



Associazione Italiana
Information Systems Auditors



Il XXII Convegno AIEA e altro.....

Questo numero esce con qualche giorno di ritardo, perché volevamo dare, ai soci che non sono potuti venire al Convegno di Parma, alcune informazioni sull'evento.

Come già a Livorno, l'anno scorso, anche a Parma la platea dei soci è stata numerosa e partecipe. Un grazie a tutti i partecipanti ed ai relatori che, con la loro professionalità, hanno esposto temi interessanti ed innovativi, dando un panorama ampio dello stato dell'arte e delle prospettive future.

Un particolare ringraziamento al dr. Maurizio Ruggerini (Responsabile della Direzione Audit del gruppo Cariparma-Friuladria) ed al socio dr. Maurizio Guasti (Responsabile della Funzione Auditing Strutture Centrali del gruppo Cariparma-Friuladria), che ci hanno permesso di accedere al prestigioso Auditorium della Banca, mettendoci a disposizione strutture e persone per la migliore riuscita dell'evento.

Quest'anno, i presenti sono stati quasi 150, il numero più alto registrato per il nostro convegno.

I commenti nel "foyer" e la lettura dei questionari di valutazione ci aiuteranno a migliorare sempre più l'organizzazione di eventi.

Rinnovo della convenzione tra AIEA e la casa editrice NUOVA PERIODICI ITALIA.

Sono stati 183 i soci che hanno richiesto l'abbonamento a CW e che riceveranno, per 12 mesi, le seguenti pubblicazioni:

- * Computerworld (con allegato Network World) 45 numeri
- * CSO (4 numeri)
- * CIO (5 numeri)

Ricordiamo che l'abbonamento, al prezzo speciale di 7 euro, viene erogato direttamente da AIEA e nulla è dovuto dal socio sottoscrittore.

Da Protiviti riceviamo.....(vedi allegato S&P)

Sperando di far cosa gradita, Le segnaliamo che alcune settimane fa la società di rating Standard & Poors ha annunciato di voler proseguire nel progetto di analisi dei processi ERM ai fini dell'attribuzione dei meriti di credito alle società operanti in settori diversi da quello finanziario e dell'Energia.

L'iniziativa costituisce un'ulteriore occasione per avviare quanto prima processi di assessment sull'adeguatezza dei processi implementati per l'identificazione, misurazione, valutazione, gestione e monitoraggio dei principali rischi di business.



In allegato, un flash illustrativo dell'iniziativa di recente annunciata da S&P.

Gruppi di ricerca

Gruppo di Lavoro "Traduzione COBIT 4.1"

Dopo la diffusione dei primi due domini, disponibili sul sito (area Downloads), sono in corso sia il controllo qualità sia l'editing finale degli altri domini.

Gruppo di Lavoro "Business Continuity"

E' in corso il controllo qualità del documento finale. Si prevede che venga rilasciato entro la fine dell'anno.

Gruppo di Lavoro "COBIT-Legge 262"

Il 5 giugno 2008 si è tenuta a Parma la prima riunione del Gruppo di Ricerca: COBIT(tm) e Legge 262/05.

Il GdR ha l'obiettivo di redigere un documento che entro l'anno 2008 andrà ad arricchire la collana delle "GuideAIEA" contenente le linee guida e i modelli di riferimento per l'applicazione del COBIT(tm) ai fini della definizione di procedure previste dalla L.262/05 a fronte del controllo interno sulla componente tecnologica inerente procedure contabili e di bilancio.

Hanno dato la loro adesione al GdR Soci AIEA appartenenti a 10 grandi realtà aziendali nei settori Bancario, Postale, delle Telecomunicazioni, Automobilistico e della Revisione Contabile che intendono mettere a confronto e al servizio della professione le esperienze fatte in questa materia in sede di prima applicazione.

L'utilità della ricerca è legata alla opportunità di fornire schemi e impostazioni pratiche che possano guidare sia la prima applicazione per i nuovi soggetti obbligati, sia percorsi di efficientamento nelle applicazioni degli anni a seguire il primo per i soggetti che abbiamo già adottato un proprio framework di controllo, sia infine percorsi virtuosi di controllo interno sulle procedure contabili e di bilancio per realtà aziendali complesse, ancorchè non formalmente obbligate.

Il numeroso GdR è stato articolato in sei sottogruppi tematici per raggiungere in tempi ragionevoli e con alta qualità dei contenuti il risultato di coprire tutte le diverse tematiche che la redazione e applicazione delle procedure di controllo richieste dalla Legge 262 hanno sollevato.

Esame CISA e CISM

I corsi organizzati da AIEA si sono conclusi, la data dell'esame è oramai passata e, come ogni anno, aspettiamo i risultati!

A conferma della sempre maggiore importanza della certificazione CISA, quest'anno, a Milano, la sede di esame è stata la prestigiosa Università Cattolica. Dopo alcune difficoltà logistiche, emerse negli anni scorsi, AIEA si è prodigata per trovare una sede adeguata all'importanza dell'esame. Ringraziamo l'Università Cattolica per l'ospitalità accordata.

A metà luglio inizia l'iscrizione per l'esame di dicembre 2008. Ci si potrà iscrivere fino al 24 settembre ma solo fino al 20 agosto si potrà usufruire di una quota ridotta.

I prossimi eventi di AIEA



Calendario Eventi AIEA

Luglio

24Milano – Assemblea soci

Settembre

25.....Torino – Sessione di studio

Ottobre

8Milano – Sessione di studio

9.....Roma - Sessione di studio

17.....Veneto - Sessione di studio

Notizie da ISACA 1

Riceviamo da ISACA:

Member Benefit of the Month: **ISACA Career Centre**

The ISACA Career Centre is dedicated exclusively to information systems audit, control, security and assurance professionals, and it is free for job seekers. The résumé/CV posting and e-mail notification services are reserved for ISACA members only. The ISACA Career Centre is available at www.isaca.org/careercentre.

