



Associazione Italiana
Information Systems Auditors



A tutti voi gli auguri di un sereno 2008.

Buon Anno!

E' con questo augurio che vogliamo aprire il primo numero della Newsletter del 2008.

Buon Anno a tutti i soci che stanno contribuendo a rendere sempre più importante la professione di un IS Auditor e che con noi stanno partecipando alla crescita dell'Associazione stessa.

Siamo entrati nel 29esimo anno di vita dell'Associazione e siamo arrivati a 640 soci. Un numero ragguardevole che, solo qualche anno fa, avremmo giudicato irraggiungibile. E' un numero che sprona tutto il Consiglio Direttivo ad accrescere e migliorare i benefici per i soci.

Siamo certi che il 2008 porterà risultati ancora migliori e che la "squadra" dei soci (così intendiamo la comunità professionale che rappresentiamo) sarà sempre più forte. Ma lo saremo veramente se tutti si sentiranno parte della squadra, condividendo obiettivi e risultati.

Come scritto nel redazionale dell'ultimo numero di InfoAiea: "**Share your knowledge!** Cosa aspettate a darci una mano, il contributo di tutti è prezioso. Siamo fortemente convinti che nel 2008 conseguiremo

ulteriori risultati per affermare la nostra professione: auguri a tutti di un felice e proficuo anno nuovo.

Notizie dai Gruppi di Lavoro

Gruppo di lavoro "SOX2"

Il Gruppo di Lavoro "Sarbanes Oxley 2" ha concluso i lavori. Il documento originale è stato completamente tradotto ed è terminato anche il controllo qualità. Il documento è in fase di stampa e sarà reso disponibile ai soci entro febbraio.

Esame CISA e CISM

Ricordiamo che i risultati dell'esame saranno comunicati, direttamente agli interessati, entro il mese di febbraio.

Sul sito www.isaca.org è già possibile l'iscrizione on-line all'esame di giugno 2008.

Le prossime attività di AIEA

1. Per il sesto anno consecutivo, AIEA organizza a Lugano, in collaborazione con ATED e il chapter svizzero, una Sessione di Studio sul tema IT Governance. La locandina è stata diffusa ai soci.
2. Ricordiamo ai soci che è disponibile, sul sito www.aiea.it, il calendario aggiornato di tutti gli eventi e dei corsi programmati nell'anno.



Il prossimo Convegno annuale

Tutto il Consiglio Direttivo, al quale si affiancano alcuni soci, sta lavorando all'organizzazione del prossimo Convegno. Prevediamo che si terrà nella seconda quindicina del mese di maggio 2008, probabilmente in una città dell'Emilia-Romagna. Vi terremo informati.

Notizie da ISACA

Riceviamo da ISACA:

ISACA Benefit of the Month

The Information Systems Control Journal is an authoritative, peer-reviewed publication that has reported on topics such as Internet security, IT governance, computer crime, information integrity, computer confidentiality issues and IT risk management. ISACA members receive a subscription to the print version of the Journal which is published six times a year. Members also have exclusive access for one year to the online version, JOnline, which features additional articles not featured in the print version. Visit www.isaca.org/currentissue to view the latest Journal today!

Important upcoming dates:

- 21-22 January, Asia-Pacific CACS, Muscat, Sultanate of Oman
- 22 January, deadline to submit articles for consideration for vol. 3, 2008, of Information Systems Control Journal
- 28-29 January, Information Security Conference, Panama, Republic of Panama
- 30 January, early-bird registration deadline for the April ISACA Training Week in Dallas, Texas, USA
- 13 February, early-bird registration deadline for the June 2008 CISA and CISM exams and 2008 North America CACS
- 25-29 February, ISACA Training Week, Atlanta, Georgia, USA

Il sito AIEA

Continua la nostra lettura di chi, come e quando, accede al nostro sito.

Di seguito la percentuale dei paesi di provenienza, sul totale degli accessi di dicembre:

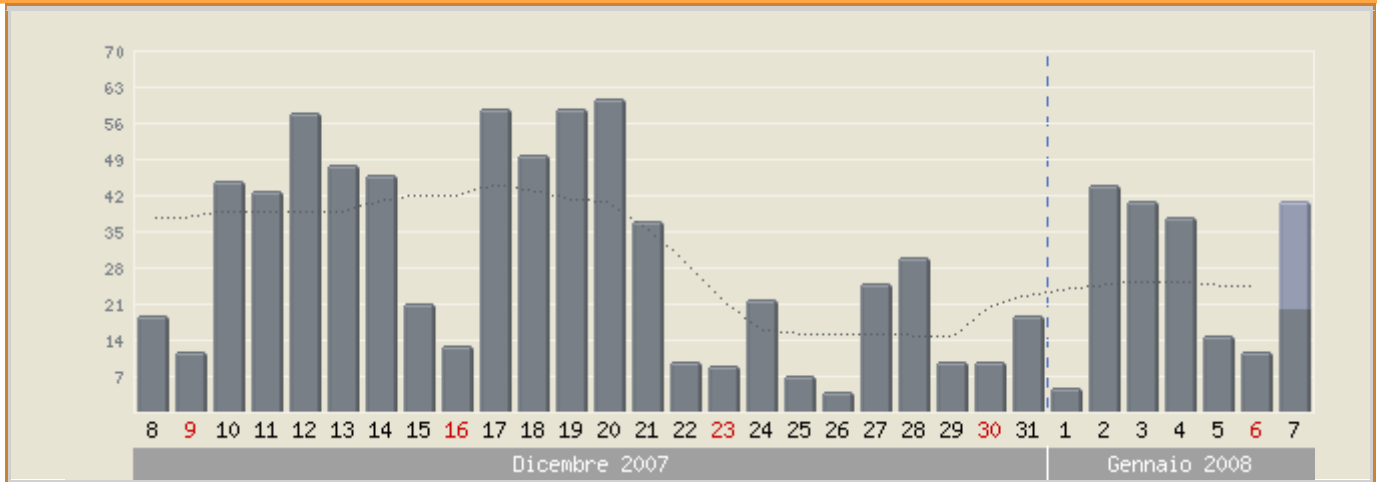
■ Italia	83,66 %
■ Regno Unito	4,55 %
■ Germania	2,59 %
■ Stati Uniti d'America	1,86 %
■ Svizzera	1,76 %
■ Altri	5,58 %

Dopo la Svizzera, i "primi paesi della voce "Altri" sono il Giappone, l'Irlanda, il Brasile e la Francia.

