Cesare Gallotti

From: it_service_management-news-bounces@mailman.cesaregallotti.it on behalf of IT Service Management NewsLetter [it_service_management-news@mailman.cesaregallotti.it]

Sent: Wednesday, 15 July, 2009 15:16

To: Mailing list

Subject: [IT Service Management] Newsletter del 15 luglio 2009

Attachments: ATT00012.txt

****
IT SERVICE MANAGEMENT NEWS
****

Newsletter mensile con novità in materia di sicurezza delle informazioni, IT Service Management, Qualità. E' possibile dare il proprio contributo e diffonderla a chiunque; è possibile iscriversi, disiscriversi e modificare le proprie opzioni, oltre a vedere l'informativa sul trattamento dei dati personali, all'indirizzo http://mailman.ipnext.it/mailman/listinfo/it_service_management-news

****
Indice

****
00- Chiusura estiva

Ad agosto la newsletter dovrebbe andare in ferie.

Come vedete, però, il materiale da segnalare in questo mese è insolitamente numeroso ed è quindi molto probabile che ci sarà un numero "speciale" nei primi giorni di agosto; l'uscita successiva è prevista per il 15 settembre, mantenendo poi la solita scadenza di metà mese.

****
01- Novità legali

Al Security Summit di Roma si è tenuta una serie di interventi su "Tutte le novità sulla sicurezza digitale nella Pubblica Amministrazione", in particolare su interoperabilità, fascicolo sanitario elettronico, regole tecniche sulla firma digitale e passaporti elettronici. Trovate le presentazioni al link: https://www.securitysummit.it/upload/file/Convegni%20e%20Tavole%20Rotonde/Convegno_Sicurezza_Digitale_PA.zip

---- Privacy ----

Il 25 giugno, il Garante per la Protezione dei Dati Personali ha parzialmente modificato il provvedimento relativo agli "amministratori di sistema" e ne ha postposto il termine per l'adozione al 15 dicembre.

Le nuove disposizioni del Garante: http://www.garanteprivacy.it/garante/doc.jsp?ID=1626595

Il mio testo consolidato:
http://www.cesaregallotti.it/normativa/privacy/2008_11_27_Garante_Amministratori%20di%20Sistema.htm

A parte la proroga, l'unica novità di rilievo riguarda l'elenco degli Amministratori di Sistema, ora non più da allegare al DPS.

Altre perplessità non hanno trovato risposta, se non sulle FAQ, peraltro ambigue in alcuni passaggi (guardate, per esempio, la FAQ 14, che non dice nulla su un tema importante come quello delle verifiche).

La newsletter del Garante del 25 giugno non ha riportato questa notizia, come non riportò la notizia sulla pubblicazione delle FAQ. Mi piacerebbe lamentarmi con chi la cura, ma non sarei efficace. Se conoscete qualcuno...

---- Firma digitale ----

Il 6 giugno è stato pubblicato il Decreto del Presidente del consiglio dei ministri 30 marzo 2009 con le nuove regole tecniche sulla firma digitale e la validazione temporale, che abroga quello del 13 gennaio 2004.

Le potete trovare sul sito del Comune di Jesi: http://gazzette.comune.jesi.an.it/2009/129/1.htm.

Manlio Cammarata fornisce qualche spunto di riflessione su Interlex: http://www.interlex.it/docdigit/regtecn09.htm.

Altre riflessioni le trovate nell'intervento di Stefano Arbia del CNIPA, tenuto al Security Summit di Roma (nello zip https://www.securitysummit.it/upload/file/Convegni%20e%20Tavole%20Rotonde/Convegno_Sicurezza_Digitale_PA.zip)

Sul sito del CNIPA, nulla! Meno male che dovrebbero essere loro a dare il buon esempio alla Pubblica Amministrazione.

---- Posta elettronica certificata ----

Sempre da Interlex, segnalo il DPCM del 6 maggio 2009 con le "Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini": http://www.interlex.it/testi/dpc090506.htm

Sul sito del CNIPA, opportunamente NON in home page, trovate la versione scansionata della Gazzetta Ufficiale (http://www.cnipa.gov.it/html/docs/21-gu%20n.119-dpcm-rilascio%20casella%20pec%20ai%20cittadini.pdf).