Certification Update

March Certifications

In March 2008, 1,442 Certified Information Information Security Manager[®] (CISM[®]) IT[™] (CGEIT[™]) candidates completed their



Systems Auditor[™] (CISA[®]) candidates, 202 Certified candidates and 18 Certified in the Governance of Enterprise requirements and were awarded their respective certification.

CGEIT Certification and Exam

- Applications under the 2008.



Updates

grandfathering provision will be accepted until 31 October



- The first CGEIT exam will be offered on 13 December 2008 at the same locations as the CISA and CISM exams. The exam will consist of 120 multiple-choice questions and will be offered in English only. Registration for the December exams will begin in early July at www.isaca.org/examreg.
- ISACA is eliciting the support of professionals around the world to construct a quality CGEIT certification exam. Exam item submissions are being reviewed for the CGEIT exam. Professionals with enterprise IT governance experience and interested in supporting this effort can become involved by visiting www.isaca.org/cgeit and choosing "Exam Item Writer Program" from the navigation list on the left.

Ricordiamo i prossimi eventi ISACA:

Calendar of Events

Dates of conferences are indicated in **RED**; other dates and deadlines are indicated in **BLACK**.

June

- 19-20 June **Sarbanes-Oxley Symposium** Rosemont, Illinois, USA
- 23-27 June **ISACA Training Week**
Minneapolis, Minnesota, USA
- 25 June Early-bird registration deadline for Information Security Management Conference and Network Security Conference in Las Vegas, Nevada, USA

July

- 2 July Early-bird registration deadline for the Training Week in Edinburgh, Scotland, UK
- 16 July Early-bird registration deadline for the Training Week in Washington DC, USA
- 27-30 July **International Conference**
Toronto, Ontario, Canada

Il sito AIEA

Come già negli anni scorsi, anche quest'anno il nostro sito si è meritato l'ISACA Award. Dopo la medaglia d'oro e quella d'argento, ora abbiamo anche quella di bronzo.

Un grazie a Gianni Soperchi che, con la sua disponibilità, ci permette di mantenere aggiornato il sito.

Avviso ai soci

Rinnoviamo l'invito ai soci di 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!



Associazione Italiana
Information Systems Auditors



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.

Ci rivediamo a settembre

Con questo numero, anche la nostra Newsletter ...va in vacanza.

Saremo di nuovo con voi nel mese di settembre.

A tutti i soci, un augurio di un sereno periodo estivo, da parte di tutta la redazione!



Associazione Italiana
Information Systems Auditors



ESTRATTO NEWSLETTER ANSSAIF DEL 2/5/2008

Nuova forma di Social Engineering

Il Compartimento della Polizia Postale di Potenza ha individuato e denunciato due persone che avevano adottato una nuova forma di *social engineering* finalizzata non a carpire credenziali (logonid, password,...) da utilizzare direttamente in operazioni di Home Banking e similari, ma ad accedere alle caselle email delle potenziali vittime.

L'accesso alle mailbox delle vittime consentiva ai malfattori non solo di accedere a informazioni personali e riservate sugli utenti, ma li metteva anche in condizione di ricevere password di accesso ad ulteriori servizi Internet, oltreché ottenere tutti i dati anagrafici degli utenti poco accorti caduti nella trappola, con conseguente furto di identità.

Il meccanismo adottato aveva inizio con email di "spamming" con le quali gli ideatori della truffa, seguendo un rituale ormai consolidato (phishing), inducevano gli utenti a cliccare su un indirizzo web inserito nel messaggio stesso. Un indirizzo che portava gli sprovveduti su due siti all'apparenza del tutto identici a quelli dei propri fornitori di servizi di posta elettronica, siti nei quali le vittime inserivano username e password, in cambio dei quali ricevevano un errore di connessione.

I legittimi proprietari delle mailbox, ovviamente, per molto tempo non si sono accorti di aver "condiviso" le proprie caselle email con degli sconosciuti: sono centinaia le persone che sembrano aver subito questa truffa. Un raggio scoperto soltanto quando alcuni utenti hanno denunciato l'accesso abusivo a conti correnti bancari online e ad altri servizi, una circostanza che ha messo la Polizia Postale sulle tracce dei due uomini ritenuti responsabili di quanto accaduto.

Sulle due persone fermate sono state mosse accuse di accesso abusivo a sistemi informatici, sottrazione di codici di accesso personali, furto di identità (sostituzione di persona, art. 494 C.P.)



ESTRATTO NEWSLETTER ANSSAIF DEL 4/6/2008

Sicurezza e utenti interni

Un recente sondaggio che ha interessato oltre 7.000 professionisti di sicurezza in tutto il mondo, ha fatto emergere che le Aziende sono molto più preoccupate che in passato dei rischi rappresentati dalle minacce provenienti dall'interno e pongono sempre maggiore attenzione sulla formazione del personale e la protezione dei dati.

I punti più significativi della ricerca:

Il 51% del campione ha ammesso di considerare come minaccia principale la propria forza lavoro interna. Percentuale questa cresciuta rispetto ad un analogo sondaggio del 2006. Fenomeno che può trovare giustificazione con l'aumento del numero di dipendenti che operano da remoto: "Ciò ha accresciuto le possibilità di attacco da parte di un aggressore, sia esso un dipendente disonesto che uno in buona fede ma in possesso di dispositivi che non gli consentono un accesso protetto ai dati da remoto".

Il 48% degli intervistati è convinto che la sicurezza non la si implementa unicamente con strumenti tecnologici. Tutti sono difatti convinti che il rispetto volontario delle policy aziendali di sicurezza è stato il fattore principale ad aver garantito fino ad oggi una sufficiente protezione dei dati. Per questo si è rilevata una maggiore propensione delle aziende ad investire in formazione del proprio personale.

E' stato rilevato inoltre un crescente interesse nel proteggere i dati di natura confidenziale. Circa il 68% degli intervistati prevede un aumento della spesa nel 2008 per la protezione dei dati: il 66% considera più importante la sicurezza dei database, mentre il 58% reputa vitali i processi di rimozione e conservazione dei dati.