E' interessante rilevare che, anche durante il periodo natalizio, a parte i giorni di Natale, ci siano stati molti accessi.



Grafico Visite



Avviso ai soci

Con l'obiettivo di coinvolgere nella vita associativa tutti i soci, invitiamo i lettori a fornire le proprie indicazioni su argomenti o temi che desiderano vengano trattati nel corso del 2008 sia nelle Sessioni di studio sia in Workshop.

Chi volesse dare il proprio contributo, è pregato inviare una mail a aiea@aiea.it, specificando, nell'oggetto "ARGOMENTI DI INTERESSE".

In una successiva newsletter provvederemo ad elencare tutti i temi proposti.

Partecipazione di soci ad eventi

Tutti i soci possono segnalare eventi, fatti e informazioni di possibile interesse comune da segnalare ad esempio nella newsletter.

In particolare, se partecipate ad un evento in qualità di organizzatore, relatore o chairman, valutate la possibilità di partecipare a nome AIEA. La partecipazione dell'Associazione ad un evento "deve" però essere decisa dal Consiglio Direttivo: siete quindi pregati di contattare il CD con ragionevole anticipo!

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 che alla stesura di numerosi documenti hanno partecipato diversi nostri soci e che inoltre CNIPA organizza incontri o seminari aperti anche ai soci AIEA.



AIPSI - Associazione Italiana Professionisti di Sicurezza Informatica

ESTRATTO Newsletter numero 17, 24 Dicembre 2007

Disponibile in PDF all'indirizzo

http://www.aipsi.org/newsletter/Aipsi_NewsLetter-18-2007_12.pdf

Attività dell'Associazione ##

- AIPSI a eSecurity Lab 2008 - Milano 31 Gennaio 2008

Presso il prestigioso Palazzo Bocconi Corso Venezia, 48, si svolgerà la manifestazione e-Security LAB organizzata da BCI Italia con il patrocinio di AIPSI e altre associazioni quali CLUB-TI e FIDA Italia. Il Keynote di apertura sarà a cura del presidente AIPSI. Maggiori informazioni sono reperibili sul sito <http://www.bci-italia.com>. L'agenda completa è disponibile al link

http://www.bci-italia.com/confexpo/eSecurity/2008/esecurity08_agenda.htm

Ad AIPSI è riservato un numero di inviti gratuiti. Gli interessati possono mandare un'email ad info@aipsi.org, con subject "Richiesta di Partecipazione e-Security Lab 2008", fornendo i propri dati: Nome, Cognome, Ruolo, Azienda.

- AIPSI a Infosecurity 2008 - Milano 5,6 e 7 Febbraio

AIPSI, già dallo scorso anno partner della manifestazione, partecipa ad Infosecurity con un proprio Stand. La manifestazione, che avrà luogo presso il Padiglione 17 della Fiera (il medesimo degli ultimi anni) si svolgerà nei giorni 5, 6 e 7 febbraio.

Il giorno 7 dalle ore 14:00 alle ore 17:00, AIPSI terrà un interessante Corso introduttivo di Forensic Analysis valido per accumulare Crediti (CPE).

Maggiori informazioni sono reperibili sul sito www.infosecurity.it e sul sito AIPSI www.aipsi.org

Anche quest'anno AIPSI dispone di un numero cospicuo di Inviti per Infosecurity. I suddetti codici sono richiedibili ad info@aipsi.org.

Qualora vogliate invitare Vostri conoscenti, non esitate a chiedere i codici al link info@aipsi.org specificando il n° di invitati.

- Sicurezza e Assicurazioni:

Nell'ambito di incontri con professionals del settore Assicurativo è emersa la possibilità di offrire ai soci AIPSI la:

- Polizza di Tutela Legale per i professionisti ed i consulenti dell'IT, da studiare con ISI Insurance del Gruppo Assicurativo Arca (compagnia specializzata nella Difesa Legale): un prodotto assicurativo di Tutela Legale studiato per le necessità del settore.

ISSA News ##



Associazione Italiana
Information Systems Auditors



- Nominations for ISSA International Awards Accepted Through January 1, 2008

Take this opportunity to honor your mentors, outstanding peers, remarkable chapters and supporting organizations for their contributions to ISSA and the industry. Award categories include:

1. Chapter Communication Program of the Year
2. Outstanding Information Security Professional of the Year
3. Outstanding Organization of the Year
4. Honor Roll
5. Outstanding Chapter of the Year

Chapters may self-nominate for Outstanding Chapter of the Year and Chapter Communication Program of the Year awards. Nominations should be submitted on the attached form and sent by January 1, 2008 to Ralph Spencer Poore, 2007 Awards Chair, at poorer@issa.org, with a copy to Lyn Trainer, ltrainer@issa.org. Please download the ISSA Award Nomination Template Form.

