Cesare Gallotti

**********

**IT SERVICE MANAGEMENT NEWS - LUGLIO 2013**

**********

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 dis-iscriversi
- 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**



**********

## 00- Editoriale

Questa newsletter arriva con un po' di ritardo, in parte per mia pigrizia, in parte perché il prossimo numero dovrebbe arrivare a metà settembre e non volevo far passare troppo tempo tra questi due numeri.

Non mi rimane che augurare a tutti un buon agosto, a coloro che si prendono una pausa e a coloro che continuano a lavorare.

E ricordo ancora: segnalate, segnalate, segnalate (oppure, commentate)!

**********

**01- Novità legali - Vigilanza Banche: Istruzioni BdI su rischi, controlli, esternalizzazioni, IT e BCM**

Vincenzo Cassati di MPS mi ha informato della pubblicazione delle "Nuove disposizioni di vigilanza prudenziale per le banche - Circolare n. 263 del 27 dicembre 2006 – 15° aggiornamento del 2 luglio 2013".

Lo si trova a questa pagina (poi bisogna scaricare l'aggiornamento 15):
- http://www.bancaditalia.it/vigilanza/banche/normativa/disposizioni/vigprud

Copio e incollo il commento di Vincenzo, che ringrazio per la segnalazione
(ho trovato interessante la lettura del documento: anche se criticabile in alcuni punti, si trovano spunti utili).

<<
E' un documento relativamente faticoso da inquadrare perché ne aggiorna un altro precedente (il 263) sommandogli 3 capitoli nuovi ed eliminando altre normative esterne e, inoltre, parte di queste notizie, insieme alle date di efficacia delle varie disposizioni, sono contenute in un ulteriore "bollettino" esterno.

Per quanto riguarda il BCM in senso stretto ci sono poche differenze rispetto a prima. Fra queste:
- processo sistemico obbligatorio la gestione del contante
- norme definite sull'outsourcing

Io faccio due considerazioni:
- se si interpreta la normativa sul BCM sine grano salis, ne possono derivare piani di continuità prolissi e ingestibili: la BIA per processi è collegata con le soluzioni di continuità, quindi 1 soluzione/ processo/ scenario/ contingency/ continuity. La numerosità e la ripetitività crescono in modo esponenziale al crescere dei processi e soprattutto degli scenari. Ve bene per la BIA, ma le soluzioni andrebbero ingegnerizzate e rese riutilizzabili al variare di processo/ unità org/ scenario.Tanto più che se la tassonomia dei processi è vera e non tarocca (cioè non è una falsa tassonomia dove 1 ufficio=1 processo) ogni ufficio, spesso con le stesse persone, esegue più di un processo critico.

- è richiesta la dichiarazione formale dello stato di crisi, a partire dalla quale partono i tempi, con la raccomandazione di arrivare alla situazione di crisi il prima possibile. In uno SLA questo criterio non lo userei.
>>

**********

**02- Novità legali - Wi-fi libere? Boh!**

Nel DL 69 del 2013 (il famoso Decreto del "fare") è presente l'articolo 10 con le pubblicizzate disposizioni per il wi-fi libero.

Se ho capito giusto: chiunque offra l'accesso Internet, quando questa non è la sua attività prevalente (immagino quindi hotel, bar e aziende con connessioni per gli ospiti), non hanno più l'obbligo di registrare i dati dell'utente. Però devono "garantire la tracciabilità del collegamento (MAC address)".

Ecco... arrivato a questo punto mi sono chiesto se questo non sia peggio della precedente disposizione (DL 144 del 2005, poi convertito dalla Legge 155 del 2005) perché quelli che si erano già adeguati, se vogliono continuare ad essere conformi alla normativa, dovranno fare altri investimenti.

Comunque: aspettiamo fino a quando il DL sarà convertito in Legge e speriamo negli emendamenti.

Il DL elimina anche le disposizioni sulla certificazione degli impianti di connessione alla rete informatica pubblica, abrogando la normativa pertinente (cioè il Dlgs 198 del 2010 che a sua volta aveva abrogato la Legge 109 del 1991).