Nuova forma di Phishing

Oltre a far leva su vincite di televisori, accrediti sui conti, assegnazione per sorteggio di apparati tecnologici, comunicazione di reati e preavviso di sanzioni al codice della strada, si sta diffondendo in questi giorni una diversa forma di *social engineering* che utilizza la formula del "*rimborso su ritardi dei treni*" e sembra provenire da Trenitalia SpA.

La mail che viene inviata, a firma di un presunto responsabile rimborsi Trenitalia SpA, si presenta come segue:

Da: *Trenitalia* [mailto:trenitalia@rimborsi-online.com]
Inviato: *mercoledì 4 giugno 2008 0.02*
A: *info@anssaif.it*
Oggetto: *Rimborso Trenitalia*

Gentile Viaggiatore,
Ferrovie dello Stato è lieta di informarla che dal 1° Maggio 2008 è possibile richiedere il rimborso sui ritardi effettuati su tutte le tratte nazionali.

A seguito di ciò, la informiamo che da un nostro controllo contabile, le spetta un rimborso di Euro 780,00.

La invitiamo a visualizzare il modulo in allegato, e seguire le istruzioni per farci pervenire tale modulo.

N.B. Il rimborso avverrà mediante bonifico bancario entro e non oltre 5 giorni lavorativi dalla ricezione.

Qualora si verificassero problemi con il mdulo allegato, può visitare il nostro [sito](#) o scaricare nuovamente il modulo [qui](#)

Certi di averle fatto cosa gradita Porgiamo Distinti Saluti

Ennio Zibris
Responsabile Rimborsi
Trenitalia S.p.A.

Alla mail viene allegato un file "*MODULO_A344508.zip*" (642 B) che, unzippato, risulta contenere due file entrambi di 1Kb NESSUNO DEI QUALI APRIBILE e precisamente:

? AcrobatReader.txt



Associazione Italiana
Information Systems Auditors



? MODULO344508.pdf.txt

La pericolosità di tale tecnica di social engineering consiste proprio nella furbizia adottata: nell'impossibilità di aprire i moduli allegati (CHE NON CONTENGONO NULLA) il destinatario della mail viene invitato a visitare il sito www.rimborsi-online.com dal quale scaricare il modulo citato zippato.

Tuttavia il file ZIP che si scarica, contiene un EXE al cui interno si annida il virus

"Trojan-Downloader.Win32.Agent.lyg"

(Engine error code: 0x00010000: Engine version: 5.0.0.38: Pattern version: 080604.093211.828550: Pattern date: 2008.06.04 09:32:11) individuato dai più comuni antivirus, se installati.

Il sito civetta, per completezza di informazione, risulta essere stato registrato in California il 2 giugno 2008 a nome di un utente anonimo (*WhoisGuard Protected (a3d100cd29d0483b960f33ed32667381.protect@whoisguard.com)*) che ha fornito come indirizzo "8939 S. Sepulveda Blvd. #110 - 732 Westchester, CA 90045"



ESTRATTO Newsletter CLUSIT del 31/05/2008- www.clusit.it

[disponibile in PDF all'indirizzo www.clusit.it/newsletter_31_05_08.pdf]

=====
Cronaca dell'attacco informatico all'estonia Pubblicata su ITnews Australia
(<http://www.itnews.com.au/News/76651,expert-dissects-estonian-cyberwar.aspx>).

A security researcher involved in defending against last year's Web attacks on Estonia has shared his account of the crisis, and is offering advice on how to prevent similar assaults in the future.. Gadi Evron has published an article in the Georgetown Journal of International Affairs (<http://journal.georgetown.edu/>) detailing his experiences in helping Estonia's government defend against a "cyber-riot" from Russian nationalist hackers.

Il racconto dell'esperto che ha aiutato il governo Estone a difendersi, è disponibile su <http://www.ciaonet.org/journals/gjia/v9i1/0000699.pdf>.

(Autore: Stefano Quintarelli)

=====
VULNERABILITÀ IN SOFTWARE SCADA

E' forse la prima volta che una vulnerabilità di un pacchetto software SCADA (<http://en.wikipedia.org/wiki/SCADA>) di grande diffusione (alcune centinaia di migliaia di installazioni al mondo, in molti settori, dai processi industriali, chimici ecc., alle infrastrutture ed utilities), per applicazioni per automazione di fabbrica e controllo di processo, supervisione e monitoraggio di impianti, finisce sotto i riflettori degli addetti alla security dei sistemi utilizzati nell'industria e nelle infrastrutture.

"A vulnerability was found in Wonderware SuiteLink Service (slssvc.exe) that could allow an un-authenticated remote attacker with the ability to connect to the SuiteLink service TCP port to shutdown the service abnormally by sending a malformed packet. Exploitation of the vulnerability for remote code execution has not been proven, but it has not been eliminated as a potential scenario."

(vedi www.coresecurity.com/?action=item&id=2187)

A fronte di questa segnalazione si è acceso un vivace dibattito nella community del comitato ISA s99 (Industrial Automation and Control System Security).

Per molti è suonata la sveglia (non ci si può più fidare della security dei prodotti per l'automazione industriale out-of-the-box) ed è necessario quindi iniziare a pensare alla cyber security come processo anche in ambiente industriale, identificare i rischi, pensare ad adeguate contromisure.

Di Cyber-Security Industriale ne abbiamo parlato anche nel 2007: Clusit ha pubblicato il quaderno dal titolo "Introduzione alla protezione di reti e sistemi di controllo ed automazione (DCS, SCADA, PLC, ecc.)" che si può scaricare da www.clusit.it/download/Q07_web.pdf. (Autore: Enzo Maria Tieghi)

=====
AL VIA LA 4a EDIZIONE DEL PREMIO TESI

Sono già aperte le iscrizioni alla quarta edizione del premio Clusit > "Innovare la Sicurezza delle Informazioni". Il premio, riservato alle migliori tesi sulla sicurezza delle informazioni, ha lo scopo di promuovere una collaborazione tra i soggetti che si occupano di sicurezza informatica in Italia:



le aziende, le Università, gli studenti. Un punto scambio tra mondo produttivo e mondo scientifico, tra studenti e mondo del lavoro, alimentato direttamente dai singoli soggetti che vi partecipano portando i propri bisogni e le proprie esperienze.