- ISSA Webcast

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

- ISSA Journal

Ti interessa contribuire con un articolo all'ISSA Journal?
Contatta editor@issa.org e rivedi le Linee Guida Editoriali
<http://www.issa.org/PDF/TheISSAJournalGuidelines.pdf> - PDF, 48kb)

Varie ##

- Corso di Perfezionamento in "computer forensics e investigazioni digitali" dell'Università degli Studi di Milano

E' stato pubblicato sul sito dell'Università di Milano
(<http://www.unimi.it/studenti/corsiperf/5411.htm>) il bando di ammissione alla prima edizione del Corso di Perfezionamento in "computer forensics e investigazioni digitali" dell'Università degli Studi di Milano, il primo corso post laurea in Italia interamente dedicato a questi argomenti.

Il corso è pensato per avvocati, giuristi in genere, informatici, ingegneri, economisti, responsabili di sicurezza interni alle aziende, investigatori, responsabili privacy e sicurezza. E' focalizzato sulle indagini informatiche, anche in ambito aziendale e nel settore pubblico.

Tra i docenti spiccano i maggiori esperti di computer forensics del nostro paese, tra i quali svariati soci di AIPSI.

Per maggiori informazioni si può contattare la Presidenza della Facoltà di Giurisprudenza - Segreteria Didattica - Via Festa del Perdono, 7 - 20122 Milano, Tel. 02-5031.2473/2694/2087, Fax 02-5031.2475, e-mail infomaster.giurisprudenza@unimi.it.



Associazione Italiana
Information Systems Auditors



ESTRATTO NEWSLETTER ANSSAIF DEL 3/1/2008

ANSSAIF si decentra.

Con l'apertura di sedi a **Lecce**, **Siena** e **Milano**, l'Associazione si prefigge di raggiungere i seguenti obiettivi:

1. un maggiore contatto con le realtà locali, non solo aziendali (ci si riferisce ad esempio alle Università, associazioni culturali, ecc.), attraverso incontri e seminari di studio più vicini alle esigenze delle aziende e delle Università;
2. un maggiore parallelismo nella conduzione delle iniziative ed un migliore scambio informativo;
3. la prosecuzione nell'attenzione ai costi per i soci derivanti dalle trasferte;
4. un maggiore coinvolgimento dei membri del consiglio direttivo.

Responsabili di ciascuna sede sono i Consiglieri ivi residenti. Ove assenti, il riferimento locale può essere anche assunto temporaneamente da un socio che ricopra un ruolo di responsabilità in un'azienda di intermediazione finanziaria locale.

I referenti locali forniscono notizie ed esigenze informative al Segretario ed al Presidente, che provvederanno a trattarle secondo il loro contenuto e priorità, tenendo a mente che l'obiettivo principale di ANSSAIF è *l'information sharing*.

Le sedi di prossima apertura sono a **Lugano** e **Parigi**, per le quali sono stati già individuati i Soci che saranno il punto di riferimento.

Tra le iniziative a livello europeo, vi è la costituzione di un Osservatorio sulla Sicurezza.

E' possibile contattare i referenti locali via Email ai seguenti indirizzi:

LECCE - Consigliere **Stefania Patavia**, Email: anssaif.lecce@anssaif.eu

SIENA - Consiglieri **Vincenzo Giardina**, **Giovanni Becattini** Email: anssaif.siena@anssaif.eu

MILANO - Consiglieri **Stefano Cabianca**, **Leonardo Procopio**, **Armando Righetti**, Email: anssaif.milano@anssaif.eu

Email di phishing: la situazione attuale (1).

Lo spamming sta aumentando l'intensità dei suoi picchi (anche di nove volte in raffronto al precedente), la tipologia di email è la stessa da mesi, tranne, come vedremo, che per il phishing.

Ad oggi, le email di spamming si possono dividere nelle seguenti categorie:

phishing (tese ad ottenere le credenziali di accesso al proprio conto on line);

vendita di prodotti (medicinali, orologi, ecc.);



scommesse;

suggerimenti (es: investimenti in azioni, interventi per migliorare le "prestazioni", opportunità di lavoro, ecc.);

richieste di contatto (ragazza russa sola, erede unico di un'ingente fortuna, ecc.);

vincite alla lotteria;

saluti (biglietti augurali, messaggi vocali, ecc.).

A volte le email pervengono ad ondate successive. In alcuni casi, inondano con centinaia o migliaia di email i domini di una determinata Azienda o Ente, in modo da provocare un forte rallentamento nella ricezione della posta e riempire le caselle, se non prontamente svuotate dalla email spazzatura.

Anche quelle di phishing, una volta più discrete, ora arrivano a gruppi e, molto spesso, con il risultato che il ricevente nemmeno le legge, e le cancella tutte in un colpo solo. Infatti, risultano pervenire da quattro o cinque banche diverse, come se tutti avessero più rapporti di conto on line con così tante banche!

Sul fronte della tipologia di messaggi, da pochi giorni si nota qualche novità nella speranza, per il criminale, di riuscire ad ingannare qualche utente.

Possiamo raggruppare le email di phishing in base alla tipologia di messaggio che viene inviato, vuoi positivo (ad esempio, per prevenire atti criminali o per premiare), o negativo (ad esempio, perché l'utente ha sbagliato più di tre volte l'immissione della password).

Vediamo le diverse tipologie:

POSITIVI:

la banca o Ente emittente la carta di credito è attento alla sicurezza; con la email inviata chiede la verifica dei dati per l'accesso online, oppure per attivare un rapporto di conto (in alcuni casi la email dice che il codice dispositivo arriverà via posta, ma per attivarlo bisogna digitare le credenziali, e quindi il codice dispositivo!

