Cesare Gallotti

From: Cesare Gallotti [cesaregallotti@cesaregallotti.it]
Sent: Monday, 15 February, 2010 19:46
To: cesaregallotti@cesaregallotti.it
Subject: [IT Service Management] Newsletter del 15 febbraio 2010

****
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 secondo la licenza http://creativecommons.org/licenses/by-nc/2.5/it/ .
E' possibile iscriversi o disiscriversi o scrivendo a cesaregallotti@cesaregallotti.it o seguendo le istruzioni riportate nella pagina http://www.cesaregallotti.it/newsletter.htm. L'informativa sul trattamento dei dati personali è alla pagina http://www.cesaregallotti.it/newsletter.htm.

****
Indice

****
00- Mie presentazioni

Mi faccio pubblicità e vi ricordo che terrò delle presentazioni:
- a Milano il 17 febbraio: http://www.aiea.it/pdf/sessioni%20di%20studio%20e%20di%20formazione/2010/Milano%2017%20Febbraio%202010.pdf
- a Roma il 3 marzo: http://www.aiea.it/pdf/sessioni%20di%20studio%20e%20di%20formazione/2010/Roma%203%20marzo%202010.pdf

****
01- Novità legali

** DigitPa **

Da Iged.it online, trovo la notizia che il 1 dicembre è stato deciso il cambio di denominazione del CNIPA. Ora si chiamerà DigitPA.
Non capisco la ragione del cambio di denominazione. In alcune associazioni, si cambia periodicamente denominazione per fare in modo che il Presidente possa continuare a rimanere in carica anche dopo essere stato eletto il numero massimo accettabile di volte. Chissà perché anche l'AIPA e il CNIPA seguono questa prassi?

Ad ogni modo, potete trovare maggiori dettagli:
- su iged.it http://www.iter.it/iged_online.htm
- dal Dlgs 177/2009: http://www.camera.it/parlam/leggi/deleghe/09177dl.htm

** Codice dell'Amministrazione Digitale **

Anche le continue modifiche al CAD potrebbero fornire materia per la "psicologia del Diritto", sempre che tale materia possa esistere.

Ad ogni modo, dalla Newsletter Filodiritto ho trovato la notizia di un nuovo schema di Decreto Legislativo per il CAD. Ma sembra che l'operazione abbia avuto un rallentamento, come si legge da un articolo del Sole 24 Ore pubblicato su Anorc.it
http://www.anorc.it/notizia/154_Rinviato_il_Decreto_sulla_PA_Digitale_.html

Per saperne di più, il Presidente dell'Anorc ha pubblicato le sue riflessioni (poco elegantemente, le ha pubblicate sul suo sito e non su quello dell'Anorc, ma vabbè)
http://www.studiolegalelisi.it/news.php?id=241

Segnalo anche un altro articolo ad esso collegato
http://www.filodiritto.com/index.php?azione=visualizza&iddoc=1687

** Privacy e linee guida **

Franco Ferrari (DNV) mi segnala un articolo su PuntoSicuro sulle recenti sentenze di cause civili:
- Bassano del Grappa del 12 maggio 2009
- Roma del 30 settembre 2009

Le due sentenze, in poche parole, dicono che le "Linee Guida" del Garante della Privacy non hanno valore precettivo. In altre parole, non è perseguibile chi non le segue.

Aggiungo io: è però chiaro, per il Codice Privacy, che bisogna sempre dimostrare di aver implementato le "misure idonee" atte alla salvaguardia dei dati personali. Quindi, ignorare completamente le linee guida del Garante è comunque un errore.

Si ricordano le "linee guida" del Garante:
- "Linee-guida per il trattamento di dati dei dipendenti privati" (http://www.garanteprivacy.it/garante/doc.jsp?ID=1364099); dove però il capitolo 4 sui dati biometrici ha valore prescrittivo;
- "Lavoro: le linee guida del Garante per posta elettronica e internet" (http://www.garanteprivacy.it/garante/doc.jsp?ID=1387522)
- "Linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali" (http://www.garanteprivacy.it/garante/doc.jsp?ID=1407101);
- "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" (http://www.garanteprivacy.it/garante/doc.jsp?ID=1417809);
- "Linee guida in materia di trattamento di dati personali da parte dei consulenti tecnici e dei periti ausiliari del giudice e del pubblico ministero" (http://www.garanteprivacy.it/garante/doc.jsp?ID=1534086);
"Linee guida per trattamenti dati relativi al rapporto banca-clientela" http://www.garanteprivacy.it/garante/doc.jsp?ID=1457247
- "Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali" (http://www.garanteprivacy.it/garante/doc.jsp?ID=1533155);
- "Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario" (http://www.garanteprivacy.it/garante/doc.jsp?ID=1634116);
- "Linee guida in tema di referti on-line" (http://www.garanteprivacy.it/garante/doc.jsp?ID=1679033).