La Commissione designata ad assegnare il Premio sarà costituita da membri del Comitato Tecnico Scientifico, membri del Comitato Direttivo e Soci CLUSIT.

Le iscrizioni saranno accettate fino al 31.12.2008 e la premiazione si svolgerà durante Infosecurity 2009.

Le prime 5 tesi classificate saranno premiate ed in particolare il primo riceverà la somma di 2.000 €; al secondo classificato sarà offerto un Corso di preparazione alla certificazione internazionale ISECOM OPST - OSSTMM Professional Security Tester; al terzo classificato un corso Lead Auditor ISO IES 27001.

A tutti i classificati sarà accordata l'adesione gratuita al Clusit per il 2009. Sul portale <https://tesi.clusit.it/> sono disponibili tutte le informazioni sul premio.

=====
INIZIATIVA CLUSIT PER LE PICCOLE E MICROIMPRESE
=====

Continua l'attività del CLUSIT per favorire l'introduzione di una corretta gestione del rischio ICT nelle piccole e microimprese italiane. Per intervenire sulle microimprese è necessario un modello che sia facilmente scalabile sui grandi numeri e che tenga conto delle competenze disponibili sul territorio. Per questo, il CLUSIT sta sviluppando un modello di intervento che coinvolge fortemente le associazioni imprenditoriali, che sono in grado di individuare le esigenze dei loro associati, di veicolare informazioni e di tutelare gli associati riguardo all'adeguatezza di quanto viene loro proposto.

.....
Naturalmente il CLUSIT è interessato al supporto di queste iniziative da parte di aziende e sponsor. Chi fosse interessato, può contattare ctelmon@clusit.it. Parallelamente a questa attività, continua la partecipazione al gruppo di lavoro di ENISA sulle esigenze di sicurezza delle informazioni delle microimprese. La partecipazione a questo gruppo di lavoro permette fra l'altro di scambiare informazioni ed esperienze con rappresentanti di altri paesi, di individuare best practices e di discutere le difficoltà e i vantaggi delle diverse iniziative in atto in Europa.

(Autore: Claudio Telmon, coordinatore del progetto Clusit "Rischio IT e piccola impresa")

=====
NOTIZIE E SEGNALAZIONI DAI SOCI
=====

Convegno sul Computer Forensics Investigation.

Mercoledì 18 Giugno 2008 - Ore 9:30 - Aula Magna "Francesco Leoni" presso la Libera Università S. Pio V (Roma).

Il programma dell'evento è disponibile sul sito <http://www.cfitaly.net>

Sono stati pubblicati i bandi relativi alla V edizione del Master di I livello in "Sicurezza dei sistemi e delle reti informatiche per l'impresa e la Pubblica Amministrazione" ed alla III edizione del Master di II livello in "Gestione della sicurezza informatica per l'impresa e la Pubblica Amministrazione"- a.a. 2008/2009, attivati dal Dipartimento di Informatica dell'Università degli Studi di Roma "La Sapienza", la cui didattica anche quest'anno si svolgerà il venerdì pomeriggio ed il sabato mattina.

I Corsi avranno inizio a fine ottobre 2008 per terminare a luglio 2009. La data di scadenza per la presentazione delle domande è fissata per l'08/10/2008.

Maggiori informazioni sono disponibili su <http://mastersicurezza.uniroma1.it/>



- PASSWORD PIÙ SICURE CON IL RICONOSCIMENTO VOCALE
- GRADUATORIE ON LINE: NO A ELENCHI SEPARATI PER LE CATEGORIE PROTETTE
- L'INDAGINE EUROBAROMETRO SULLA PROTEZIONE DATI IN UE: ANCORA MOLTE OMBRE

Password più sicure con il riconoscimento vocale

Password più sicure con il riconoscimento vocale. Il Garante privacy ha autorizzato una multinazionale ad utilizzare un sistema di riconoscimento biometrico basato sul rilevamento delle impronte vocali dei propri dipendenti per gestire in maniera sicura e reimpostare automaticamente la password necessaria per accedere ai sistemi informatici. La società, che dovrà informare i dipendenti sul trattamento dei dati biometrici e acquisirne il consenso, dovrà comunque garantire sistemi alternativi per cambiare le password.

Il sistema di rilevamento biometrico, sottoposto alla verifica preliminare dell'Autorità, si basa sull'identificazione dell'utente attraverso l'elaborazione dell'impronta vocale, registrata e memorizzata su un server. Per la trasmissione dei dati è previsto l'uso di una rete protetta.

Gli utenti durante la cosiddetta fase di addestramento, "parlano" per telefono con il sistema pronunciando per quattro volte tre coppie di parole per rendere possibile la registrazione della voce. Le informazioni vocali così raccolte vengono trasformate in un modello di riferimento digitale ("template") che il sistema confronta con le parole pronunciate dall'utente che intende cambiare password. Una volta accertata l'identità dell'utente, il sistema procede automaticamente ad impostare la parola chiave comunicandola al dipendente. Nell'ambito della verifica preliminare il Garante ha ritenuto (con un provvedimento di cui è stato relatore Giuseppe Fortunato) che il sistema sottoposto alla sua attenzione sia in grado di garantire, per il rinnovo delle password d'accesso dei dipendenti ai servizi informatici, un elevato livello tecnologico di sicurezza, tenuto anche conto che l'impronta vocale, acquisita e codificata secondo il processo descritto, sarebbe impossibile da "ricostruire" e, quindi, inutilizzabile per altri scopi. L'Autorità ha comunque prescritto alla società l'adozione di misure organizzative per prevenire

eventuali rischi di utilizzo abusivo dei dati personali raccolti nella fase di addestramento. Infine, in caso di cessazione del rapporto di lavoro devono essere tempestivamente cancellati tutti i dati del dipendente.

