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: Tuesday, 14 April, 2009 18:44
To: it_service_management-news@mailman.cesaregallotti.it
Subject: [IT Service Management] Newsletter del 14 aprile 2009
Attachments: ATT03826.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
<http://mailman.ipnext.it/mailman/listinfo/it_service_management-news>

****
Indice

****
1- Normativa: Regole tecniche sulla firma digitale

In occasione di Omat 2009, Giovanni Manca del CNIPA ha dichiarato che è stato emesso il DPCM 30 marzo 2009 che sostituirà il DPCM 13 gennaio 2004 su "Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici".

Il nuovo DPCM dovrebbe essere pubblicato in GURI entro metà maggio ed entrare in vigore entro i prossimi 9-12 mesi.

****
2- Normativa: privacy

2.1- Sanità

Il 5 marzo, il Garante ha emesso un Provvedimento dal titolo "Linee guida in tema di fascicolo sanitario elettronico e di dossier sanitario".

http://www.garanteprivacy.it/garante/doc.jsp?ID=1598313

2.2- Milleproroghe
(da Interlex n. 385)

La Legge "mille proroghe" 14/2009 (già DL 207/2008) indica, all'articolo 44: "I dati personali presenti nelle banche dati costituite sulla base di elenchi telefonici pubblici formati prima del 1° agosto 2005 sono lecita mente utilizzabili per fini promozionali sino al 31 dicembre 2009, anche in deroga agli articoli 13 e 23 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, dai soli titolari del trattamento che hanno provveduto a costituire dette banche dati prima del 1° agosto 2005".

Il Garante ha emesso le relative prescrizioni, che limitano di parecchio le possibilità di abusi.
http://www.garanteprivacy.it/garante/doc.jsp?ID=1598808

Potete leggere gli articoli di Interlex:
http://www.interlex.it/675/ricchiu33.htm
http://www.interlex.it/675/ricchiu34.htm

****

3- Normativa: PEC
(da Michele Giambruno di ITNET)

A fronte del mio entusiasmo sulle nuove disposizioni sulla PEC, mi hanno segnalato un articolo più critico:
http://punto-informatico.it/2571537/PI/Commenti/pec-cos-altro.aspx

In questa pagina è riportato anche un link a questo interessante articolo
http://www.diritto.it/art.php?file=/archivio/27228.html

****

4- Password deboli

Su Crypto-gram del 15 marzo, si cita una ricerca effettuata sulle password utilizzate dagli utenti del sito di social network phpbb. Le password erano state pubblicate a seguito di un'azione di hacking.

E' evidente che molti utilizzano password deboli per questo genere di siti, mentre ne utilizzano di più robuste per i sistemi utilizzati a scopo professionale. Questo anche perché in molte aziende ci sono controlli automatici sulla complessità delle password. E' altrettanto evidente che altri non sono stati educati ad utilizzare password più robuste in ambito professionale, ma questa è una storia nota.

Rimane interessante vedere come sono distribuite le tipologie di password.
http://www.darkreading.com/blog/archives/2009/02/phpbb_password.html

Il problema è che il worm Conficker.B si è diffuso grazie alla sua capacità di crackare le password degli amministratori di sistema. Evidentemente, ha ragione il Garante ad avere dei dubbi sulle loro competenze! (Ne ho conosciuti tanti preparati e attenti, ma non tutti lo sono)

Altrettanto interessante è l'articolo (sempre citato da Crypto-gram del 15 marzo) sulla backdoor dei sistemi di allarme della Sentex. Ciò conferma il fatto che la tecnologia è molto bella e molto utile, ma che in troppi (anche chi si occupa di sicurezza!) la utilizzano senza porvi la necessaria attenzione.

http://david.weebly.com/1/post/2009/03/how-to-open-many-keypad-access-doors.html

****

5- Modello di maturità per la sicurezza applicativa
(da SANS NewsBites Vol. 11 Num. 20)

E' disponibile una best practice sui modelli di maturità per lo sviluppo della sicurezza nelle applicazioni.
http://bsi-mm.com/

Ne approfitto per ricordare l'utilità del Systems Security Engineering Capability Maturity Model (SSE-CMM). La versione attuale è la 3.0, sviluppata dal modello della Canergie Mellon University del 1995

http://www.sse-cmm.org

****

6- Metriche di sicurezza

Il NIST segnala la pubblicazione del draft di un report sulle metriche di sicurezza (Interagency Report (IR) 7564, Directions in Security Metrics Research). In attesa della ISO/IEC 27004 (ma anche dopo!), questo può essere un buon punto di riferimento, insieme alla SP 800-55, su questo argomento.

NIST IR 7564: http://csrc.nist.gov/publications/PubsDrafts.html#nistir-7564
NIST SP 800-55: http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

****

7- Software ITIL compliant
(dal gruppo ITIL-certified experts di LinkedIn)

Ora che il mercato è invaso da software "ITIL-compliant", la OGC sta sviluppando uno schema di certificazione dei prodotti software.

http://www.itil-officialsite.com/News/newitilsoftwarescheme.asp

Mi chiederò sempre come si possa dichiarare una conformità a delle best practices. Soprattutto quando queste presentano molte alternative come ITIL.

La difficoltà di avere dei "requisiti certificabili" da ITIL è ampliamente dimostrata da come è stata scritta male la ISO/IEC 20000-1 e dal grosso lavoro che sta facendo il comitato SC7 della ISO per la sua revisione.