Ciò è interessante, in quanto sembra che con queste email i criminali sembrano puntare a clienti con qualche problema di comprensione o fortemente distratti, e tutto ciò fa riflettere sulla reale composizione dell'universo degli utilizzatori di funzionalità offerte dal mondo finanziario e sulla possibile percentuale di utenti con ridotte capacità critiche);

un addebito sul conto è andato a buon fine; se il Cliente ha qualche rimostranza, acceda al conto digitando le note credenziali (è ovvio che, nella mente dell'ignoto criminale, il Cliente sprovveduto accede subito per vedere di che si tratta!);

il Cliente è stato premiato per la sua fedeltà all'accesso online: per ottenere la vincita (da 350 a 500 euro a seconda dell'Azienda) si deve accedere al conto digitando le credenziali, ovviamente!



Email di phishing: la situazione attuale (2).

NEGATIVI:

la banca o Ente è intervenuto bloccando il conto; ciò per una di queste cause: tentativi di accesso che hanno provocato il blocco della password, accesso da un indirizzo del Cliente diverso da quello solitamente utilizzato (in questo caso si nota una incongruenza: l'accesso è bloccato, ma si chiede al Cliente di digitare le credenziali per accedere!)

un accredito è stato bloccato, in quanto vi sono delle irregolarità; il Cliente acceda al conto per correggere tali difformità.

Ciò che fa piacere osservare, è sia come le Aziende - tramite l'Autorità Giudiziaria - intervengano immediatamente per bloccare gli indirizzi Internet forniti dalle email di phishing, sia sulla efficacia dei più recenti software prodotti per difendere i computer (antiphishing, antispyware, personal firewall, ecc.).

In conclusione, ci sembra che, per le ragioni sopradette, la situazione phishing, a tre anni dal suo manifestarsi, appaia oramai avere un lento declino nell'area dell'efficacia.

Una preoccupazione, invece, ci assilla. Come scritto diversi mesi fa, e riportato anche dalla stampa specializzata, non si assiste da tempo ad un attacco virus massiccio. Aumentano invece gli spyware ed i malware, ossia, programmi atti a catturare le informazioni digitate sul computer ovvero a dirottare su siti criminali gli utenti.

Appare pertanto esserci una stretta correlazione fra i due fenomeni. Infatti, qualora vi fosse un massiccio attacco di virus tesi a bloccare le comunicazioni o a distruggere il contenuto dei computer, gli utenti interverrebbero con tempestività e senza tentennamenti nel migliorare le difese dei computer.

Il consiglio, quindi, che ci sentiamo di dare, è chiaramente quello di adottare misure periodiche quali le seguenti:

sensibilizzare gli utenti ed i Clienti sui possibili rischi nei quali possono incorrere se: non aggiornano il software a protezione del computer utilizzato, evitano di accedere a siti non conosciuti, non scaricano musiche o filmati o foto da siti sconosciuti

intensificare i controlli sui computer, specialmente alla ricerca di spyware; possibilmente, tal fine, eseguire la scansione del pc tramite un antivirus o software diverso da quello dell'antivirus attivo sul computer;

mettersi in allarme in caso di attività insolita del computer (da non confondere con l'aggiornamento in background del software di sistema).



CLUSIT ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA

31 dicembre 2007 – ESTRATTO Newsletter CLUSIT - www.clusit.it

[disponibile in PDF all'indirizzo

www.clusit.it/newsletter_31_12_07.pdf]

=====

NOTE DA BRUXELLES

=====

Il 7 dicembre scorso si è tenuto a Bruxelles un seminario organizzato dalla Direzione Generale Information Society and Media della Commissione Europea dal titolo "Raising security awareness and strengthening the trust of end-users in information society: policy challenges for the next decade" a cui erano invitati, oltre ai rappresentanti dei governi dei paesi membri, esponenti del mondo accademico ed esperti di sicurezza a vari livelli.

Il CLUSIT era presente, nella persona del suo presidente, Gigi Tagliapietra, sia come organizzazione focalizzata alla sicurezza che come rappresentante del Dipartimento per l'innovazione e le tecnologie della Presidenza del Consiglio dei Ministri. L'obiettivo dichiarato del seminario era quello di fornire indicazioni alla Commissione su quali passi compiere, all'interno dell'iniziativa i2010, per costruire una società dell'informazione che sia anche sicura. Il seminario era diviso in tre sessioni di brainstorming

- Tecnologia: quali impatti ci si devono aspettare dalle nuove tecnologie rispetto alla privacy e alla fiducia degli utenti sia business che privati.
- Dipendenza: come le reti, intese come insieme di oggetti e servizi, siano sempre più determinanti per la vita sociale e come garantirne la continuità
- Percezione: quali fattori psicologici influiscono sulla fiducia, come trasformare la consapevolezza in fiducia, come misurare la fiducia e come bilanciare responsabilità e legalità.

Già nel titolo si colgono due aspetti importanti: l'attenzione si sposta sempre più dal tema "sicurezza" (che sottintende tecnologia) a quello della "fiducia" (che implica fattori emotivi e psicologici) e l'orizzonte temporale deve essere quello di medio-lungo periodo, dieci anni, perchè le politiche di breve termine non possono sperare di fronteggiare le sfide che abbiamo di fronte a noi.

Lo scenario

Le presentazioni di apertura del dr. Andrea Servida, responsabile dell'unità A3 della DG Information Society, e del prof. Michel Riguidel dell'Ecole Nationale Supérieure des Télécommunications di Parigi, hanno dipinto uno scenario contraddittorio.

Un livello ancora insufficiente di consapevolezza dei rischi e la conseguente limitata protezione dei sistemi (secondo un'indagine Eurostat solo il 30% degli utenti protegge i propri sistemi) a fronte di una crescente complessità e fragilità dell'infrastruttura: "Dobbiamo vedere i sistemi come 'inestricabili' e non più come sistemi 'complessi'"

A fronte di una esigenza a breve di recuperare il ritardo accumulato è importante guardare al futuro con un'ottica completamente diversa rispetto al passato che faccia superare la dicotomia macchina-rete verso una visione molto più dinamica e olistica dei sistemi e delle relazioni che si instaurano tra i partecipanti.