Graduatorie on line: no a elenchi separati per le categorie protette

Non si possono diffondere via web dati idonei a rivelare lo stato di salute di una persona, specie se questa appartiene ad una categoria protetta. E' quanto ribadito dall'Autorità nel richiamare due sedi provinciali del Ministero della pubblica istruzione che sul loro sito Internet avevano inserito i nominativi del personale cui sono riservati posti nei concorsi pubblici (in quanto appartenenti a categorie protette) in un elenco separato, che ne precisava le caratteristiche: "Gruppo 2 Disabili art 1 L.n. 68/99". La suddivisione dei riservisti in tre gruppi in base alla specifica disabilità, adottata da taluni uffici scolastici provinciali, era stata successivamente inibita, attraverso una circolare, dal Ministero della pubblica istruzione poiché questo tipo di trattamento di dati sensibili è eccedente rispetto all'obiettivo perseguito con la pubblicazione delle graduatorie e determina la diffusione di informazioni sullo stato di salute e sulle condizioni familiari degli interessati. Diversi uffici scolastici, tuttavia, avevano continuato a mantenere nella pubblicazione dei loro elenchi la suddivisione in gruppi.

A seguito di alcuni accertamenti, l'Ufficio del Garante ha individuato l'inadempienza dei due enti provinciali interessati ed ha constatato che la loro condotta non era conforme alla disciplina in materia di protezione dei dati personali. La dicitura utilizzata nel sito, infatti, riportava un dato in grado di rivelare lo stato di salute dei soggetti individuati. Ma soprattutto, ha sottolineato l'Autorità, non risultava espressamente prevista dalla normativa

vigente la costituzione di una separata graduatoria dei soggetti appartenenti alle categorie protette.

L'Ufficio del Garante ha pertanto richiamato l'ufficio invitandolo ad eliminare dalle graduatorie provinciali il separato "Elenco riservisti" "Gruppo 2 Disabili art. 1 L.n. 68/99" e ogni altra dicitura dalla quale si possa desumere l'appartenenza dei soggetti a specifiche categorie protette.

Da parte loro, i due uffici scolastici hanno immediatamente adempiuto e dato conferma al Garante dell'avvenuta cancellazione dell'elenco.

L'indagine Eurobarometro sulla protezione dati in Ue: ancora molte ombre

Il 64% dei cittadini europei è preoccupato per la propria privacy.

Per la quarta volta, dal 1991, un'indagine Eurobarometro prende in esame la percezione di cittadini ed imprese rispetto alla protezione dei dati personali in Europa (http://ec.europa.eu/public_opinion/flash/fl_226_en.pdf; http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf).

Il quadro che emerge è molto composito. Il campione comprende circa 27.000 cittadini nei 27 Paesi UE e 4.835 imprese ("titolari di trattamento"), intervistati ad inizio 2008. Le domande poste ai due gruppi, seppure formulate e organizzate in modo diverso, hanno riguardato sostanzialmente la conoscenza della normativa nazionale e dei propri diritti/doveri, la percezione del livello di pericolo per i propri dati personali, anche rispetto all'uso di Internet, la conoscenza delle autorità nazionali e del loro lavoro, il rapporto fra protezione dati e sorveglianza per finalità connesse alla lotta contro il terrorismo.

Sul versante cittadini, colpisce soprattutto l'elevata preoccupazione manifestata in tutti i Paesi per i propri dati personali (media: 64%), un dato che rimane sostanzialmente invariato nel corso degli anni; in Italia, tuttavia, solo 12 persone su 100 si dicono "molto preoccupate" al riguardo. I cittadini hanno scarsissima fiducia, in particolare, nelle società che fanno marketing, nelle centrali rischi e nelle agenzie di viaggio, mentre si fidano dei medici, delle forze dell'ordine e degli organismi di previdenza sociale – ed il livello di fiducia in questi ultimi soggetti è andato crescendo negli anni. Quali sono gli elementi positivi? In primo luogo, il fatto che la stragrande maggioranza dei cittadini sappia di avere alcuni diritti rispetto ai propri dati personali (opporsi all'uso per scopi di marketing diretto, dare il consenso, chiedere la cancellazione o rettifica) compreso il diritto ad un'informativa adeguata (2/3); l'Italia si

allinea sulla media europea in questi ambiti. Va poi sottolineato che più dell'80% sa che si corrono rischi specifici su Internet e che sono necessarie cautele adeguate a protezione dei dati; più del 40% di chi usa Internet (una percentuale molto più alta rispetto al 2004) sa che esistono tecnologie che possono aiutare gli utenti a difendersi, ad esempio, dal rischio di un furto di identità, e 1 su 4 vi ha fatto ricorso.

Sono però più numerose le ombre, come dicevamo. Più della metà dei cittadini non ritiene che la protezione offerta ai propri dati (dalle norme nazionali) sia sufficiente; più di un terzo, in media, non sa che un cittadino ha diritto al risarcimento in caso di danni derivanti da abusi dei suoi dati personali (in alcuni Paesi questa percentuale supera la metà degli intervistati); la metà non sa che ha il diritto di accedere ai propri dati personali detenuti da terzi. Appena 1 cittadino su 6 (17%) sa che non si possono trasferire dati verso Paesi extra-Ue che non garantiscono un livello adeguato di protezione (in Italia appena il 13% ne è consapevole). E poi: solo il 28% sa che esiste un'autorità nazionale incaricata della protezione dei dati (in Italia 1 cittadino su 3 ne è consapevole) – un dato che non è cambiato rispetto a quattro anni fa. Sembra quindi che ci sia molto da fare, soprattutto per sensibilizzare i cittadini rispetto ai propri diritti e far conoscere le attività ed i poteri delle autorità nazionali – anche perché un dato comune è che la conoscenza di diritti e doveri aumenta con il livello di educazione e l'età degli intervistati. Il fattore educazione risulta quindi estremamente importante: è su questo versante che le autorità sembrano chiamate ad impegnarsi di più.