Per chi volesse approfondire, segnalo questo post sul blog de l'Espresso segnalato sul gruppo infotechlegale.it di LinkedIn:
- http://scorza.blogautore.espresso.repubblica.it/2013/06/22/wifi-decretodelfare-c%E2%80%99etantodarifare/

Per chi non apprezza il pdf segnalato dal post, il DL 69 è anche presente su www.normattiva.it.

**********

**03- Standardizzazione - Sito sulle future ISO/IEC 27001 e 27002**

Dopo aver letto e ascoltato di tutto e di più sulle future ISO/IEC 27001 e 27002, ho avuto notizia di questo link, che ritengo essere molto interessante per tutti coloro che ne vogliono sapere di più:
- http://www.gammassl.co.uk/27001/revision.php

**********

**04- Standardizzazione - NIST SP 800-124 sui mobile devices**

Il NIST ha annunciato la pubblicazione della Special Publication 800-124 Revision 1, "Guidelines for Managing the Security of Mobile Devices in the Enterprise". La trovate al link:
- http://csrc.nist.gov/publications/PubsSPs.html#800-124

E' una guida breve, con le "solite" indicazioni per la sicurezza dei dispositivi mobili (password per accedere, cifratura dei dati, wiping dei dati, whitelisting delle apps, eccetera). Alla fine, proprio in fondo, si trovano 3 simpatici link ai "Mobile Device Security-Related Checklist Sites".

Un solo dubbio: sono indicati dei sistemi per il controllo centralizzato dei dispositivi mobili, anche BYOD (mobile device management solutions); mi chiedo perché non pubblichino una sorta di lista di comparazione degli stessi. Credo possa essere utile.

**********

**05- Bring Your Own Device - Un articolo**

Segnalo questo articolo sul Bring Your Own Device di Antonio Ieranò e diffuso dal gruppo Clusit su LinkedIn.

L'ho trovato interessante perché presenta una storia dei dispositivi portatili dagli anni Settanta ad oggi e qualche riflessione su come si sono modificati (o, meglio, non modificati) gli atteggiamenti verso la sicurezza:
- http://aitechupdate.wordpress.com/2013/07/15/bring-your-own-deviceparte-1-dal-webminar-che-ho-tenuto-per-isc2/
- http://aitechupdate.wordpress.com/2013/07/16/bring-your-own-deviceparte-2-dal-webminar-che-ho-tenuto-per-isc2/
- http://aitechupdate.wordpress.com/2013/07/16/bring-your-own-deviceparte-3-dal-webminar-che-ho-tenuto-per-isc2/
- http://aitechupdate.wordpress.com/2013/07/18/bring-your-own-deviceparte-4-dal-webminar-che-ho-tenuto-per-isc2

**********

**06- Standardizzazione - GPG 2013 sulla business continuity**

Segnalo la pubblicazione delle " Good Practice Guidelines 2013 - Global Edition - A Guide to Global Good Practice in Business Continuity". Io apprezzo molto le GPG del BCI, anche se costano ben 25 sterline!

Sono l'evoluzione dell'edizione del 2010, con un maggiore allineamento alla ISO 22301. Personalmente, non mi sembra abbiano apportato straordinari cambiamenti rispetto alla precedente edizione, a parte qualche termine modificato e una grafica più accattivante.

Il link: http://www.thebci.org/index.php/resources/the-good-practice-guidelines

Per chi invece volesse dedicarsi solo al materiale gratuito, segnalo la ottima SP 800-34 del NIST:
- http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

oppure un giro nella Knowledge Bank del The BCI:
- http://www.thebci.org/index.php/resources/knowledgebank

**********

**07- Standardizzazione - Nuova ISO 9001: prevista per il 2015**

Dalla newsletter del DNV Italia, segnalo questo articolo sulla futura ISO 9001:
- http://www.dnvba.com/it/information-resources/news/Pages/Nuova-ISO-9001.aspx

In poche parole: ne è prevista la nuova edizione nel 2015.

Ho avuto la possibilità di leggerne una bozza, ma non pienamente significativa. Sono molto curioso di vedere come adotteranno il Testo comune per i sistemi di gestione (il cosiddetto Annex SL). Nella bozza che ho visto, sono stati più coraggiosi di noi del SC27 nel modificare il testo base, ma chissà come arriverà alla fine del percorso.