La sicurezza del futuro sarà non un sistema monolitico ma la negoziazione di una serie di informazioni tra due entità (il singolo e l'ente o azienda) che vogliono dialogare, in cui la fiducia non sarà affidata integralmente a sistemi tecnologici ma anche a reti di referenza e trust reciproco di micro-comunità.

In più non dovremo pensare solamente alla sicurezza ma alla "sovranità" e alla "dignità" digitale come temi centrali per la costruzione di una società dell'informazione in cui i cittadini possano riconoscersi.



Tra le sfide più serie vi è quella della comprensione dei tempi diversi dei diversi fattori in gioco (la vita media di un sistema di sicurezza era stimato in 10 anni mentre le generazioni di attacchi mutano ogni 3) e il fatto che la distinzione tra mondo reale e virtuale si assottiglia sempre più e dovremo aspettarci nei prossimi 5 anni virus e malware che causeranno la morte di persone (si pensi a un pacemaker connesso alla rete sanitaria per monitoraggio che viene messo fuori uso da un virus).

Di certo la tecnologia pone quesiti importanti e non solo perchè parliamo di RFID ma perchè dovremo pensare a come securizzare il nanomondo e gli oggetti infinitamente piccoli o come securizzare i futuri computer quantici che non sono "digitali".

Dovremo infine accettare il fatto che non tutto sarà controllabile e sicuro e che "infosfere", di cui noi non avremo e non potremo avere il controllo, appartengono al nostro futuro.

Il dibattito

Dalla discussione sono emersi spunti molti interessanti.

Janne Uusilehto, responsabile product security di NOKIA, ha fatto notare come nel 2015 si prevede siano 5 miliardi le persone "always connected" e un livello di traffico moltiplicato per 100 volte rispetto a quello attuale e ha ricordato che "La tecnologia non protegge le persone ma offre strumenti alle persone che vogliono proteggersi."

Ha sottolineato inoltre che se è vero che il grande tema è quello della alfabetizzazione di massa dei cittadini e degli utenti, non bisogna dimenticare che occorre preparare e formare in modo preciso anche tutta una nuova generazione di tecnici, che oggi non sono in grado di sviluppare software sicuri fin dall'inizio.

Gerald Spindler dell' Università di Gottingen ha ricordato che servono norme che introducano "minimum security standards" (oggi presenti solo per i prodotti medicali) e che la direttiva europea sulla responsabilità di prodotto non include il software come "prodotto". Gli ha fatto eco Kornelia Kutterer della European Consumer Association condividendo l'idea delle regole minime di sicurezza ma ha sottolineato che bisogna anche definire chi garantisce l'imposizione e il rispetto di queste norme e per di più la Commissione Europea dovrebbe essere molto più precisa quando usa termini come pirateria, sicurezza, cybercrimine che oggi assimilano gli utenti ai terroristi.

Il tema della fiducia

Angela Sasse Professor of Human-Centered Technologies all' University College di Londra ha sviluppato il tema della "fiducia" che era il punto chiave del seminario.

Ne ha dato innanzitutto una definizione: Fiducia come volontà di essere vulnerabile basandosi su positive aspettative sulle azioni degli altri.

La fiducia è cognitiva (razionale) o immediata (pre-cognitiva) ad esempio con i familiari e si sviluppa nella lettura di segnali che spesso mancano nel mondo virtuale e rappresenta una scorciatoia per un approccio analitico alla valutazione costi-rischi-benefici.

Dopo le prime interazioni in un ambiente di fiducia, l'utente trasforma la fiducia in affidabilità e abbassa la percezione della vulnerabilità (vedi il phishing), non si tratta quindi di manipolare la richiesta di fiducia (mettere un viso sorridente sulla pagina web) ma di aiutare gli utenti a comportamenti positivi in cui "La tecnologia consente agli utenti di prendere la giusta decisione in termini di fiducia".

L'interazione deve dare incentivi che premiano comportamenti corretti e fornire segnali che gli utenti possono leggere: servono SINTOMI (es. prodotti di relazione fiduciaria) e non semplicemente SIMBOLI. Compito delle istituzioni è quindi anche quello di ridurre le situazioni di "incertezza" e un possibile percorso da seguire è quello di sostenere comunità di utenti che costruiscono legami di fiducia e che poi si autoregolano.



Su questo tema è intervenuta Albena Spasova, responsabile dell' ufficio legale di eBay, per la quale il 100% del business di eBay dipende dalla fiducia: se un utente ha una esperienza negativa non torna più. La risposta è una iniziativa decisa e costante che si basa certo sulla tecnologia, ma soprattutto sulla completa trasparenza con gli utenti, informazioni continue e accurate, un servizio h24 per rispondere alle potenziali frodi, un software gratuito che garantisce l'autenticità del sito eBay. In sostanza non UNA risposta ma un insieme di azioni coordinate e focalizzate.

Due commenti degni di nota:

"Un mondo con l'identificazione univoca di singoli oggetti e persone è estremamente pericoloso, dobbiamo pensare a forme di "proxy" che mettano delle generalizzazioni tra noi e la rete garantendo la protezione dell'identità e nel contempo la partecipazione responsabile."

