****
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.

E' disponibile il blog http://blog.cesaregallotti.it

E' possibile iscriversi o disiscriversi
- scrivendo a cesaregallotti@cesaregallotti.it
- seguendo le istruzioni riportate nella pagina http://www.cesaregallotti.it/Newsletter.html

Sulla stessa pagina è possibile consultare l'informativa sul trattamento dei dati personali.

****
Indice

****
01- Sentenza: il blogger non è "direttore responsabile"

Da Interlex (http://www.mcreporter.info/)

Importante sentenza della Corte d'Appello di Torino: il gestore di un blog non può essere equiparato al direttore responsabile di un giornale e quindi non esiste il reato di "omesso controllo". Resta la responsabilità per diffamazione.

http://www.mcreporter.info/giurisprudenza/to100423.pdf

****
02- Sentenza: rubare files non è reato

Su www.ictlex.net è pubblicata la notizia della sentenza della Corte di Cassazione sui reati configurabili in materia di sottrazione di file sul luogo di lavoro.

Riporto il testo di Andrea Monti, che riassume:
- il reato non sussiste: Sottrazione di soli file contententi informazioni riservate – reato di furto ex art. 624 C.p. – carenza della qualità di cosa mobile dei file informatici
- il reato sussite: Sottrazione di dati commerciali da parte del dipendente e successivo utilizzo in azioni concorrenziali – configurabilità del reato di rivelazione di segreto professionale ex art. 622 C.p.

Non sussiste il reato di furto, per carenza di tipicità, quando la condotta riguarda l'appropriazione di file svincolati dal loro supporto.

La copia di file appartenenti al proprio datore di lavoro e il loro riutilizzo successivo alle dimissioni da parte del dipendente in attività concorrenziale integra il reato di cui all'art. 622 C.p.

Il testo integrale e' disponibile a questo indirizzohttp://www.ictlex.net/?p=1218

Cerco (io, Cesare Gallotti) di tradurre: pare quindi che si possano rubare file, purché successivamente non si utilizzino. Il Diritto è certamente una materia strana...

****

03- Sul Dlgs 198 del 2010 sull'installazione di reti IT

Dopo la segnalazione di settimana scorsa (http://blog.cesaregallotti.it/2010/12/decreto-legislativo-198-del-2010.html) sul Dlgs 198 del 2010, Andrea Rui mi ha riportato un paio di commenti che condivido e riporto (anche un poco filtrate da mie idee):

1- Dopo tanto parlare dell'eliminazione degli albi professionali, ci si inventa il nuovo albo o registro per gli installatori. A cui saranno iscritti i soliti noti alla faccia delle liberalizzazioni.

2- Se l'azienda sarà nell'albo, poi si corre il rischio che gli operatori sul campo non saranno sempre opportunamente preparati, come troppo spesso succede.

3- Perché invece non richiedere certificazioni personali? Anche se il mercato delle certificazioni personali potrebbe deteriorarsi, almeno rimarrebbe valida la responsabilità personale di chi svolge i lavori.

****

04- ISO/IEC 20000-1

La FDIS della ISO/IEC 20000-1 è stata approvata. Tra qualche mese dovrebbe essere pubblicato il nuovo standard che sostituirà la versione del 2005.

****

05- Nuova versione della ISO/IEC 19770-1

Come membro dell'ISACA, ho ricevuto la richiesta di commentare il draft della nuova versione della ISO/IEC 19770-1 dal titolo "Information technology — Software asset management — Part 1: Processes and tiered assessment of conformance".

Questa sarebbe la nuova versione della ISO/IEC 19770:2006 che aveva titolo "Information technology — Software asset management — Part 1: Processes"

Come si vede dal titolo, ora viene proposto un approccio su più livelli, da 1 a 4. In altre parole, sarebbe possibile dichiarare la propria conformità ad uno dei 4 livelli dello standard, da quello più semplice ("Dati affidabili") a quello completo ("Piena conformità"). Ogni livello comprende il precedente.

Questa scelta, stando agli autori, faciliterebbe l'adozione dello standard e permetterebbe di dare massima priorità alla gestione delle licenze.

Mi sono dichiarato contrario a questa scelta per 2 motivi: il primo è che se si presenta uno standard di requisiti questi dovrebbero costituire un insieme coerente di aspetti e farne uno spezzatino introduce invariabilmente incoerenze; il secondo (riprendendo a modo mio il parere di Tony Coletta) è che qui si sta parlando di UN solo processo e "facilitarne la conformità" sembra un poco ridicolo.