Per quanto riguarda le "imprese", l'indagine mostra invece qualche ombra in meno. La metà non crede che le norme nazionali siano in grado di tutelare sufficientemente i cittadini, e circa il 50% non ritiene sufficiente l'armonizzazione delle norme a livello europeo; tuttavia, 9 imprese su 10 vedono positivamente l'esistenza di norme (nazionali ed europee) a tutela dei diritti dei cittadini in questo ambito, e solo 3 imprese su 10 non adottano misure di sicurezza nei trasferimenti di dati personali effettuati attraverso Internet (prassi comune al 65% di esse). Oltre la metà sa che esistono strumenti (come le Pet, Privacy Enhancing Technologies) che consentono di potenziare la tutela della privacy online; in Italia la percentuale è superiore al 65%. La consapevolezza dei doveri legati alla normativa in materia è diffusa, e qui l'Italia guida la classifica: il 96% delle imprese italiane sa che deve fornire un'informativa sulla privacy (o una privacy policy) e la aggiorna regolarmente, e più di 2/3 verifica quante volte la policy sia visitata dagli utenti. Ben 4 imprese su 10 in Italia hanno contattato il Garante (soprattutto per chiarimenti sulla normativa e/o in materia di notificazione dei trattamenti) – contro una media europea del 13%. Per l'80% delle imprese, inoltre, occorre concentrarsi in futuro su norme più armonizzate in materia di informativa, e ben il 75% chiede maggiori chiarimenti sull'applicazione di

definizioni e concetti-chiave della direttiva UE. Ancora una volta, c'è spazio per le attività di sensibilizzazione ed educazione da parte delle autorità di protezione dati; occorre rilevare, in modo particolare, che le iniziative adottate negli ultimi anni anche dalla Commissione europea e dal Gruppo Articolo 29 per una "migliore attuazione della direttiva" si sono concentrate sugli stessi obiettivi. Tuttavia, resta evidentemente ancora molto da fare.

Un discorso a parte merita il rapporto fra protezione dati e lotta al terrorismo, sul quale cittadini ed imprese hanno manifestato lo stesso atteggiamento. La maggioranza è nettamente favorevole ad una sorveglianza potenziata (telefono, Internet, linee aeree), ma è anche nettamente contraria a misure generalizzate e di durata illimitata. Sì, dunque, a misure di sorveglianza più severe se finalizzate alla lotta contro il terrorismo internazionale, ma deve trattarsi di misure limitate nel tempo e focalizzate su alcune categorie di soggetti (ad esempio, solo soggetti sospettati di appartenere ad organizzazioni di stampo terroristico – indicazione espressa da circa 1/3 degli intervistati).

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



- TELECAMERE CONDOMINIALI, SERVONO REGOLE CHIARE
- IL GARANTE AL COMUNE DI ROMA: OSCURATE SUBITO I DATI SULLA SALUTE
- PRIVACY E COMUNICAZIONI ELETTRONICHE

Telecamere condominiali, servono regole chiare

Telecamere condominiali, servono regole chiare. Il Garante per la protezione dei dati personali ha segnalato al Parlamento e al Governo l'opportunità di valutare l'adozione di una disciplina che regoli alcuni aspetti relativi al trattamento dei dati personali determinati dall'installazione di impianti di videosorveglianza nei condomini, materia allo stato non disciplinata specificamente.

Recenti quesiti e segnalazioni rivolti all'Autorità hanno infatti posto il caso in cui non i singoli condomini, ma l'intero condominio intende installare tali impianti in aree comuni, quali portoni d'ingresso, androni, cortili, scale, parcheggi, anche presso residence o multiproprietà. Dal loro esame emerge l'esistenza di due interessi contrapposti: da un lato l'esigenza di sicurezza delle persone e di tutela di beni comuni; dall'altro, la preoccupazione dei singoli che gli impianti di videosorveglianza possano incidere sulla libertà di muoversi, senza essere controllati, nel proprio domicilio e all'interno delle aree comuni.

La questione sottoposta alle Camere non trova (né avrebbe potuto trovare) puntuale regolamentazione nel Codice civile del 1942 e, anche rifacendosi ai principi generali, non appare chiaro se l'installazione di sistemi di videosorveglianza possa essere effettuata in base alla sola volontà dei proprietari o se si debba tener conto anche del consenso di altri soggetti, in particolare dei conduttori; non risulta chiaro, poi, con quale tipo di maggioranza possa essere approvata. In questa materia, peraltro, non può essere sottovalutato il divieto contenuto nell'art. 615 bis del codice penale che sanziona chiunque si procura indebitamente immagini relative alla vita privata che si svolge nel domicilio, nozione che secondo alcune decisioni giurisprudenziali può giungere fino a ricomprendere le aree comuni; cosa che comporterebbe la necessaria acquisizione del consenso di un numero assai ampio di soggetti, non sempre di agevole identificazione.

Il Garante al Comune di Roma: oscurate subito i dati sulla salute

E' vietato diffondere dati sullo stato di salute. Il principio è stato riaffermato dal Garante privacy che ha disposto, in via d'urgenza, il "blocco" di dati sanitari pubblicati su tre siti web, tra cui quello istituzionale del Comune di Roma. "Invalido", "figlio di invalido per servizio" erano le diciture, in grado di fornire informazioni sulla salute, che comparivano in Internet accanto ai nomi di alcuni idonei a un concorso per istruttore di polizia municipale nella graduatoria pubblicata on line. Dubbi sulla liceità della loro diffusione erano stati segnalati al Garante da un cittadino. Con il "blocco" il Comune e le due società che gestiscono i siti hanno dovuto oscurare i dati sanitari dei concorrenti e limitarsi alla sola conservazione, in attesa di ulteriori accertamenti che il Garante ha avviato per valutare la conformità delle modalità di diffusione della graduatoria al Codice privacy. Al provvedimento inibitorio di blocco, al quale il Comune di Roma ha già ottemperato, si è giunti al termine di una prima verifica dalla quale è emerso un grave illecito. Contrariamente a quanto previsto dalla legge, infatti, che vieta la diffusioni di dati sanitari, alcuni dei titoli di preferenza (invalido, figlio di invalido per servizio, di guerra ecc.) indicati accanto ai nomi dei concorrenti erano in grado di rivelare lo stato di salute dei partecipanti o dei loro familiari. Tali dati per la loro stessa presenza in Internet risultavano, peraltro, immediatamente accessibili a chiunque, attraverso una semplice ricerca nominativa effettuata in rete, anche tramite i motori di ricerca. Il Comune ha immediatamente adempiuto al provvedimento del Garante.

