponibili su
<http://www.issa.org/current-webcast.html> a partire dalla data indicata.

- ISSA Journal
Are you interested in contributing an article to the ISSA Journal? Please contact editor@issa.org, and review the Editorial Guidelines <http://www.issa.org/PDF/TheISSAJournalGuidelines.pdf> - PDF, 48kb)

Banca d'Italia, emanata la Circolare n.263 "Nuove disposizioni di vigilanza prudenziale per le banche"

La circolare, scaricabile dal sito della Banca d'Italia (o, volendo, da quello di ANSSAIF), è estremamente importante, non solo per chi si occupa di Risk Management, ma anche per chi è responsabile della **protezione dei dati e della continuità operativa**.

Alcune informazioni tratte dalla circolare.

Le disposizioni - che divengono efficaci dal **1° gennaio 2007** - si basano sulle modifiche apportate al Testo Unico Bancario (TUB) dal decreto-legge approvato dal Consiglio dei Ministri in data 22 dicembre 2006 e sui criteri contenuti nel decreto adottato in via d'urgenza dal Ministro dell'Economia e delle finanze, Presidente del CICR, su proposta della Banca d'Italia, in data 27 dicembre 2006.

La nuova struttura della regolamentazione prudenziale si basa su **"tre pilastri"**.

Il **primo** introduce un requisito patrimoniale per fronteggiare i rischi tipici dell'attività bancaria e finanziaria (di credito, di controparte, di mercato e operativi); a tal fine sono previste metodologie alternative di calcolo dei requisiti patrimoniali caratterizzate da diversi livelli di complessità nella misurazione dei rischi e nei requisiti organizzativi e di controllo.

Il **secondo** richiede alle banche di dotarsi di una strategia e di un processo di controllo dell'adeguatezza patrimoniale, attuale e prospettica, rimettendo all'Autorità di vigilanza il compito di verificare l'affidabilità e la coerenza dei relativi risultati e di adottare, ove la situazione lo richieda, le opportune misure correttive.

Il **terzo** introduce obblighi di **informativa al pubblico** riguardanti l'adeguatezza patrimoniale, l'esposizione ai rischi e le caratteristiche generali dei relativi sistemi di gestione e controllo.

Tale impianto normativo, basato su un rinnovato sistema di regole e incentivi, consente di perseguire con maggiore efficacia gli obiettivi della regolamentazione prudenziale, sanciti dall'art. 5 TUB. Esso, assicura, infatti, una misurazione accurata di un più ampio novero di rischi e una dotazione patrimoniale più strettamente commisurata all'effettivo grado di esposizione al rischio di ciascun intermediario; stimola le banche a migliorare le prassi gestionali e le tecniche di misurazione dei rischi, anche in ragione dei possibili risparmi patrimoniali; favorisce la parità concorrenziale, attraverso una maggiore estensione delle attività e delle tecniche oggetto di armonizzazione; valorizza il ruolo disciplinante del mercato con l'introduzione di specifici obblighi di informativa al pubblico.

La disciplina si articola in un sistema di regole modulari per la determinazione dei requisiti patrimoniali, che recepisce le migliori prassi sviluppate dagli intermediari nelle metodologie di gestione dei rischi. In attuazione del principio di proporzionalità, che informa ampie parti della nuova disciplina, **la regolamentazione tiene conto delle diversità degli intermediari** - in termini di dimensioni, complessità e altre caratteristiche - dettando, per taluni ambiti, regole differenziate e sollecitando, in via più generale, un'applicazione delle disposizioni coerente con le specificità di ciascun intermediario. Ove possibile, essa tende, inoltre, a evitare un'eccessiva prescrittività, indicando solo principi di carattere generale, integrati da linee guida applicative e indicazioni su prassi accettabili, diffuse e utilizzate presso gli intermediari. La regolamentazione si ispira, infine, a un criterio di gradualità: ciascun intermediario, anche in modo differenziato per ciascuna tipologia di rischio, può articolare nel tempo l'accesso a metodologie e processi progressivamente più avanzati. Nel complesso, l'adesione ai suindicati principi e criteri assicura flessibilità di applicazione e contenimento degli oneri della regolamentazione.

Aumentano gli "spyware".

Avevamo ribadito, anche nella Newsletter di dicembre 2006, la nostra preoccupazione per un aumento di programmi "malvagi" (c.d."malware" e "spyware") sui personal computer dei Consumatori e di piccole aziende.

In questo mese, che è trascorso, abbiamo avuto altri riscontri e, fra questi, abbiamo **raccolto un'informazione riguardante un crescente interesse** - da parte di varie fonti, certamente non lecite - **nell'acquisto di software "malevolo"**. Dato che questa notizia è uscita dall' "underground", vuol dire che il sistema dei software "spioni" piace, e molto.