---- 231 e responsabilità amministrativa delle imprese ----

Maria Galletti di Cartasi mi segnala un articolo sul 24 Ore dal titolo "Sono più di 100 i reati che fanno scattare le sanzioni alle imprese". Con la nuova legge sulla sicurezza saranno inclusi nel Dlgs 231/2001, tra gli altri, i reati su diritto d'autore, frodi in commercio e contraffazioni di marchi.

Si prospetta sempre più complessa la preparazione di un modello organizzativo "a prova di reato". Intanto, le Linee Guida settoriale (in primis quelle di Confindustria) non mi risultano ancora aggiornate con i reati introdotti dalla Legge 48/2008.

--- Codice dell'Amministrazione Digitale ---

A Omat 2009 si è molto discusso sulle modificazioni poste dal Decreto Anti-crisi (Legge 2/2009, già DL 185/2008) alla normativa sulla documentazione elettronica.

Uno degli interventi più interessanti è stato quello dell'Avv. Allegra Stracuzzi. Vi segnalo un articolo su iged.it 02.2009.

In particolare, nell'articolo si fa notare come il meccanismo della copia informatica (articolo 23 del Dlgs 82/2005 modificato) si ponga in contrapposizione con altri punti del Codice Penale e del Codice Civile e riduca i livelli di garanzia del processo di dematerializzazione. Infine, ci ricorda che le regole tecniche attualmente in vigore sono quelle previste dalla Delibera CNIPA 11 del 2004, oggi un po' antiquata rispetto alle evoluzioni normative degli ultimi 4 anni.

Il mio testo consolidato del Dlgs 82/2005:
http://www.cesaregallotti.it/normativa/Gestione_documentale/2005_Dlgs_82_Codice_amministrazione_digitale.htm

****

02- Standard - Novità

--- ISO/IEC 27000 ---

Fabio Guasconi di Mediaservice.net mi segnala che la ISO/IEC 27000 è stata pubblicata ed è liberamente disponibile tramite ITTF:
http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

Aggiungo che la ISO è al Final Draft della ISO 31000 sui "principi e linee guida per il risk management" e sta revisionando la ISO Guide 73 "Risk Management - Vocabolary".

Tra gli atti del Security Summit 2009 di Roma, vi segnalo quelli relativi a "Le novità nel campo degli standard per la sicurezza It":
https://www.securitysummit.it/upload/file/Seminari/Seminario-Clusit-10-giugno.zip

--- PCI DSS ---

Dalla newsletter del SANS vedo che il PCI SSC sta mettendo in moto un processo di revisione degli standard PCI DSS basato, tra le altre cose, sui commenti degli utilizzatori.

Il processo è simile a quello di tutte le altre norme. Quello che mi sorprende sono i tempi brevi: ogni 2 anni è prevista una revisione.

PCI DSS versine 1.2 dell'ottobre 2008
https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html

Il ciclo di vita delle revisioni del PCI DSS
https://www.pcisecuritystandards.org/pdfs/OS_PCI_Lifecycle.pdf

****

03- Minacce

Sul sito del Concilio d'Europa ho trovato un interessante report del marzo 2008 sulle minacce informatiche. Il report è limitato all'analisi delle minacce condotte a scopo di reato (diffusione di virus, frodi, pornografia, eccetera).
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study1-d-provisional%20_13%20Mar%2008.pdf
Per approfondire l'argomento o per tenere sotto controllo futuri aggiornamenti, la pagina del Consiglio d'Europa dedicata al Cybercrime è http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Default_en.asp

Giovanni Francescutti del DNV Italia mi segnala una particolare minaccia. Fisica, logica o organizzativa? ;-)
http://www.corriere.it/cronache/09_giugno_29/pordenone_computer_tilt_pensionato_spara_4590a7f8-64b3-11de-91da-00144f02aabc.shtml

Franco Ferrari, sempre del DNV Italia, mi ha segnalato questa ben più grave notizia:
http://archiviostorico.corriere.it/2009/giugno/27/Milano_visibili_tutti_segreti_dei_co_9_090627038.shtml
Avrei voluto scrivere un commento su ciò che si sarebbe dovuto fare, ma sarebbe troppo lungo: mettere in opera un sistema di sicurezza non è banale né breve.