**********

**08- Novità legali - Aggiornamento sul Regolamento Europeo Privacy**

Ricevo da Stefano Tagliabue di Telecom Italia "un aggiornamento sui (lenti) avanzamenti del processo di approvazione del General Data Protection Regulation":

<<
E' stato confermato che la votazione in Commissione LIBE (Libertà Civili, Giustizia e Affari Interni) della bozza di relazione sulla proposta della Commissione di Regolamento sulla protezione dei dati è stata rimandata ulteriormente al prossimo ottobre.

LIBE negli scorsi mesi ha ricevuto i pareri delle altre commissioni coinvolte (IMCO, JURI, INTRE, EMPL ) e, a causa dell'ingente numero di emendamenti presentati –più di 3000-, la votazione, inizialmente programmata per il 24 aprile, è successivamente slittata a fine maggio, luglio ed ora ad ottobre. Non è ancora stata pubblicata la data precisa.

La transizione dovrebbe avvenire dopo due anni dalla pubblicazione del Regolamento nella Gazzetta Ufficiale della Comunità Europea, almeno stando alla bozza attuale.
>>

**********

**09- Axelos: la Joint venture di ITIL**

Il mese scorso avevo segnalato la nascita della joint venture tra the Cabinet Office (UK) e Capita plc per gestire il Best Management Practice portfolio, di cui fa parte ITIL:
- http://blog.cesaregallotti.it/2013/06/itil-venduto-ad-una-joint-venture.html

Con comunicato stampa del 1 luglio 2013, è stato comunicato che questa joint venture si chiama Axelos.

Per saperne (poco) di più, segnalo il link al ITSM Portal:
- http://www.itsmportal.com/news/and-its-name-axelos-joint-venture-cabinet-office-and-capita

**********

**10- La formazione sulla sicurezza è utile? (risposte - parte 3)**

Ad aprile avevo pubblicato un post dal titolo "La formazione sulla sicurezza è utile?":
- http://blog.cesaregallotti.it/2013/04/la-formazione-sulla-sicurezza-e-utile.html

Mauro Cicognini di WID Consulting mi ha dato il suo punto di vista. Dico che mi pare molto condivisibile e sfuma meglio quanto da me scritto (infatti, io stesso erogo corsi di formazione e sensibilizzazione sulla sicurezza; non posso reputarli sempre inutili!).

Quindi, copio e incollo la risposta di Mauro, ma prima ricordo le altre risposte ricevute:
- http://blog.cesaregallotti.it/2013/04/la-formazione-sulla-sicurezza-e-utile.html
- http://blog.cesaregallotti.it/2013/06/la-formazione-sulla-sicurezza-e-utile.html

<<
Leggendo bene il post di Schneier (https://www.schneier.com/blog/archives/2013/03/security_awaren_1.html) - come al solito, effettivamente molto ben scritto - e le varie reazioni che ha ricevuto, mi trovo in realtà molto più vicino all'opinione di David Kennedy (linkata dallo stesso Bruce sul suo post).

Trovo il post di Bruce molto parziale, puntato com'è esclusivamente su contromisure tecnologiche che, per quanto importanti, come sappiamo non sono sufficienti a portare a casa il risultato: a me viene in mente quello che mi raccontano i miei amici che di mestiere fanno i Penetration Tester, che ottengono il risultato nel 100% dei casi, e nella maggior parte di essi usano non la tecnologia ma una qualche combinazione di tecniche di social engineering. Difficile dire quindi che la formazione delle persone non conti.

Il "dettaglio" di cosa intendiamo per formazione, ovviamente, fa la differenza, e - come autorevolmente commentato anche da chi ha risposto a Bruce - non è lecito inferire dal fatto che la maggior parte dei programm di formazione sulla sicurezza fanno schifo (indubitabile) il fatto che allora la formazione sulla sicurezza non serve. Il sillogismo non regge.

