

Indice

1. LAVORO: LE LINEE GUIDA DEL GARANTE PER POSTA ELETTRONICA E INTERNET
2. CERTIFICAZIONE DELLA PROTEZIONE DEI DATI: L'INIZIATIVA SVIZZERA
3. CYBERCRIME
4. INFOSECURITY ITALIA 2007: BILANCIO FINALE
5. INFOSECURITY ROMA
6. DOCUMENTI ENISA
7. PRESENTATO IL RAPPORTO E-FAMILY 2007
8. NOTIZIE DAI SOCI
9. EVENTI SICUREZZA

1. LAVORO: LE LINEE GUIDA DEL GARANTE PER POSTA ELETTRONICA E INTERNET

Lavoro: le linee guida del Garante per posta elettronica e internet.

Le regole aziendali, il doppio indirizzo e-mail, il fiduciario, i siti non accessibili.

I datori di lavoro pubblici e privati non possono controllare la posta elettronica e la navigazione in Internet dei dipendenti, se non in casi eccezionali. Spetta al datore di lavoro definire le modalità d'uso di tali strumenti ma tenendo conto dei diritti dei lavoratori e della disciplina in tema di relazioni sindacali.

Il Garante privacy, con un provvedimento generale che sarà pubblicato sulla "Gazzetta Ufficiale", fornisce concrete indicazioni in ordine all'uso dei computer sul luogo di lavoro. "La questione è particolarmente delicata – afferma il relatore Mauro Paissan – perché dall'analisi dei siti web visitati si possono trarre informazioni anche sensibili sui dipendenti e i messaggi di posta elettronica possono avere contenuti a carattere privato. Occorre prevenire usi arbitrari degli strumenti informatici aziendali e la lesione della riservatezza dei lavoratori".

L'Autorità prescrive innanzitutto ai datori di lavoro di informare con chiarezza e in modo dettagliato i lavoratori sulle modalità di utilizzo di Internet e della posta elettronica e sulla possibilità che vengano effettuati controlli. Il Garante vieta poi la lettura e la registrazione sistematica delle e-mail così come il monitoraggio sistematico delle pagine web visualizzate dal lavoratore, perché ciò realizzerebbe un controllo a distanza dell'attività lavorativa vietato dallo Statuto dei lavoratori. Viene inoltre indicata tutta una serie di misure tecnologiche e organizzative per prevenire la possibilità, prevista solo in casi limitatissimi, dell'analisi del contenuto della navigazione in Internet e dell'apertura di alcuni messaggi di posta elettronica contenenti dati necessari all'azienda.

Il provvedimento raccomanda l'adozione da parte delle aziende di un disciplinare interno, definito coinvolgendo anche le rappresentanze sindacali, nel quale siano chiaramente indicate le regole per l'uso di Internet e della posta elettronica.

Il datore di lavoro è inoltre chiamato ad adottare ogni misura in grado di prevenire il rischio di utilizzi impropri, così da ridurre i controlli successivi sui lavoratori.

Per quanto riguarda Internet è opportuno ad esempio:

- individuare preventivamente i siti considerati correlati o meno con la prestazione lavorativa;
- utilizzare filtri che prevengano determinate operazioni, quali l'accesso a siti inseriti in una sorta di black list o il download di file musicali o multimediali.
- Per quanto riguarda la posta elettronica, è opportuno che l'azienda:
 - renda disponibili anche indirizzi condivisi tra più lavoratori (info@ente.it; urp@ente.it; ufficioreclami@ente.it), rendendo così chiara la natura non privata della corrispondenza;
 - valuti la possibilità di attribuire al lavoratore un altro indirizzo (oltre quello di lavoro), destinato ad un uso personale;
 - preveda, in caso di assenza del lavoratore, messaggi di risposta automatica con le coordinate di altri lavoratori cui rivolgersi;
 - metta in grado il dipendente di delegare un altro lavoratore (fiduciario) a verificare il contenuto dei messaggi a lui indirizzati e a inoltrare al titolare quelli ritenuti rilevanti per l'ufficio, ciò in caso di assenza prolungata o non prevista del lavoratore interessato e di improrogabili necessità legate all'attività lavorativa.

Qualora queste misure preventive non fossero sufficienti a evitare comportamenti anomali, gli eventuali controlli da parte del datore di lavoro devono essere effettuati con gradualità. In prima battuta si dovranno effettuare verifiche di reparto, di ufficio, di gruppo di lavoro, in modo da individuare l'area da richiamare all'osservanza delle regole. Solo successivamente, ripetendosi l'anomalia, si potrebbe passare a controlli su base individuale.

Il Garante ha chiesto infine particolari misure di tutela in quelle realtà lavorative dove debba essere rispettato il segreto professionale garantito ad alcune categorie, come ad esempio i giornalisti.