Privacy e comunicazioni elettroniche

I Garanti Ue chiedono più sicurezza per cittadini e consumatori

Per i Garanti europei, il futuro quadro normativo in materia di privacy e comunicazioni elettroniche, sul quale stanno lavorando le istituzioni comunitarie, dovrà garantire più efficacemente la sicurezza delle reti e facilitare l'esercizio dei diritti degli utenti.

Il Gruppo Articolo 29, che riunisce le Autorità europee per la protezione dei dati, ha elaborato un parere sulle proposte di modifica della direttiva detta "e-Privacy" (2002/58) in materia di comunicazioni elettroniche (link: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp150_en.pdf). Va sottolineato che il pacchetto di proposte della Commissione comprende anche una "proposta di Regolamento" concernente l'istituzione di un'Autorità europea di regolazione del mercato delle comunicazioni, fra i cui compiti rientra la definizione di standard di sicurezza paneuropei.

Il parere dei Garanti europei, che risale alla fine di maggio, condivide alcune delle osservazioni contenute nel documento pubblicato sullo stesso tema dal Garante europeo per la protezione dei dati (10 aprile 2008). I Garanti concordano sull'opportunità di guardare alle reti in una prospettiva più ampia, data la loro natura sempre più spesso "mista" (pubblica/privata), su alcuni emendamenti proposti dalla Commissione: in particolare, l'applicabilità delle disposizioni della direttiva a tecnologie quali le cosiddette "etichette elettroniche" Rfid (in quanto utilizzano "reti di comunicazione elettronica disponibili al pubblico" per veicolare i segnali di trasmissione), e l'attribuzione del diritto di intraprendere azioni legali in caso di violazioni della normativa nazionale (ad esempio, in materia di spam) anche a soggetti non direttamente colpiti, ma comunque direttamente interessati, quali i provider di servizi Internet.

A tutto questo si aggiunge la proposta di estendere l'obbligo per i provider di servizi di comunicazione di notificare violazioni e/o rischi per la sicurezza delle reti a tutti gli "utenti" dei servizi di comunicazione elettronica (anziché ai soli "abbonati" a tali servizi); ciò dovrà avvenire secondo un approccio equilibrato che tenga conto dei costi e dell'impatto che tali notifiche possono esplicare sull'attività dei provider (ad esempio, in termini di danno di immagine). Inoltre, il Gruppo ha segnalato l'opportunità di ampliare la definizione di "sistemi di chiamata" contenuta nella direttiva 2002/58 (art. 13) includendovi i sistemi di "comunicazione" (per tenere conto degli sviluppi tecnologici legati, ad esempio, alla tecnologia Bluetooth, il cui funzionamento è difficilmente assimilabile ad una "chiamata" sul terminale dell'utente); ciò consentirebbe di garantire una protezione più efficace nei confronti delle comunicazioni indesiderate. Per lo stesso motivo,

l'estensione del "diritto di intraprendere azioni legali" dovrebbe comprendere anche le violazioni dell'articolo 5.3 della direttiva, ossia l'uso e l'installazione, per esempio, di spyware.

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



- PRIVACY E SEMPLIFICAZIONI
- ATTENZIONE A NON CONSERVARE I DATI DEI CLIENTI A TEMPO INDETERMINATO
- RINNOVATE LE AUTORIZZAZIONI GENERALI PER I DATI SENSIBILI E GIUDIZIARI
- INGEGNERI E DATI NELL'ARCHIVIO DELL'ENTE PREVIDENZIALE

Privacy e semplificazioni

Intervento del Garante per l'ordinaria gestione amministrativa e contabile

Privacy meno burocratica soprattutto per piccole e medie imprese, liberi professionisti e artigiani. Garanzie effettive per i cittadini. Sono i principi alla base del provvedimento generale sulla semplificazione adottato dal Garante privacy, pubblicato oggi nella Gazzetta Ufficiale n. 152 e consultabile sul sito www.garanteprivacy.it. L'intervento dell'Autorità prosegue nel percorso di semplificazione degli adempimenti per alcune categorie già intrapreso e individua soluzioni concrete per agevolare ulteriormente l'ordinaria attività di gestione amministrativa e contabile in ambito pubblico e privato, soprattutto in quei casi in cui non sono trattati dati sensibili o giudiziari. Basta con i moduli lunghi e burocratici, basati sull'eccessivo uso di espressioni giuridiche che non aiutano a far comprendere ai cittadini come sono trattati i loro dati personali. Un'informativa snella, essenziale, efficace e un consenso richiesto solo nei casi veramente necessari, una tutela effettiva dei diritti dei cittadini: sono i principali obiettivi delle nuove linee guida del Garante.

Informativa. L'Autorità ha fornito indicazioni per la redazione di un'informativa unica per il complesso dei trattamenti di dati personali a fini esclusivamente amministrativi e contabili. Gli operatori possono anche redigere una prima informativa breve (un modello è stato messo a punto dal Garante) che può rinviare a un testo più articolato disponibile, su siti Internet, reti Intranet, in bacheca o presso gli sportelli. L'Autorità ha invitato le associazioni di categoria a predisporre informative-tipo per determinati settori o categorie di trattamenti. Il Garante prevede anche di mettere a disposizione gratuitamente un kit di istruzioni concrete e fac-simili per semplificare gli adempimenti.