****

8- Disponibilità dei servizi

Sul gruppo "ITIL-certified experts" di LinkedIn si è avviata un'interessante discussione su come calcolare la disponibilità dei servizi. Utile per un breve ripasso.

Il calcolo deve essere fatto considerando ciascuna componente, posto che le componenti siano in serie, e moltiplicandone la disponibilità. Quindi, semplificando un po' un'architettura, se il db server è disponibile al 98%, l'application server al 98% e il firewall al 98%, la disponibilità del servizio sarà uguale al 94,1% (0,98*0,98*0,98)... oops!

Il tutto per il teorema di Bayes sulla probabilità condizionale: http://plato.stanford.edu/entries/bayes-theorem/

****

9- Sequestro pagine web
(da Filodiritto del 16 marzo 2009)

Vi segnalo questa sentenza della Cassazione sul sequestro di pagine web. Copio e incollo l'articolo di Filodiritto.

Secondo la Cassazione, l'ordinanza del tribunale del riesame che aveva revocato il sequestro preventivo di alcune pagine web (disposto dal giudice per le indagini preliminari), previa rimozione sul sito internet dell'Aduc delle espressioni e dei messaggi oggetto dei reati contestati, inibendone l'ulteriore diffusione, deve essere confermata nonostante il ricorso dell'associazione.

"Il Collegio ritiene che esattamente il tribunale del riesame ha dichiarato che nel caso di specie non trova applicazione l'articolo 21, comma 3, Costituzione, secondo cui «Si può procedere a sequestro soltanto per atto motivato dell'autorità giudiziaria nel caso di delitti, per i quali la legge sulla stampa espressamente lo autorizzi, o nel caso di violazione delle norme che la legge stessa prescriva per l'indicazione dei responsabili», dato che la concreta fattispecie in esame non rientra nella più specifica disciplina della libertà di stampa, ma solo in quella più generale di libertà di manifestazione del proprio pensiero di cui all'articolo 21, comma 1, Costituzione".

In particolare, "gli interventi dei partecipanti al forum in questione, invero, non possono essere fatti rientrare nell'ambito della nozione di stampa, neppure nel significato più esteso ricavabile dall'art. 1 della legge 7 marzo 2001, n. 62, che ha esteso l'applicabilità delle disposizioni di cui all' articolo 2 della legge 8 febbraio 1948, n. 47 (legge sulla stampa) al «prodotto editoriale», stabilendo che per tale, ai fini della legge stessa, deve intendersi anche il «prodotto realizzato ... su supporto informatico, destinato alla pubblicazione o, comunque, alla diffusione di informazioni presso il pubblico con ogni mezzo, anche elettronico». Il semplice fatto che i messaggi e gli interventi siano visionabili da chiunque, o almeno da coloro che si siano registrati nel forum, non fa sì che il forum stesso, che è assimilabile ad un gruppo di discussione, possa essere qualificato come un prodotto editoriale, o come un giornale online, o come una testata giornalistica informatica".

In sostanza, "si tratta quindi di una semplice area di discussione, dove qualsiasi utente o gli utenti registrati sono liberi di esprimere il proprio pensiero, rendendolo visionabile a tutti gli altri soggetti autorizzati ad accedere al forum, ma non per questo il forum resta sottoposto alle regole ed agli obblighi cui è soggetta la stampa (quale quello di indicazione di un direttore responsabile o di registrazione) o può giovarsi delle guarentigie in tema di sequestro che l'articolo 21, comma 3, Costituzione riserva soltanto alla stampa, sia pure latamente intesa, ma non genericamente a qualsiasi mezzo e strumento con cui è possibile manifestare il proprio pensiero. D'altra parte, nel caso in esame, neppure si tratta di un forum strutturalmente inserito in una testata giornalistica diffusa per via telematica, di cui costituisca un elemento e su cui il direttore responsabile abbia la possibilità di esercitare il controllo (così come su ogni altra rubrica della testata)".

Nè si può sostenere "che la norma costituzionale dovrebbe essere interpretata in senso evolutivo per adeguarla alle nuove tecnologie sopravvenute ed ai nuovi mezzi di espressione del libero pensiero".

Da questo assunto, infatti, "non può farsi derivare che i nuovi mezzi di comunicazione del proprio pensiero (newsletter, blog, forum, newsgroup, mailing list, chat, messaggi istantanei, e così via) possano, tutti in blocco, solo perché tali, essere inclusi nel concetto di stampa ai sensi dell'articolo 21, comma 3, Costituzione, prescindendo dalle caratteristiche specifiche di ciascuno di essi. In realtà i messaggi lasciati su un forum di discussione (che, a seconda dei casi, può essere aperto a tutti indistintamente, o a chiunque si registri con qualsiasi pseudonimo, o a chi si registri previa identificazione) sono equiparabili ai messaggi che potevano e possono essere lasciati in una bacheca (sita in un luogo pubblico, o aperto al pubblico, o privato) e, così come quest'ultimi, anche i primi sono mezzi di comunicazione del proprio pensiero o anche mezzi di comunicazione di informazioni, ma non entrano (solo in quanto tali) nel concetto di stampa, sia pure in senso ampio, e quindi ad essi non si applicano le limitazioni in tema di sequestro previste dalla norma costituzionale".

(Corte di Cassazione - Sezione Terza Penale, Sentenza 10 marzo 2009, n. 10535: Forum - Sequestro preventivo sito web).

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