** Decreto Pisanu **

Con il DL 194 del 2009, il Decreto Pisanu (Legge 155 del 2005) ha avuto un'estensione di validità fino al 31 dicembre 2010.

Sono piuttosto deluso dall'informazione che ho ricevuto in merito: a dicembre si è fatto un gran parlare della possibile estensione del Decreto (doveva scadere il 31 dicembre 2009), ho letto alcuni articoli, molto filosofeggianti, in materia. Poi... quando il Decreto è stato prorogato... nessuna notiza.

Non lo trovo molto serio. E meno male che si diceva che grazie a Internet sarebbe stato possibile ricevere notizie accurate. Invece si è avuto un ulteriore esempio di come funziona l'informazione: le informazioni sono date solo finché qualcuno ci guadagna (in termini di visibilità, in questo caso).

** Altra normativa in materia di criminalità informatica **

Dalla newsletter del SANS trovo segnalato un articolo di MSNBC su uno schema di Legge per controllare il

contenuto dei video di Google e YouTube.
http://www.msnbc.msn.com/id/35017877/ns/technology_and_science-security/

L'articolo è accompagnato da qualche commento sull'utile che ne ricaverebbe il nostro Premier.

Non ho trovato alcuna notizia in merito nelle newsletter italiane che seguo. Notizia vera o falsa? Chi ci sta guadagnando a darla o a non darla? Non ho risposta.

** Responsabilità Amministrativa (Dlgs 231/2001) **

Una recente sentenza, finalmente, accetta come "valido" un modello organizzativo secondo il Dlgs 231/2001 e non condanna l'ente:
http://www.filodiritto.com/index.php?azione=visualizza&iddoc=1698

** Diritto d'autore **

Interlex segnala l'iniquità del "equo compenso per la copia privata".
http://www.interlex.it/copyright/iniquo.htm

** Commenti su Amministratori di Sistema, Decreto Ronchi e sequestro Pirate Bay **

Finalmente su Interlex i primi commenti sui recenti dispositivi di Legge con commenti più esaustivi delle mie brevi enunciazioni dei mesi precedenti.

Su http://www.interlex.it/675/ricchiu36.htm il commento su
- Decreto Ronchi
- Amministratori di Sistema

Su http://www.interlex.it/regole/ricchiu37.htm il commento su
- sequestro Pirate Bay

Tra l'altro, nello scorso numero avevo scritto "Privatebay" al posto di "thePirateBay". Grazie ad Andrea Rui per la segnalazione.

****
02- Certificazioni professionali - CRISK dell'ISACA

ISACA ha rilasciato e sta pubblicizzando una nuova certificazione professionale denominata CRisk.
http://www.isaca.org/Template.cfm?Section=CRISC1&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=16&ContentID=54691

Forse si sta un poco esagerando con il valore attribuito alle certificazioni professionali. Ho sentito certi interventi di persone ultra-certificate da fare accapponare la pelle, ma è comprensibile: passano il tempo a studiare sui libri e non a farsi un'esperienza sul campo.

Trovo corretto dover dimostrare le proprie competenze e trovo corretto che i bandi di gara richiedano una qualche certificazione. Non trovo invece corretto dover dimostrare le mie competenze di sicurezza con la certificazione CISM per alcuni bandi, LA 27001 per altri, CISSP per altri ancora. Non sarebbe ora di parlare di "equivalenze" e di "esperienze" in un certo campo? Non voglio dover spendere dei soldi per affrontare degli esami sempre sulle stesse cose ma con dei nomi diversi!

(Giusto... i soldi. Ma questo è un tema troppo scottante per affrontarlo in poche righe)

****
03- Cloud Computing

Da una discussione su "Lead Auditor ISO 27001 Community" di LinkedIn, trovo il link ad un corposo documento dell'Enisa sulla materia.
http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

****

04- Computer forensics

** Legge 48/2008 **

Segnalo la nuova pagina del sito di Marco Mattiucci, con numerosi spunti di riflessione sulla Legge 48/2008 e sulla raccolta di fonti di prova da sistemi digitali. Le risposte di Cajani mi sembrano le più complete.
http://www.marcomattiucci.it/l482008.php

** Into the boxes **

Dall'Associazione Digital Forensics Alumni, ricevo notizia della nuova rivista digitale Into the Boxes dedicata alla digital forensics. Gli articoli sono molto tecnici.
http://intotheboxes.wordpress.com/

****

05- Attacchi

Dalla Newsletter del Sans, trovo la notizia che 3 delle maggiori compagnie petrolifere USA sono state oggetto di spionaggio grazie a delle vulnerabilità delle reti interne. Molto difficile trovare notizie di questo genere, visto che nessuno (anche se oggetto di attacchi) vuole che siano pubblicate.
La scoperta è stata fatta dall'FBI, non dai sistemisti delle compagnie. Dimostrando così quanto sia difficile rilevare gli attacchi riusciti, quando il termine "riusciti" può comprendere anche la capacità di non essere notati.
http://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved

Dalla Newsletter Crypto-Gram si ha un'altra notizia di un altro attacco riuscito, con impatti per tutti.
http://precision-blogging.blogspot.com/2009/12/another-leak-worst-so-far.html

****

06- Standardizzazione - ISO/IEC 27004:2009

Dopo 4 anni dall'uscita della ISO/IEC 27001 che richiede di misurare l'efficacia dei controlli di sicurezza, è stata pubblicata la ISO/IEC 27004 dal titolo "Information technology — Security techniques — Information security management — Measurement".

Francamente, non mi ha convinto.

Una buona parte del documento tratta della gestione delle misurazioni (responsabilità della Direzione, programma di misurazione, ciclo PDCA, eccetera). Nulla di nuovo per chi si occupa di qualità, di misurazione dei processi e di conformità dei prodotti, tecniche SPC, eccetera. Convengo che questo standard può essere utile a chi non ha competenza sulla misurazione dei processi e dei prodotti.

Aggiungo, però, che tutto il costrutto della 27004 mi pare eccessivamente teorico e molto difficile da mettere in pratica con pragmaticità.

La cosa più deludente, però, sono gli esempi. Da una parte perché anche questi troppo "costruiti teoricamente", con 2 pagine di descrizione per ciascuna misura (quale azienda troverebbe efficace ed efficiente questo metodo?). Dall'altra parte perché non mi sembrano misure particolarmente significative.

Un esempio: l'indicatore sulla qualità delle password prevede di calcolare il numero di password non conformi alle policy aziendali (es. lunghezza minima di 8 caratteri) chiedendo agli utenti se la propria password soddisfa le policy aziendali. Mi vien da dire che tutti risponderanno di sì. Meno male che l'esempio successivo prevede di far girare un software di cracking e quindi si dimostra che gli estensori della norma non vivono in un mondo diverso dal nostro, ma il primo esempio l'avrei lasciato perdere.

Altri esempi: il numero di verifiche annue da parte di valutatori indipendenti, il numero totale di incidenti (che si sa, dipende anche dall'efficacia della loro registrazione), il numero di azioni correttive implementate (non il numero di azioni implementate secondo i tempi, i costi e i risultati previsti!), la percentuale tra virus rilevati nella rete aziendale e quelli bloccati (qui il risultato potrà, forse, essere calcolato in Parti Per Milione), il livello di robustezza del controllo accessi fisici (ma se il livello è inadeguato, allora si tratta di una vulnerabilità), numero di requisiti di sicurezza previsti dalle politiche aziendali ma non presenti nei contratti con i fornitori (ma questa dovrebbe essere considerata una non conformità e una vulnerabilità, più che un elemento di misura).

Insomma, come tutti, neanche le persone all'interno del SC27 hanno dimostrato di sapere come misurare l'efficacia dei controlli, anche se il requisito è inserito nella ISO/IEC 27001:2005 e noi auditor e consulenti e manager della sicurezza cerchiamo di gestirlo nel modo più dignitoso possibile.

Curioso, infine, come alcune misurazioni "naturali" non siano state trattate: disponibilità dei sistemi o costi di gestione degli incidenti (misura difficile, molto difficile). Alcuni esempi sono effettivamente realistici e interessanti, (il grado di copertura dei piani di formazione e manutenzione), ma sono troppo pochi rispetto a quelli troppo teorici per essere veri.

Concludo dicendo che, come in tutti i sistemi di gestione, in questo ambito o si fanno costruzioni teoriche utili per i consulenti o si mettono in campo azioni utili al processo decisionale. La ISO/IEC 27004:2009 sembra far parte del primo gruppo.

****

07- Sui tool di project management

Andrea Rui risponde ad un mio precedente articolo, scrivendo:
<<
- per uno strumento di project management libero, puoi dare un'occhiata a OpenProj, compatibile MS Project, ed è FLOSS;
- a parte la testa, che è l'elemento fondamentale, personalmente ritengo che il miglior strumento da utilizzare per il project management sia quello che è meglio conosciuto e più frequentemente utilizzato dal personale, indipendentemente da quale sia; ritengo che i tool 'nucleari' abbiano un senso in quelle realtà che hanno un processo di gestione della sicurezza talmente consolidato che tutto il personale è in grado di percepire ed apprezzare i vantaggi offerti da strumenti più evoluti
>>

Condivido. Solo i consulenti "mordi e fuggi" o senza esperienza o con altri interessi possono proporre tool faraonici ad un'impresa convincendola che in breve tempo tutto il personale lo utilizzerà senza problemi.