Dalla Forensic Focus newsletter di Giugno 2009 c'è un link sui virus degli ATM (i nostri Bancomat). Anche loro...
http://www.newscientist.com/article/mg20227135.700-cash-machines-hacked-to-spew-out-card-details.html

****

04- Mercato della sicurezza ICT

Dalla newsletter del Clusit, vi segnalo lo studio sul mercato della sicurezza informatica in Europa. Ci sono diverse cose interessanti, a livello di standard disponibili e normative applicabili.
http://ec.europa.eu/information_society/policy/nis/strategy/activities/data_ict_market/index_en.htm

****

05- Editoria web

Sul numero 64 di ICT Professional ho trovato l'interessante articolo "Stampa cartacea e Web agli occhi della legge" di Gabriele Faggioli e Andra Reghelin.

L'articolo si chiede cosa si intende per prodotto editoriale, soprattutto in considerazione del web e delle sue caratteristiche.

Mi limito a riportare che l'articolo segnala alcuni buchi normativi, visto che le definizioni applicabili sono quelle della Legge 47/1948 (di 60 anni fa).

Altri riferimenti più recenti, ma con ambito di applicazione più ridotto, sono la Legge 62/2001 (articoli 2, 3 e 5 ma "ai fini della presente legge") e il Dlgs 70/2003 (articolo 7 limitatamente alla registrazione delle testate editoriali telematiche).

Ulteriori riferimenti degni di nota sono:
- una sentenza del tribunale di Modica del 8 maggio 2008 (http://www.mcreporter.info/giurisprudenza/modica080508.htm) con i commenti di Manlio Cammarata http://www.mcreporter.info/stampa/c_ruta2.htm
- la sentenza dell'11 dicembre 2008 Cass. Sez. III penale Sent. 10535 che fa notare come i blog non siano da sottoporre a sequestro in base alla normativa sulla stampa.

****
06- Dizionario delle best practices e degli standard

L'AIEA comunica che il CNIPA ha pubblicato il “Manuale di riferimento n. 9 - Dizionario delle best practices e degli standard” nell’ambito delle “Linee guida sulla qualità dei beni e dei servizi ICT per la definizione ed il governo dei contratti della Pubblica Amministrazione”.

Suggerisco a tutti di dare un'occhiata ai manuali del CNIPA, sempre utili.
http://www.cnipa.gov.it/site/it-IT/Attivit%C3%A0/Qualit%C3%A0_delle_forniture_ICT/Manuali/

In merito a queste specifiche linee guida, trattano delle best practices CMMI-DEV, COBIT, ITIL, PMBOK, PRINCE2 e degli standard ISO 9001, ISO 10006, ISO/IEC 20000-1 e ISO/IEC 27001.

Una mia personale riflessione: diffido molto di questi lavori. Sono troppo orientati ai "confronti", quando invece la cosa fondamentale è capire l'ambito di ciascuna linea guida (best practice, standard) per capire se approfondire la materia e dove applicarlo (sviluppo, governance, gestione dei servizi IT, project management) a seconda delle necessità.

Le linee guida
http://www.cnipa.gov.it/site/it-IT/Attivit%c3%a0/Qualit%c3%a0_delle_forniture_ICT/Manuali/Ricognizione_di_alcune_Best_Practice_applicabili_ai_contratti_ICT/

****
07- ECL 2009

Il mese scorso avevo pubblicizzato il convegno ECL 2009 (Exploring Cyberspace Law, http://donaunnetbook.org), tenuto a Pescara in favore della popolazione aquilana a seguito del terremoto di aprile.

Molte cose interessanti sono state dette. In particolare la tavola rotonda sulla privacy e quella sul settore pubblico sono state veramente partecipate: interventi da parte del pubblico, dibattiti, domande, tentativi di risposte e manifestazione di dubbi ancora aperti. Insomma: una vera tavola rotonda.

Per ora, vi potete accontentare delle poche slides del mio intervento, in cui ho presentato alcuni spunti di dibattito su compliance e organizzazione aziendale (pdf, in italiano, 749 KB).
http://www.cesaregallotti.it/art_pres/20090619-Presentazione-Abruzzo.pdf

Se riceverò notizia di altri documenti pubblici, lo renderò noto.