"Dobbiamo sviluppare forme di ragionamento non lineare: le cinture di sicurezza riducono gli incidenti? No, riducono i morti, è vero, li dimezzano. Ma il numero totale dei morti in Inghilterra non è diminuito perchè sono aumentati gli incidenti, anche perchè, siccome la gente si sente più sicura, viaggia più veloce e corre maggiori rischi." (Sasse)

Come misurare la fiducia

Già dal prossimo anno la Commissione Europea collaborerà con Eurostat per sviluppare sistemi che misurino il livello di fiducia degli utenti nei sistemi informativi, per poter valutare in termini concreti l'efficacia delle iniziative che vengono messe in campo. E' un terreno difficile, come ha sottolineato Tobias Husing, ricercatore di Empirica, una società Tedesca che ha già collaborato con la DG su questo tema, perchè nelle indagini sulla sicurezza per gli utenti finali, la gran parte degli intervistati non è nemmeno in grado di capire la domanda. Innovativo non è solo il terreno d'indagine ma devono essere innovati anche gli strumenti di misura e devono venire correlati indicatori anche marginali ma che possano aiutare a capire se il cambiamento di fiducia induce cambiamenti nei comportamenti. Qualunque analisi statistica classica non funziona per misurare la fiducia: serve un "benchmarking analitico" che analizzi in dettaglio anche micro-indicatori.

Due punti di vista significativi

Sono stati presentati nel dibattito finale due punti di vista significativi da parte di istituzioni governative. Ferenc Suba, Presidente del PTA, una emanazione del CERT ungherese, che ha scelto la via della costruzione di una fondazione di tipo privatistico che garantisce rapidità ed efficienza nell'azione quotidiana mantenendo il ruolo governativo di guida e orientamento ma evitando la farraginosità tipica delle pubbliche amministrazioni.

Il rappresentante del Governo Greco (Ministero delle Finanze) ha sostenuto che non si tratta di costituire nuove authorities ma di far interagire i player attuali (providers, operatori di telecomunicazioni, associazioni) e di unificarne i linguaggi e gli sforzi coordinandone le iniziative, favorendo l'interscambio di esperienze e la condivisione delle best practices. Un richiamo alla collaborazione tra attori, istituzioni e paesi come chiave per la soluzione alle sfide della sicurezza del prossimo decennio.

=====

VITTORIA AL "CAPTURE THE FLAG"

=====

Sono i "Chocolate Makers" dell'Università degli Studi di Milano i vincitori dell'edizione 2007 del torneo internazionale a squadre "Capturethe Flag" organizzato dall'Università di Santa Barbara, in California. "Una grande soddisfazione per una piccola squadra come la nostra che nel 2005 aveva già vinto una competizione analoga, anche se minore, promossa dall'Università di Aachen, in Germania " -



Associazione Italiana
Information Systems Auditors



dice Roberto Paleari, uno degli 8 membri dei Chocolate (<http://security.dico.unimi.it/ictf07.shtml>) che hanno sfidato gli altri 34 team provenienti in massima parte da Stati Uniti e Germania ma anche da Russia, India, Austria e Argentina. Settima classificata l'altra squadra italiana: "The Tower of Hanoi" del Politecnico di Milano, che aveva invece vinto l'edizione 2004.

La gara di sicurezza informatica, nata nel 2003, vede la partecipazione internazionale di squadre di studenti che si affrontano difendendo l'integrità e il funzionamento di un dato numero di servizi in rete, su piattaforma Linux o Windows, mentre cercano di sabotare quelli degli avversari. "Una sorta di versione virtuale di "bandiera" - spiega Paleari - dove le bandierine si conquistano individuando e riparando la vulnerabilità di file che dovrebbero invece risultare inaccessibili". A garanzia di un comportamento etico, ogni anno sono ammesse a partecipare alla competizione solo le squadre che fanno capo a un'istituzione scolastica.

Per saperne di più: <http://www.cs.ucsb.edu/~vigna/CTF/>

=====

PRIMA CONFERENZA NAZIONALE SERVIZI INNOVATIVI E TECNOLOGICI

=====

I Servizi innovativi insieme alle Tecnologie dell'informazione e della comunicazione consentono di raggiungere obiettivi irrinunciabili dal punto di vista sia dell'efficacia che dell'efficienza, ottimizzando la performance di imprese e Pubbliche amministrazioni. Nello sviluppo dell'Economia dei Servizi innovativi il nostro Paese segna un ritardo a causa di diversi fattori che ci impediscono di crescere ed essere competitivi al pari dei nostri partner europei. L'innovazione è un sistema complesso, perché i soggetti coinvolti sono molteplici e gli strumenti per diffonderla innumerevoli. L'innovazione è valore, perché costituisce la chiave per la crescita stessa della società, e questo crea sviluppo. L'economia dell'innovazione trova nell'iniziativa imprenditoriale, nelle tecnologie e nei Servizi innovativi i fattori propulsivi, essenziali per imprimere al nostro sistema produttivo la necessaria accelerazione nella sfida globale. Per riflettere sul ruolo dei Servizi innovativi e tecnologici come volano di crescita per l'economia del Paese e per dare visibilità alle dimensioni del settore, Confindustria Servizi Innovativi e Tecnologici organizza la "1a Conferenza Nazionale dei Servizi Innovativi e Tecnologici" che sarà occasione per discutere di modelli e strumenti per la crescita e di come "rimettere in corsa" il nostro Paese.

La Conferenza si terrà il 4 febbraio 2008, a Milano, presso l'Auditorium di Assolombarda, con inizio lavori alle ore 9 e conclusioni alle ore 14 circa.

Interverranno a questo importante appuntamento autorità ed esperti. Tra i contributi già confermati, il saluto di apertura del Presidente Assolombarda, Diana Bracco e le relazioni di Nando Pagnoncelli e Antonio Catricalà che introdurranno la sessione dedicata agli interventi dei Presidenti delle principali Rappresentanze dei Servizi di Confindustria.

Seguiranno la relazione del Presidente di Confindustria Servizi Innovativi e Tecnologici, Alberto Tripi, e l'intervento del Presidente di Confindustria, Luca Cordero di Montezemolo. Il Ministro dello Sviluppo Economico, Pier Luigi Bersani, chiuderà i lavori.