Fonte: Autorità Garante per la protezione dei dati personali
www.garanteprivacy.it

L'intero provvedimento è disponibile all'indirizzo:
www.garanteprivacy.it/garante/document?ID=1387522

Questo provvedimento, che interessa tutte le aziende, ha creato molto interesse. La materia è oggetto di un seminario Clusit Education, appena svoltosi a Milano e programmato a Roma per il prossimo 18 aprile (i posti sono ormai tutti esauriti) e a Firenze per il 9 maggio.

2. CERTIFICAZIONE DELLA PROTEZIONE DEI DATI: L'INIZIATIVA SVIZZERA

È quasi giunta al termine la revisione della legge federale svizzera sulla protezione dei dati.

La novità più rilevante è l'introduzione di un marchio di qualità sulla protezione dei dati, sia per le organizzazioni e le procedure che per i prodotti (programmi e sistemi).

Vengono stabiliti i requisiti che dovranno avere gli organismi di certificazione, che risultano in sostanza dalle guide ISO/IEC 62 e 65 (la prima divenuta norma ISO/IEC 17021, la seconda prossimamente sostituita da un'altra norma ISO). Tali norme specificano in particolare il principio di indipendenza e disciplinano la procedura di certificazione e di esame dei prodotti. In aggiunta, il progetto di revisione della legge federale specifica i requisiti di qualifica dei certificatori e del personale addetto agli esami dei prodotti.

Il progetto di revisione della legge federale è il frutto di un lungo e approfondito lavoro, cui hanno contribuito i colleghi del CLUSIS, con i quali ci complimentiamo per la qualità del lavoro ed il livello di approfondimento.

In questi anni in Italia, dopo l'entrata in vigore del DLGV 196/03, molte organizzazioni hanno chiesto al Clusit se ci fosse la possibilità di certificare le loro procedure di trattamento dei dati. Sicuramente non è il ruolo del Clusit ma in futuro potremmo contribuire ad una iniziativa simile nel nostro paese, ad esempio nella definizione dei requisiti di qualifica dei certificatori e del personale addetto alle verifiche.

3. CYBERCRIME

Inspector Lists Computers With Atomic Secrets as Missing - New York Times

www.nytimes.com/2007/04/01/washington/01missing.html?_r=1&oref=slogin

Il New York Times del 30 marzo ha riportato che dal dipartimento del governo americano responsabile della protezione dei segreti tecnici sulle armi nucleari da spie straniere, sono scomparsi 20 computer dei quali almeno 14 venivano usati per dati riservati.

Questa è la tredicesima volta in poco meno di 4 anni che un audit aveva messo in luce che il dipartimento aveva perso il controllo dei computer impiegati.

Questo rivela come la gestione dei computer, in particolare dei laptop e di ogni dispositivo mobile, rappresenti una delle vulnerabilità sempre crescenti. [n.d.r. Clusit]

4. INFOSECURITY ITALIA 2007: BILANCIO FINALE

Bilancio positivo per Infosecurity e Storage Expo 2007 (dal 6 all'8 febbraio scorsi in Fieramilanocity): tre giorni fitti di convegni, incontri, dimostrazioni,

e talk show hanno coinvolto oltre 5.500 visitatori (+3% rispetto alla precedente edizione).

Confermato l'interesse per la vetrina espositiva: un parterre di 170 aziende (+13% rispetto all'edizione 2006).

Buona l'accoglienza riservata alle due nuove aree tematiche dedicate alla Sanità e alla Tracciabilità – "Trackability". In particolare, il forte interesse verso quest'ultima conferma l'importanza delle nuove tecnologie di identificazione automatica e RFID per lo sviluppo di alcuni settori produttivi come, per esempio, quello agro-alimentare, che rappresenta il secondo comparto per fatturato annuo nel nostro Paese (100 miliardi di Euro nel 2005, secondo i dati Federalimentare) e che occupa 1 milione di operatori.

Buona l'affluenza media ai 20 convegni tenutisi nell'ambito della manifestazione.

Eccezionale l'interesse dimostrato per i seminari Clusit Education (in uno dei seminari l'affluenza era tale che è stato necessario trasferire il pubblico dalla sala inizialmente assegnata, con capienza di "soli" 110 posti, in una molto più capiente).

5. INFOSECURITY ROMA

Si rinnova l'appuntamento con Infosecurity e Storage Expo Italia a Roma, nei giorni 5 e 6 giugno 2007.

Il Clusit ha ancora una volta contribuito ad organizzare i principali appuntamenti convegnistici della manifestazione.

PROGRAMMA

Martedì 5 giugno (10.30-13.00) - Manifestazione di Apertura - Sicurezza delle informazioni e dei sistemi come servizio per il cittadino e le imprese

Una Tavola Rotonda con i rappresentanti, ai massimi livelli, di: istituzioni, industria, associazionismo, mondo accademico e della ricerca.