Ricordiamo che parliamo di un sistema consistente nel far memorizzare un software sui pc di ignari cittadini, ai fini di catturare utili informazioni dai file contenuti sui dischi e da quanto digitato sulla tastiera.

Se è vero che il sistema è nato per conoscere le abitudini e le preferenze dei Consumatori, è anche vero che è utilissimo ai criminali, e, perché no, ai terroristi.

E' già accaduto che alcuni computer, "innocenti", sono serviti per lanciare degli attacchi a siti di aziende nemiche, in quanto appartenenti ad ideologie, religioni, ecc. non condivise. Siccome una domanda crescente non può che far aumentare l'offerta, ci dobbiamo attendere una recrudescenza su questo campo.

Su questo tema, che meriterebbe ben più di quattro righe, **dobbiamo segnalare alcuni articoli** usciti questa settimana.

Il primo accenna alla presenza di **pc "zombi"**, pronti quindi ad agire ad un comando da remoto. Su *quotidiano.net* e su altri giornali si può trovare trattato questo tema:

<http://qn.quotidiano.net/chan/tecnologia:5454941:/2007/01/14:>

Il secondo, dal titolo "quando il virus diminuisce, phishing e spam festeggiano", tende a dare una spiegazione - supportata da dati - sul perché si è vista una diminuzione nella "cattiveria" di attacco dei virus.

MessageLabs lo giustifica, come dice il titolo, dalla necessità - per i criminali - di attirare i Consumatori nelle trappole connesse alle email con titoli allettanti o che sembrano provenire da aziende o Enti conosciuti, e con i quali si ha un rapporto cliente-fornitore.

Appunto le spam e le email di phishing.

(Per maggiori informazioni:

<http://www.vnuned.it/it/vnuned/article/2007/01/22/strategie-sempre-pi-complesse>)

A proposito di titoli allettanti, possiamo citare il recente caso - segnalato da **Symantec** - delle email riportanti il titolo "**230 morti a causa della tempesta che ha colpito l'Europa**".

Una volta aperto l'allegato (un videoclip), il computer viene infettato dal Trojan Peacomm, il quale cercherà di connettersi a un indirizzo remoto ed usare il computer infetto per inviare un alto numero di messaggi spam.

(per maggiori informazioni consultare la pagina:

<http://www.agi.it/oggi-in-italia/notizie/200701232034-cro-rt11289-art.html>)

La **Polizia di Stato** ha realizzato facili istruzioni per i Consumatori.

Suggeriamo di accedere al sito:



<http://www.poliziadistato.it/pds/cittadino/consigli/internet.htm>

Cogliamo l'occasione per ribadire l'utilità di valutare la possibilità di collegare il sito aziendale, dedicato all'home banking, al sito della Polizia di Stato, anche in ragione dei continui aggiornamenti ai suggerimenti pratici che vengono forniti; avvisi non di certo fonte di possibile preoccupazione per i Clienti, sia per le modalità espositive che per i contenuti.

Ci si deve consentire di insistere su questo punto, perché una più stretta collaborazione tra azienda e Polizia, non può, innanzitutto, che rafforzare la protezione dei siti da attacchi di *defacement* o di *phishing*, e dall'altro, non ultimo, costituire un momento di collaborazione fra specialisti che operano su un fronte comune: la **prevenzione**.

Nel conversare con più di una banca, abbiamo recepito che quanto andiamo dicendo è già in via di realizzazione.

Ciò che ci preoccupa, è che trattasi solamente di grandi banche, mentre ci saremmo attesi anche, e soprattutto, realtà medio-piccole.

ANSSAIF è chiaramente a disposizione per eventuali approfondimenti.

ABI sigla intesa con Federutility sull'uso dell'energia

Il presidente dell'Associazione Bancaria Italiana, Corrado Faissola, e il presidente di Federutility, Giuliano Zuccoli, hanno firmato un **protocollo di intesa** che prevede una serie di iniziative congiunte, fra le quali figura **lo studio delle specifiche esigenze del settore bancario in materia di continuità del servizio; la prevenzione e la risoluzione di situazioni di "disagio" dovute a disalimentazione elettrica; il monitoraggio dei siti bancari privilegiati e l'analisi congiunta di quelli a maggior rischio; l'approfondimento sulle procedure di emergenza;** la realizzazione di attività congiunte nell'ambito dell'efficienza energetica.

Per maggiori informazioni, consultare anche:

<http://www.borsaitaliana.it/bitApp/news.bit?target=NewsViewer&id=251147>





AIEA
(Associazione Italiana Information System Auditors)
Via Valla , 16
20141 Milano
Tel. +39/2/70608405
Fax. +39/2/700507644
P.IVA 10899720154
<http://www.aiea.it>