Ciò detto, le due cose positive che scrive, sono in realtà assolutamente vere, giuste, commendabili, e da divulgare il più possibile:
1. spendere di più per educare i programmatori sulla sicurezza. Bisogna davvero spendere molto di più per formare i programmatori; anzi mi verrebbe voglia di prendere per le orecchie quanti ancora oggi si dimenticano di inserire alcune cose assolutamente basilari come la validazione dei dati in ingresso.
2. almeno una parte della consapevolezza che gli utenti hanno della sicurezza deve essere "respirata nell'aria", percepita in modo informale, ecc., come peraltro scrivi anche tu riferendoti alle pratiche e alla cultura aziendale (ma non basta, la sicurezza non può fermarsi alla cancellata dell'azienda).
>>

Il link all'articolo di David Kennedy:
- https://www.trustedsec.com/march-2013/the-debate-on-security-education-and-awareness/

**********
**11- Quaderno Clusit: "Certificazioni Professionali in Sicurezza Informatica 2.0"**

Con molto piacere, segnalo la pubblicazione del Quaderno Clusit: "Certificazioni Professionali in Sicurezza Informatica 2.0".

Gli autori siamo io e Fabio Guasconi.

Sono molto contento del risultato ottenuto, sia per la raccolta e schematizzazione dei dati sia perché nell'introduzione siamo riusciti a esporre i pregi delle certificazioni professionali insieme alle dovute cautele da prendere.

Il Quaderno è disponibile su http://www.clusit.it/download/Q09_web.pdf.

**********
**12- Recensione "Flawless Consulting"**

Piccola recensione del libro "Flawless consulting - 2ed." di Peter Block (Pfeiffer, USA, 2000).

Quando me lo sono trovato tra le mani, ho pensato fosse inutile e pretenzioso. Infatti ci ho messo 5 anni per decidere di dargli una possibilità e ho scoperto che mi sbagliavo.

L'autore è un americano e alcune cose fanno riflettere sulle differenze di culture. La più evidente è quando dice che i consulenti si vestono casual mentre gli interni in giacca e cravatta. In Italia non

sembra... Inoltre, presenta alcune riflessioni che non condivido pienamente e un metodo di lavoro non applicabile a tutti i lavori di consulenza.

Detto ciò, ci sono cose molto interessanti. Provo a elencarne solo alcune:
- è importate che consulente non ha il compito di scegliere, ma solo di dare la sua opinione (in altre parole, non deve illudersi di essere un manager, non deve prendere le decisioni per il management, non deve arrabbiarsi se il management agisce diversamente da come avrebbe voluto)
- il lavoro di consulenza deve essere fatto al 50-50% tra cliente e consulente;
- qualunque manager ha paura, a fronte di cambiamenti, di perdere potere e controllo e ci sono diversi metodi per riconoscerla e affrontarla da parte del consulente;
- è importante, in fase di contrattazione, non solo stabilire cosa vuole il cliente dal consulente, ma anche cosa vuole il consulente dal cliente (oltre ai soldi... e ho finalmente capito perché sono a disagio quando la contrattazione l'ha fatta un altro);
- un consulente deve sempre rinunciare ai lavori che non può seguire come vuole lui;
- se un consulente segnala altri consulenti, deve farlo gratis;
- è meglio non credere a chi ti chiede sconti perché poi ci saranno "grandi opportunità".

Certo: parla di consulenti, non dei prestatori di manodopera, così come purtroppo troppo spesso siamo visti.

**********

**13- Raccomandazioni della FDA per i dispositivi medici**

Dalla newsletter SANS Newsbytes trovo la notizia per cui l'agenzia USA Food and Drug Administration (FDA) ha pubblicato delle raccomandazioni sulla sicurezza dei dispositivi medici:
-
http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm356186.htm
- http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm

Trovo interessante ed inquietante che i dispositivi medici siano così vulnerabili alle minacce informatiche. Inoltre, sembra che le loro configurazioni di default siano molto insicure.

Personalmente sono contento della strada presa da Microsoft e altri nel rendere più sicura la configurazione di default dei loro sistemi, ma ancora non capisco perché ciò non succeda anche per gli altri software, soprattutto se critici come quelli collegati a dispositivi medici (credo che alcune colpe siano anche di auditor e consulenti).