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: Friday, 16 January, 2009 17:33

To: Mailing list

Subject: [IT Service Management] Newsletter del 16 gennaio 2009

Attachments: ATT00128.txt

****

IT SERVICE MANGEMENT NEWS

****

Newsletter mensile con novità in materia di sicurezza delle informazioni, IT Service Management, Qualità. E' possibile 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

****

1- Novità normative: Privacy

Smaltimento di apparecchiature elettriche ed elettroniche
(Dal Numero 285 - 15 dicembre 2008 - Newsletter Giuridica di Filodiritto)

Con il Provvedimento del 13 ottobre 2008, il Garante ha dato indicazioni precise sulle modalità di cancellazione dei file in conformità ai punti 21 e 22 dell'Allegato B del Codice sulla Privacy.
http://www.garanteprivacy.it/garante/doc.jsp?ID=1571514

A questo provvedimento ha inoltre fatto seguire delle istruzioni pratiche, con indicazioni tecniche precise, inclusi link a prodotti specifici.
http://www.garanteprivacy.it/garante/doc.jsp?ID=1574080

A mio parere si tratta di una buona iniziativa, che aiuta tutti a rispondere in modo adeguato ai requisiti di sicurezza contemplati dal Codice Privacy

Semplificazione delle misure di sicurezza
(Dal Numero 285 - 15 dicembre 2008 - Newsletter Giuridica di Filodiritto)

Con la Legge 133/2008 viene modificato il Codice Privacy e si riducono alcuni adempimenti per alcuni soggetti, tra cui la sostituzione del DPS con un'autocertificazione in cui si dichiari di rispettare le altre misure di sicurezza prescritte dal Codice.

L'articolo modificato è il 34, a cui è stato aggiunto il comma 1-bis. Potete trovare il Codice Privacy aggiornato su
http://www.cesaregallotti.it/normativa/privacy/2003_Dlgs_196.htm

Inoltre, il Garante ha emanato un provvedimento per indicare cosa si intenda per "altre misure di sicurezza"

http://www.garanteprivacy.it/garante/doc.jsp?ID=1571218

Amministratori di sistema
(da Ivan Antonietti di GetSolution)

Il 27 novembre, il Garante ha emesso le specifiche per gli Amministratori di Sistema.
http://www.garanteprivacy.it/garante/doc.jsp?ID=1577499

Molto interessante il fatto che sono richiesti audit almeno annuali sulle attività di amministrazione di sistema e dei meccanismi di logging dei loro accessi ai sistemi.

Sanzioni
(da Giovanni Francescutti, DNV Italia)

Il Decreto Legge 207/2008, all'articolo 44, modifica alcuni articoli del Codice Privacy in materia di sanzioni.
Trovate il DL sul sito del Parlamento: http://www.parlamento.it/parlam/leggi/decreti/08207d.htm
Prima di aggiornare la mia versione del Codice, aspetto di vedere cosa faranno in fase di conversione in Legge.

****

2- Novità normative: Posta elettronica certificata e archiviazione ottica
(Dal Numero 285 - 15 dicembre 2008 - Newsletter Giuridica di Filodiritto)

Il Decreto Legge "Anti-Crisi" introduce l'obbligatorietà per tutte le aziende di utilizzare un servizio di posta elettronica certificata e semplifica le modalità di archiviazione ottica in modo che si diffonda maggiormente.

Credo che la cosa migliore per capire di cosa si tratta è leggere questo articolo
http://www.filodiritto.com/index.php?azione=visualizza&iddoc=1294

Per il resto, bisognerà vedere cosa succederà al momento della conversione in Legge del DL. Io sono già fiducioso e ho modificato il Codice dell'Amministrazione Digitale (D. Lgs. n. 82/2005) e il Regolamento per l'utilizzo della Posta Elettronica Certificata (D.P.R. n. 68/2005) pubblicati sul mio sito.
http://www.cesaregallotti.it/normativa/Gestione_documentale/2005_Dlgs_82_Codice_amministrazione_digitale.htm
http://www.cesaregallotti.it/normativa/Gestione_documentale/2005_DPR_68_regolamento_posta_certificata.htm

****

3- Perché i progetti falliscono

Dall'Information Systems Control Journal, volume 6 del 2008, leggo l'articolo "Issues With Auditing the Systems Development Process" By Dave Henderson, Ph.D.

In cui si legge che, alla fine del 1995, la FoxMeyer stava introducendo un ERP. La FoxMeyer, all'epoca, fatturava 5 miliardi di dollari all'anno ed era il leader dell'industria farmaceutica. A inizio 1996, il sistema non gestiva correttamente gli ordini con problemi tali che la costrinsero, nel tempo, al fallimento.

Era il 1995... ma se volete esempi più recenti, vi invito a leggere l'articolo (sempre segnalato da Henderson) "Why Software Fails" http://spectrum.ieee.org/print/1685, dove trovate esempi e analisi interessanti.