La protezione dei dati e dei sistemi è oggi un compito che dovrebbe coinvolgere tutti gli attori della nostra società. Purtroppo, il problema è ancora sottovalutato a tutti i livelli, e valori importanti quali la privacy dei cittadini e la competitività delle imprese sono continuamente messi a repentaglio. Come uscire da questa situazione? Su questo tema si confronteranno gli invitati alla tavola rotonda.

5 giugno pomeriggio (14.00/17.30) - Convegno Infostorage - La protezione dei contenuti digitali

La libera circolazione delle informazioni è il concetto su cui è stata originariamente fondata Internet, per contro il perfetto controllo sulla circolazione delle informazioni è un principio basilare per la realizzazione di profitti nella società dell'informazione. Far convivere i due principi non è cosa facile, nell'ambito di questo convegno si discuteranno strumenti

legali e tecnologici per il controllo della circolazione dell'informazione in azienda ed il loro impatto sulla rete.

6 giugno mattino (10.30/13.00) - Convegno Infostorage -

La Computer forensic in azienda

Nato come settore per fornire i necessari supporti alle forze dell'ordine coinvolte nell'investigazione di computer crime la computer forensic sta ora trovando applicazioni particolarmente accattivanti in ambito aziendale, con particolare riferimento all'individuazione di attività di spionaggio industriale o abuso delle risorse aziendali. Per svolgere questa attività però è necessario avere un importante bagaglio di competenze in campo tecnologico ma anche legale al fine di non svolgere attività che finiscano con il ledere i diritti degli interessati. Di questi temi si tratterà nel corso di questo evento a cui parteciperanno sia produttori di tecnologie che rappresentanti del mondo legale.

6 giugno pomeriggio (14.00/17.00) - Convegno Infostorage -

La sicurezza nella PA: le ultime iniziative

Sicuramente tra i settori con un maggiore tasso d'innovazione, la PA è anche un settore che ha prestato molta attenzione al settore della sicurezza informatica.

Nell'ambito di questo convegno saranno presentate le ultime iniziative intraprese in questo importante settore in ambito di sicurezza privilegiando le iniziative di portata nazionale.

6 giugno, giornata intera (10.30/17.30) - Seminario Clusit Education -

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

Questo seminario, della durata di una intera giornata, analizzerà nel dettaglio la tecnica del Social Engineering e la sua applicazione nell'esecuzione professionale di verifiche di sicurezza, azioni di penetration testing ed ethical hacking. I due docenti, forti di dieci anni di esperienza in questo delicato settore, illustreranno alla platea le basi fondamentali dell'ingegneria sociale, per passare poi all'analisi approfondita di alcuni attacchi specifici, fornendo e dettagliando casi di studio realmente avvenuti. La seconda parte della giornata verterà sulle corrette strategie da adottare in azienda per difendersi da questa tipologia di attacchi, generalmente di difficile rilevazione, e si concluderà con delle esercitazioni teoriche e pratiche, selezionando alcuni volontari tra il pubblico.

6 giugno, giornata intera (10.30/17.30) - PRISE 2007 -

Secondo workshop italiano su PRIVACY e SECURITY.

Il workshop è aperto a ricercatori universitari ed esperti dal mondo della pubblica amministrazione e dell'industria.

<http://icsecurity.di.uniroma1.it/prise2007>

6. DOCUMENTI ENISA

Segnaliamo due documenti scaricabili dal sito dell'ENISA:

* "A Users' Guide: How to Raise Information Security Awareness"

www.enisa.europa.eu/doc/pdf/deliverables/download.htm

* "Information Security Awareness Programmes in the EU"

www.enisa.europa.eu/doc/pdf/deliverables/enisa_is_aw_programmes_eu.pdf

7. PRESENTATO IL RAPPORTO E-FAMILY 2007

Roma, 13 marzo 2007 – Vi è un'Italia che ha grande fame d'innovazione, dimostra di saper accompagnare l'evoluzione del mercato delle nuove tecnologie e di essere disposta a impegnare importanti risorse familiari per dotarsi di nuovi prodotti tecnologici o di usufruire di servizi avanzati. Sono le famiglie digitali italiane, arrivate ormai a quota 60% della popolazione, spinte ad appropriarsi dei vantaggi dell'innovazione tecnologica dai figli in età scolastica e dal livello di istruzione e attività lavorativa dei componenti. Ma vi è anche quel 40% di popolazione italiana che continua a rimanere indietro. Sono le persone anziane, le casalinghe e coloro che non conoscono la lingua inglese, che hanno grandi difficoltà ad avvicinarsi al mondo delle nuove tecnologie. E' questa, in sintesi, la fotografia della popolazione italiana che offre il Rapporto e-Family 2007, presentato oggi a Roma da Confindustria Servizi Innovativi e Tecnologici e da ANIE, Federazione Nazionale Imprese Elettrotecniche ed Elettroniche.