Consenso: Per quanto riguarda il consenso l'Autorità ha indicato i casi in non deve essere chiesto ad esempio quando i trattamenti sono svolti per adempiere ad obblighi contrattuali o normativi o quando i dati provengono da pubblici registri e elenchi pubblici, o sono relativi allo svolgimento di attività economiche.

Attenzione a non conservare i dati dei clienti a tempo indeterminato

Le aziende che raccolgono dati dei loro clienti, anche di quelli potenziali, non possono tenerli a tempo indeterminato.

Sulla base di questo principio l'Autorità per la privacy ha imposto ad una società di individuare, entro il 15 luglio, tempi massimi di conservazione dei dati personali raccolti e utilizzati.

L'azienda commercializza oggetti per la casa in occasione di visite dimostrative effettuate dai propri incaricati. I potenziali clienti richiedono un incontro e forniscono, per telefono o tramite il sito della società, i dati personali per venire contattati.

Dagli accertamenti dell'Autorità per verificare il rispetto delle norme sulla protezione dei dati personali riguardo le vendite a distanza, è emerso che l'azienda conservava non soltanto i dati anagrafici e i recapiti dei clienti che avevano poi comperato i prodotti, ma anche le schede anagrafiche (circa 400.000) di quanti non avevano effettuato alcun acquisto.

Dalle verifiche è risultato anche che la società raccoglieva i dati dei clienti non soltanto per organizzare incontri dimostrativi, ma anche per successivi contatti. Tuttavia, sia l'informativa fornita ai clienti dal call center, sia quella presente sul sito web dell'azienda, risultava incompleta e inadeguata. Inoltre, pur essendo presente la finalità di marketing, non veniva richiesto uno specifico consenso per poter utilizzare i dati anche a questo scopo. L'azienda dovrà quindi riformulare correttamente l'informativa.

Per quanto riguarda il periodo di conservazione, il Garante ha ribadito che i dati non possono essere conservati per un periodo superiore a quello necessario per il perseguimento dello scopo per il quale essi vengono raccolti e utilizzati.

“I dati che un cliente ha fornito non possono tendenzialmente essere utilizzati a tempo indefinito. Non è possibile che per il solo fatto di aver una volta soltanto acquistato un bene si debba essere contattati per altre

offerte - ha dichiarato Giuseppe Fortunato, relatore del provvedimento. - "Inoltre, è bene ricordare che per utilizzare i dati a fini di marketing occorre l'espresso e chiaro consenso del cliente. Per questo rivolgo un invito alle associazioni imprenditoriali di categoria e alle associazioni di consumatori, affinché vigilino su una corretta applicazione delle norme a protezione dei dati e segnalino al Garante i casi di violazione. Solo una chiara policy-privacy nel mondo imprenditoriale e associativo, chiaramente condivisa e vigorosamente perseguita, - ha concluso Fortunato - può far sì che i cittadini non vengano disturbati da offerte sgradite e che gli imprenditori che operano correttamente non subiscano danni da quelli senza scrupoli".

Rinnovate le autorizzazioni generali per i dati sensibili e giudiziari

Il Garante per la protezione dei dati personali ha rinnovato le autorizzazioni per i dati sensibili e giudiziari che saranno efficaci dal 1° luglio 2008 sino al 31 dicembre 2009.

I sette provvedimenti in corso di pubblicazione sulla Gazzetta Ufficiale riguardano datori di lavoro, operatori sanitari, associazioni, banche, assicurazioni, liberi professionisti, investigatori privati che per ragioni di lavoro o d'ufficio utilizzano dati di carattere giudiziario e sensibile (salute, origini etniche e razziali, opinioni politiche, convinzioni religiose, appartenenza a partiti o sindacati).

Le nuove autorizzazioni non recano significative modifiche rispetto a quelle in scadenza, alle quali sono state apportate solo alcune integrazioni relative a modifiche normative intervenute nei settori considerati.

Ingegneri e dati nell'archivio dell'ente previdenziale

Si può scegliere lo studio professionale come domicilio per ricevere la corrispondenza

Gli ingegneri possono indicare l'indirizzo dello studio professionale come domicilio eletto per ricevere la corrispondenza dell'ente di previdenza al quale sono iscritti. È quanto precisato dal Garante nell'accogliere il ricorso di un ingegnere che ha richiesto di integrare i dati conservati negli archivi dell'Inarcassa, l'associazione che assicura la previdenza e l'assistenza obbligatoria di ingegneri e architetti liberi professionisti, con quelli relativi al proprio domicilio.

Viste le difficoltà a ricevere le comunicazioni dell'associazione in orario lavorativo al suo indirizzo di residenza, il professionista aveva richiesto invano all'ente previdenziale la cancellazione dell'indirizzo di residenza, la rettificazione o l'inserimento dell'indirizzo del proprio studio professionale per l'inoltro della corrispondenza. Si era dunque rivolto al Garante sottolineando l'interesse a ricevere le comunicazioni presso il proprio studio.

L'Autorità, con un provvedimento di cui è stato relatore Giuseppe Fortunato, ha considerato legittima la richiesta di integrazione dei dati relativi al domicilio ordinando al titolare di aderire alla richiesta dell'ingegnere. Ai sensi dell'articolo 47 del Codice civile, infatti, una persona può eleggere domicilio speciale per determinati atti e affari comunicandolo per iscritto.

Del resto, anche riguardo ai dati personali contenuti negli albi professionali, il Codice privacy consente l'integrazione con ulteriori dati che siano pertinenti e non eccedenti rispetto all'attività professionale.

Il Garante ha ritenuto, invece, infondata la richiesta di cancellazione del dato relativo alla residenza, precisando che può essere conservato negli archivi e lecitamente utilizzato per finalità statutarie, e che lo stesso dato non può essere rettificato con l'indirizzo dello studio professionale trattandosi di due informazioni diverse.

L'attività del Garante.

Per chi vuole saperne di più

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

- Garante privacy su censimento nomadi – Comunicato del 26.6.2008

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