Io ridurrei il tutto a 3 punti chiave e necessari. In molti casi non saranno sufficienti, ma l'esperienza mi insegna che da qualche parte bisogna partire e che in molte realtà si tratterebbe già di una rivoluzione:
1- il business deve convincersi che i progetti IT sono anche loro responsabilità, che i potenziali impatti negativi riguarderanno soprattutto i costi indiretti (processi di business meno efficienti e quindi più costosi), che è necessario mettere a disposizione del progetto i rappresentanti del business con le migliori competenze (non quelli che sono così incapaci che "almeno lì non fanno danni")
2- I PM dell'IT e del business devono preparare e tenere monitorato un GANTT fatto in modo serio; sono convinto che il 90% dei PM dell'IT non abbia ricevuto alcuna formazione su come gestire progetti e che, in un numero ancora maggiore di casi, il business abbia delegato completamente la gestione dei progetti all'IT
3- i requisiti funzionali devono essere documentati su un documento che ne permetta la gestione coerente e ne riporti i dettagli. Non "una serie di email" di cui poi si perde il filo, né "un ppt" dove i dettagli scompaiono, incluse alcune esigenze importanti.

****

4- Programmazione sicura (i 25 errori più comuni)

Il SANS ha pubblicato i 25 errori di programmazione più pericolosi, con il solo difetto di avere un'introduzione troppo lunga
http://www.sans.org/top25errors/

Questa lista si aggiunge alle 20 vulnerabilità più diffuse
http://www.sans.org/top20/

Da leggere tutte e due.

****
5- Security Metrics

Dall'Information Systems Control Journal, volume 6 del 2008, leggo l'articolo "Accounting for Value and Uncertainty in Security Metrics" di C. Warren Axelrod. Invito coloro che sono iscritti all'ISACA a fare altrettanto.

Il mio modesto parere sulle security metrics è che è molto difficile trovarne di efficienti e significative. In definitiva mi sembrerebbe già un buon inizio vedere statistiche sulla disponibilità dei sistemi e sulle tipologie di incidenti registrati.

Comunque, segnalo altri link pubblici segnalati dallo stesso articolo:
http://www.secureitconf.com/OLD/2005/presentations/Enterprise%20Security.pdf (2005) della Canergy Mellon
www.acsac.org/measurement/proceedings/wisssr1-proceedings.pdf (2001), molto lungo e complesso
www.educause.edu/ir/library/pdf/CSD3661.pdf (2004) con tanti esempi
http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf, del NIST che è sempre il migliore, secondo me, per brevità e per esempi

****
6- Statistiche on-line

Forse vi potrebbe servire questo link con tante statistiche
http://www.swivel.com

****
7- Browser Security Handbook
(da SANS NewsBites Vol. 10 Num. 98)

Google ha pubblicato un "Browser Security Handbook" con molte cose interessanti e dettagli tecnici per la configurazione del proprio browser (IE 6 e 7, Mozilla Firefox 2 e 3, Apple Safari, Opera, Chrome e Android).
http://code.google.com/p/browsersec/wiki/Main

****
8- Novità normative: Direttive Modernizzazione e Transparency
(dalla newsletter di Protiviti)

Le Direttive Modernizzazione (2003/51/CE) e Transparency (2004/109/CE) sono state recepite dal nostro Paese con i Decreti Legislativi 32/2007 e 195/2007 scaricabili da
http://www.parlamento.it/parlam/leggi/home.htm

La prima riguarderebbe principalmente le aziende del mondo finance e la seconda le SpA.

Queste due direttive richiedono che, per il bilancio d'esercizio e per quello consolidato, la relazione sulla gestione comprenda una "descrizione dei principali rischi e incertezze cui sono esposti" (lettera e, comma 9, articolo 1 del Dlgs 195/2007).

A molte imprese italiane è quindi richiesta un'analisi dei rischi di business, di credito e operativi (inclusi quelli informatici, ma non solo). Il tutto ricorda molto quanto già previsto dagli accordi di Basilea II per le banche.

Dalla newsletter di Protiviti sembra che questo disposto sia applicabile a quasi tutte le imprese e non solo alle SpA. A me non sembra, ma chiedo chiarimenti a chi me li possa fornire.

Pare inoltre che non siano ancora stati emanati i decreti attuativi e quindi la letteratura su queste due Direttive è ancora molto incompleta e la loro applicabilità per l'anno in corso sembra incerta.

Ad ogni modo, potete scaricare
http://www.protiviti.it/downloads/PRO/pro-it/Newsletter_n23_Gen_2009.pdf

****

9- Articolo su contrattualistica con outsourcer
(da Filodiritto del 12 gennaio 2009)

In questo articolo sono segnalate alcune clausole contrattuale da considerare quando si acquistano servizi SaaS. Io estenderei le raccomandazioni a tutta la contrattualista con gli outsourcer di servizi IT.
http://www.filodiritto.com/index.php?azione=visualizza&iddoc=1312

_____
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