Secondo l'indagine, giunta alla sua settima edizione, nel 2006 nelle case degli italiani è avvenuto il boom dei collegamenti a banda larga a tariffa fissa, passati da 1,5 a 3,7 milioni, sono entrati oltre 2,5 milioni di nuovi Pc, per la maggior parte portatili, 1,3 milioni di nuove fotocamere digitali, 800.000 nuove stampanti multi-funzione, senza contare i 5 milioni di nuovi utenti di cellulari di terza generazione Umts. E' la dimostrazione che esiste una dimensione familiare italiana molto vivace, fortemente orientata verso l'innovazione e allineata agli standard internazionali nell'utilizzo delle nuove tecnologie. Anzi, addirittura prima nel mondo nel caso dell'utilizzo di cellulari e degli Umts.

Il Summary del rapporto è disponibile all'indirizzo:

www.confindustriasi.it/files/File/Documenti/Comunicati/SUMMARY%20efamily%202007.pdf

Fonte: Confindustria Servizi Innovativi e Tecnologici

www.confindustriasi.it

8. NOTIZIE DAI SOCI

Segnaliamo **Azienda aperta, mobile e collaborativa: come garantire la sicurezza?**, un evento patrocinato dal Clusit che avrà luogo a Milano il prossimo 17 aprile.

L'incontro, destinato agli utenti e la cui partecipazione è gratuita, fa parte del ciclo di riunioni "Incontri a cena con gli utenti" che ZeroUno periodicamente organizza per analizzare, insieme a imprese, fornitori e

osservatori di mercato, le tendenze evolutive dell'Information Technology applicate al business di impresa.

Per maggiori informazioni:

www.zerounoweb.it/index.php?option=com_tipologia&id=1673&id_tipologia=20&task=visualizza

9 . EVENTI SICUREZZA

14 aprile 2007, Monza - Esame CISSP

www.clusit.it/isc2/calendario_isc2.htm

16-17 aprile 2007, Amsterdam - Forrester's Security Forum EMEA 2007

www.forrester.com/events/eventdetail?eventID=1590

(Sconto 30% per i soci Clusit)

17 aprile 2007, Milano - Azienda aperta, mobile e collaborativa: come garantire la sicurezza?

www.zerounoweb.it/index.php?option=com_tipologia&id=1673&id_tipologia=20&task=visualizza

18 aprile 2007, Roma - Seminario CLUSIT

"L'utilizzo delle strumentazioni informatiche e telematiche aziendali. Poteri di controllo e repressione degli abusi da parte del datore di lavoro"

https://edu.clusit.it/scheda_seminario.php?id=6

La partecipazione e' gratuita per il soci Clusit, che possono registrarsi online su <https://edu.clusit.it>

Istruzioni per la registrazione su www.clusit.it/registrazioni2007.htm

18 aprile 2007, Roma - ITIL@GOV - Il governo delle tecnologie dell'informazione

www.clusit.it/eventi/070418_itsmf.pdf

18 aprile 2007, Milano - La gestione dell'emergenza: mix fra rischi e compliance

www.anssaif.it/allegati/ANSSAIFConvegno18aprile.pdf

19 aprile 2007, Milano - Wlan Business Forum 2007 - VIII Edizione

www.wirelessforum.it/spring2007/it/

Sconto 30% per i soci Clusit su corsi di formazione e conferenze a pagamento

9 maggio 2007, Firenze - Seminario CLUSIT

"L'utilizzo delle strumentazioni informatiche e telematiche aziendali. Poteri di controllo e repressione degli abusi da parte del datore di lavoro"

https://edu.clusit.it/scheda_seminario.php?id=7

La partecipazione e' gratuita per il soci Clusit, che possono registrarsi online su <https://edu.clusit.it>

Istruzioni per la registrazione su www.clusit.it/registrazioni2007.htm

15-17 maggio 2007, Milano - 6th OWASP AppSec Conference

www.owasp.org/index.php/6th_OWASP_AppSec_Conference_-_Italy_2007

21-23 maggio 2007, Roma - Corso OCSI sulla "Certificazione della sicurezza informatica: guida per l'applicazione dei Common Criteria"

www.ocsi.gov.it/LinkClick.aspx?link=195&mid=195

23-25 maggio 2007, Parigi - EUROSEC 2007 - 18ème Forum européen sur la sécurité des systèmes d'information

www.devoteam.fr/eurosec/2007/home.php?lang=fr

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

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

© 2007 Clusit - Vietata la riproduzione

Clausola di esclusione della responsabilità e informazioni relative al Copyright: www.clusit.it/disclaimer.htm