****

06- Libro bianco: Le Prove, i Controlli, le Valutazioni e le Certificazioni

Segnalo, da comunicazione ricevuta dal CEPAS, la pubblicazione del Libro bianco: "Le Prove, i Controlli, le Valutazioni e le Certificazioni per i prodotti, i servizi, le aziende ed i professionisti" a cura di Confindustria Servizi Innovativi e Tecnologici.

Il libro è il risultato di un'ampia indagine su diverse tipologie di certificazione, tra cui quella dei dispositivi medici (e del relativo software!), dei Sistemi di Gestione per la Qualità, di Sistemi di Gestione per la Sicurezza delle Informazioni e del personale.

Ho trovato decisamente interessante e brutalmente sincera la parte sulla 9001, mentre ho trovato diverse inesattezze nell'ambito della 27001 (ma ricordo che qualcuno mi aveva coinvolto e avevo riportato delle considerazioni... mi avrà ignorato...) e della certificazione del personale. Ho poi intercettato un riferimento alla vecchia 626 e mi sono accorto che per capire la data di pubblicazione bisogna andare fino all'ultima pagina in cui si legge un generico 2010.

Il lavoro, quindi, presenta disomogeneità tra i vari capitoli e alcune imprecisioni ci impongono di leggerlo con prudenza. Ciò non toglie che può presentare un valido punto di riferimento per capire meglio alcuni ambiti e alcuni campi di applicazione.

Il link: http://www.cepas.it/news.asp

****

07- Realtà e virtualità: qualcuno capisce le differenze

Qualche tempo fa, avevo segnalato dei casi di licenziamento di dipendenti che avevano diffamato, seppur in modi differenziati, la propria azienda sui social network:
http://www.mirror.co.uk/news/top-stories/2009/01/11/exclusive-marks-spencer-staff-ridicule-customers-on-facebook-115875-21033664/

Da Cryptogram del 15 dicembre, un articolo dimostra che alcuni pensano a quello che fanno e adottano alcune strategie per evitare che il virtuale abbia impatti negativi sul reale:
http://www.zephoria.org/thoughts/archives/2010/11/08/risk-reduction-strategies-on-facebook.html

Purtroppo, le protagoniste dell'articolo vivono in ambienti sociali disagiati e probabilmente questo le ha rese più attente. Dovremo aspettare ancora molto tempo prima che la classe media faccia andare i neuroni su questa materia?

****

08- Storia dell'algoritmo A5/2

Da CRYPTO-GRAM del 15 dicembre 2010, ripropongo il link alla "Breve storia della dismissione dell'algoritmo A5/2 dai protocolli GSM" (in inglese), dove viene dimostrata ancora una volta la pochezza di certe istituzioni e il dilettantismo che ci pervade.

http://laforge.gnumonks.org/weblog/2010/11/12/#20101112-history_of_a52_withdrawal

Non voglio dire che tutti debbano essere dei geni, ma pare che qui gli manchino le basi. E scrivono standard...

****

09- Quaderno Clusit su PCI - DSS

La newsletter del Clusit segnala la pubblicazione del Quaderno Clusit dal titolo "PCI-DSS: Payment Card Industry - Data Security Standard". Molto interessante per chiunque voglia conoscere questi standard.

http://clusit.it/download/Q08_bis.pdf

****

10- Sicurezza smartphones

Segnalo (riprendendolo dalla newsletter del Clusit) la bella guida dell'Enisa sulla sicurezza degli smartphones (compufoni? calcofoni?). Sono elencate e descritte molto accuratamente le minacce, le vulnerabilità e le misure di sicurezza suddivise per privati, impiegati e "alte cariche". La guida ha inoltre in appendice un'interessante bibliografia.

Aggiungo che questa guida mi sembra un ottimo esempio su come dovrebbero essere fatti certi lavori. In altre parole: da studiare non solo da chi si occupa di sicurezza di cellulari, ma da chiunque si occupa di sicurezza.

Il report si scarica da http://www.enisa.europa.eu/act/it/oar/smartphones-information-security-risks-opportunities-and-recommendations-for-users/at_download/fullReport.

Suggerisco di leggere anche la pagina di presentazione dell'Enisa perché riporta anche i link ad un video e alle FAQ: http://www.enisa.europa.eu/media/press-releases/security-is-there-an-app-for-that-eu2019s-cyber-security-agency-highlights-risks-opportunities-of-smartphones