La partecipazione alla Conferenza è gratuita, ma è obbligatoria l'iscrizione che potrà essere effettuata, a partire dal 10 gennaio tramite il sito www.conferenzanazionale.servizi.org nel quale saranno pubblicati anche aggiornamenti sul programma, documentazione e ogni altra informazione utile.

Ai partecipanti alla Conferenza sarà consegnata copia del Primo Rapporto sui Servizi Innovativi in Italia.



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

SERVIZIO RELAZIONI CON I MEZZI DI INFORMAZIONE

COMUNICATO STAMPA

ASSISTENZA TELEFONICA ED INFORMAZIONE AI CLIENTI

Le indicazioni del Garante per un corretto uso dei dati personali

Le società che si occupano di customer care, assistenza post vendita, prenotazioni di servizi, phone-banking non sono sempre tenute ad informare in maniera burocratica la clientela sull'uso dei dati personali. Possono non farlo quando trattano i soli dati necessari ad assicurare il servizio richiesto, o il cliente è già stato informato precedentemente, ad es. al momento della sottoscrizione di un contratto, o alcuni elementi dell'informativa possono emergere nel corso del colloquio telefonico. Fornire l'informativa in questi casi costituirebbe un inutile appesantimento burocratico per le aziende senza garantire una effettiva tutela dei diritti dell'utente - che già sa a chi si sta rivolgendo e perché - oltre a comportargli un aggravio di costi. Se poi le società intendono utilizzare i dati anche per altri fini (ad es. di marketing o profilazione) allora devono informare l'utente e chiedergli un consenso ad hoc.

L'informativa da rendere all'interessato deve comunque essere fornita con formule sintetiche, chiare e di immediata comprensione, attraverso un operatore o utilizzando messaggi preregistrati o pubblicandola su un sito web.

E' quanto stabilito dal Garante, in un provvedimento generale, di cui è stato relatore Francesco Pizzetti (pubblicato sulla Gazzetta ufficiale n. 285 del 7 dicembre) che riguarda le attività prestate in modalità "inbound", ossia a seguito di una chiamata dell'utente, effettuate anche attraverso canali completamente automatizzati.

Nel provvedimento, adottato anche tenendo conto delle richieste di chiarimento provenienti da una associazione di categoria rappresentativa di alcune società di call center, l'Autorità ha inoltre invitato le società che operano nella gestione dei servizi telefonici di assistenza e informazione al pubblico ad assicurare elevati livelli di professionalità nel trattamento dei dati ponendo specifica attenzione anche al profilo della loro messa in sicurezza.

In particolare il provvedimento ha sottolineato l'importanza di adottare adeguate cautele quando un medesimo call center si trovi a gestire contemporaneamente vari data base, con tipologie diverse di informazioni, per una pluralità di committenti. Per tale motivo, prima della stipula del contratto che affida in outsourcing il servizio deve essere effettuata un'attenta analisi delle implicazioni che il trattamento dei dati può comportare.

Roma, 10 dicembre 2007



- GLI SPAMMER RISCHIANO IL RISARCIMENTO DANNI
- SICUREZZA SITI ARCHEOLOGICI E USO DEI DATI BIOMETRICI
- TUTELA DELLA PRIVACY E INFORMAZIONI COMMERCIALI

Gli “spammer” rischiano il risarcimento danni

Il Garante ha riaffermato il principio riguardo ad un caso di invio di fax non richiesti

Il destinatario di fax, e-mail, sms e mms indesiderati può rivolgersi al giudice civile e chiedere un risarcimento per la lesione dei propri diritti. Lo ha affermato in un recente provvedimento il Garante, di cui è stato relatore Giuseppe Fortunato, che prosegue in questo modo nell'azione di contrasto allo spam. L'Autorità ha vietato l'uso illecito di dati personali a fini di marketing ad una società che inviava in modo sistematico e ad una molteplicità di persone, materiale pubblicitario e comunicazioni commerciali senza il consenso dei destinatari. La società raggiunta dal provvedimento di divieto non potrà più utilizzare i dati personali in suo possesso. Numerose irregolarità erano infatti emerse nel corso degli accertamenti svolti a seguito di alcune segnalazioni nelle quali si lamentava l'invio di fax indesiderati da parte di una società che promuoveva prodotti e servizi per conto di altre aziende. Nel definire il procedimento il Garante ha ribadito che inviare fax commerciali, senza aver prima ottenuto il consenso informato dei destinatari, comporta un trattamento illecito. Non solo: lo spam può causare danni al destinatario. Nel caso di invio via fax, tale danno può consistere, tra l'altro, nella perdita di tempo, nell'uso indebito della carta, del toner del suo apparecchio e nel disturbo provocato dalla comunicazione indesiderata che tiene occupato l'apparecchio.

La società, dal canto suo, si era giustificata asserendo di inviare fax commerciali solo a soggetti economici i cui numeri sarebbero reperibili sugli elenchi categorici (es. Pagine gialle, Pagine utili). Il Garante ha spiegato che, anche nel caso si utilizzino tali elenchi, non vi è possibilità di un invio senza consenso quando le comunicazioni commerciali sono effettuate con particolari modalità (via fax, posta elettronica, sms o mms o chiamate vocali mediante operatore automatico).

“Le comunicazioni non desiderate, siano esse quelle effettuate via telefono, fax, o quelle elettroniche via sms, mms, e-mail –afferma Giuseppe Fortunato –

rappresentano oggi le forme più invasive di disturbo nella vita quotidiana di utenti e consumatori. E' un fenomeno che va combattuto per liberare le reti di comunicazione da chi le ingolfa solo per proprio profitto. In questa battaglia di civiltà il Garante ha proceduto ad ispezioni tramite Guardia di Finanza, ha denunciato alla magistratura i responsabili, ha comminato notevoli sanzioni e su questa strada proseguirà nella difesa dei cittadini in maniera sempre più incisiva.”