Tra i vari spunti di dibattito si è discusso di contratti con i fornitori di informatica. Materia complessa, come è noto, in cui non è mai sufficiente fermarsi ai requisiti di prodotto, ma anche a quelli relativi al servizio di assistenza e

manutenzione. Infatti, è noto quanto spesso la normativa cambi, costringendo a continue modifiche dei sistemi informatici. Troppo spesso, i contratti non considerano i costi di manutenzione, che poi diventano insopportabili.

Nel mio intervento c'è una proposta di standard e best practices (meno male che poco sopra avevo detto che diffido di queste cose...) a cui fare riferimento.

****

08- Diritto d'autore

Un mio amico mi segnala il caso di un'Università che ha condotto una ricerca con la partnership di un'azienda privata.

Risultato: un ricercatore in stage ha iniziato le pratiche di brevettazione del software frutto della ricerca. Ovviamente, l'Università e l'azienda privata si trovano ora in difficoltà.

Parrebbe applicarsi l'articolo 65 del Dlgs 30/2005, Codice di proprietà industriale, ma il comma 5 dice che non è applicabile "nell'ambito di specifici progetti di ricerca finanziati da soggetti pubblici diversi dall'università".
http://www.cesaregallotti.it/normativa/diritto_autore_ed_editoria/2005_DLgs_30_Codice_proprieta_industriale.htm

Alla questione ci penseranno persone con maggiore competenza legale. Da parte mia, colgo l'occasione per ribadire l'importanza di prevedere buoni contratti tra aziende e Università, nonché tra Università e ricercatori. Ma come detto nel punto precedente, la "contrattualistica" è materia troppo spesso trascurata, in favore della sola "prezzistica".

Forse questo esempio sarà utile ad accrescere la sensibilità in merito.

****

09- Computer Forensics

Cyber forensic kit: Dalla Forensic Focus newsletter di giugno 2009 segnalo un articolo sul "kit da cyber forenser". Niente affatto economico!
http://www.forensicfocus.com/build-your-own-digital-evidence-collection-kit

TomTom: Clara Colombini ha scritto un ottimo e interessante articolo sull'analisi del TomTom http://www.marcomattiucci.it/CMColombini.art.01.v1.0.pdf, presentato anche a ECL 2009 a Pescara. Se volete fare qualche esperimento di Computer Forensics a casa, questo può essere interessante ;-)
A parte gli scherzi, l'articolo è notevole perché va oltre la semplice descrizione su come acquisire di un dispositivo, ponendosi diverse domande sul procedimento seguito e sulla sua "ripetibilità".

Virtual machines: Dalla newsletter di Marco Mattiucci (www.marcomattiucci.it) vi segnalo una bella tesi sulla virtual computer forensics (con qualche piccola ingenuità), utile anche per approfondire le tecnologie di virtualizzazione.
http://www.marcomattiucci.it/EAvagnano.art.01.v1.0.pdf

****

10- Altri documenti

Dalla newsletter di Marco Mattiucci (www.marcomattiucci.it) vi segnalo il link al sito di Guy Thomas, con molti articoli sui sistemi Windows: dai consigli per i principianti alle configurazioni di sicurezza.
http://www.computerperformance.co.uk/index.htm <http://www.computerperformance.co.uk/index.htm>

Gli atti Security Summit sono disponibili su https://www.securitysummit.it/page/atti_roma_2009
<https://www.securitysummit.it/page/atti_roma_2009>

Il NIST ha pubblicato la revisione 1 della SP 800-46 "Guide to Enterprise Telework and Remote Access Security". Altra materia poco considerata fino a quando non si subiscono incidenti (gravi, ovviamente)
http://csrc.nist.gov/publications/PubsSPs.html#800-46-rev1 <http://csrc.nist.gov/publications/PubsSPs.html#800-46-rev1>

_____
Cesare Gallotti
Ripa Ticinese 75

20143 Milano (Italy)
+39.02.58.10.04.21 (Office)
+39.349.669.77.23 (Mobile)
www.cesaregallotti.it
cesaregallotti@cesaregallotti.it