Sicurezza siti archeologici e uso dei dati biometrici

Una Soprintendenza archeologica potrà usare l'impronta della mano dei dipendenti per l'accesso ad una sala operativa.

Per la prima volta una Soprintendenza archeologica potrà usare l'impronta della mano dei dipendenti per l'accesso ad una sala operativa. Il Garante per la protezione dei dati personali ha autorizzato, con un provvedimento di cui è stato relatore Giuseppe Chiaravalloti, una Soprintendenza archeologica al trattamento di dati biometrici per consentire ad un numero limitato di dipendenti di accedere alla propria sala operativa, una area riservata particolarmente sensibile.

Il sistema di riconoscimento biometrico, di cui la Soprintendenza intende avvalersi, si basa solo sul rilevamento delle caratteristiche geometriche della mano e non su altri dati biometrici. Il dispositivo è finalizzato a controllare l'accesso alla sala operativa “ove confluiscono segnalazioni afferenti alla sicurezza anticrimine e antincendio dei siti archeologici” di competenza della Soprintendenza: obiettivo principale, contrastare l'elevato rischio di aggressione dei dipendenti da parte di ladri e tutelare i beni archeologici dichiarati dall'Unesco patrimonio dell'umanità.

Il funzionamento del sistema prevede che alle caratteristiche geometriche della mano venga associato un algoritmo crittografico poi archiviato nella memoria interna del dispositivo biometrico. Tale dispositivo non

è collegato in rete e può essere attivato per effettuare l'accesso solo attraverso una parola chiave numerica scelta dal dipendente.

Il trattamento dei dati è stato ritenuto lecito dal Garante e proporzionato allo scopo. Le caratteristiche geometriche della mano di un individuo, spiega infatti l'Autorità, a differenza delle impronte digitali utilizzabili anche in altri contesti con effetti sugli interessati, non sono descrittive al punto tale da risultare uniche; possono eventualmente non garantire l'identificazione univoca e certa di una persona, ma sono sufficientemente dettagliate per essere impiegate in circoscritti ambiti ai fini della verifica di identità. La geometria della mano appartiene a quella categoria di dati biometrici, evidenzia l'Autorità, che non lasciano tracce suscettibili di essere utilizzate per scopi diversi da quelli perseguiti da chi le raccoglie ed usa.

Inoltre, l'attività di identificazione rientra nelle finalità istituzionali della Soprintendenza, la quale, dovendo garantire nel caso di specie elevati standard di sicurezza, ha necessità di un rigoroso accertamento dell'identità dei dipendenti.

Nell'autorizzare l'uso del sistema, il Garante ha comunque prescritto di integrare l'informativa da fornire ai dipendenti riguardo al trattamento dei loro dati personali, specificando quali possano essere le modalità alternative di accesso per i dipendenti che non vogliono o non possano avvalersi del sistema di rilevazione delle caratteristiche della mano.

Tutela della privacy e informazioni commerciali

Le modalità con cui vengono resi noti e gestiti i dati personali tratti da registri pubblici aggregati in un database, devono rispettare i principi di liceità, correttezza e non eccedenza nel loro trattamento e nei tempi di conservazione. È quanto ribadito dal Garante nell'accogliere il ricorso di una persona che aveva chiesto invano ad una società di *business information* di cancellare alcuni dati relativi alla propria attività non perché falsi, ma perché riportati in maniera incompleta e quindi lesivi della propria immagine all'esterno. In particolare, si trattava di dati inerenti al fallimento, avvenuto più di vent'anni prima e poi chiuso per assenza di passivo, di una società di cui il ricorrente era socio. Il database gestito dalla società viene utilizzato da coloro che operano nel mondo degli affari per ottenere informazioni circa l'affidabilità e la solvibilità di persone o società con le quali eventualmente instaurare rapporti commerciali.

L'Autorità ha ritenuto che le informazioni presenti nella banca dati venivano messe a disposizione di un amplissimo numero di persone in maniera incompleta e fuorviante: in particolare, non erano indicate infatti le ragioni che avevano portato alla chiusura del

fallimento, pure presenti nei registri pubblici e, soprattutto, si continuava ad associare l'interessato ad un evento, peraltro avvenuto ventidue anni prima, relativo ad un altro soggetto giuridico, cioè la società fallita.

Il Garante ha perciò disposto la sospensione della visibilità dell'informazione relativa al fallimento laddove figura associata direttamente al ricorrente. L'Autorità ha ricordato di aver già deciso, in vista dell'elaborazione del previsto codice deontologico in materia, di avviare un procedimento di verifica riguardo all'uso dei dati per finalità di informazione commerciale.

L'attività del Garante. Per chi vuole saperne di più

Gli interventi e i provvedimenti più importanti recentemente adottati dall'Autorità

Avviso pubblico di avvio della consultazione su "Linee guida per i trattamenti di dati nell'ambito delle sperimentazioni cliniche di medicinali" - 11.12.2007

- Adempimenti semplificati per il *customer care* – Comunicato dell' 11.12.2007

- Flusso transfrontaliero di dati: il Garante chiede nuove regole per aiutare le imprese multinazionali a tutelare i cittadini – Comunicato del 6.12.2007

NEWSLETTER

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

Direzione e redazione: Garante per la protezione dei dati personali, Piazza di Monte Citorio, n.121 - 00186 Roma.
Tel: 06/69677751 - Fax: 06/69677755. Newsletter è consultabile sul sito Internet www.garanteprivacy.it