****
IT SERVICE MANAGEMENT NEWS - Luglio 2011
****

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

****
00- Editoriale

Il prossimo numero uscirà a metà settembre.

Vi auguro quindi un "buon agosto": a chi va in vacanza e a chi resta a lavorare.

In questi mesi ho riflettuto sulla possibilità di lanciare una proposta di incontro (a gennaio, il mese solitamente più tranquillo) per discutere e riflettere su novità e casi reali. Pensavo a qualcosa di gratuito (tranne forse l'affitto di un locale), di specialistico (evitare i venditori di se stessi o di fumo o di prodotti non ancora sviluppati o i relatori che partono sempre da zero), che inviti alla discussione (pubblicazione delle presentazioni con anticipo rispetto all'incontro) e di ben controllato (scelta accurata degli argomenti). Ogni volta vedo i pro e i contro di questa idea. Se qualcuno ha voglia di aiutarmi ad andare avanti, me lo faccia sapere. Si accettano anche risposte del tipo "non ti posso aiutare, ma parteciperei".

****

01- Privacy: dei Titolari e dei Responsabili esterni - Parte 3

Seguito del post http://blog.cesaregallotti.it/2011/04/privacy-dei-titolari-e-dei-responsabili_04.html

Fabrizio Bottacin mi ha inviato alcuni riferimenti a sentenze del Garante.

Io riassumo (e commento) come segue:
- il 2 giugno 1999 [doc. web n. 39857] il Garante ha stabilito che un fornitore dell'INPS dovesse essere nominato Responsabile esterno (commento di Cesare: non dice però che "ogni fornitore deve essere nominato Responsabile esterno")
- il 29 luglio 1998 [doc. web n. 31023] il Garante stabilisce che una struttura esterna ad un soggetto pubblico può essere nominata Responsabile o detenere la qualità di Titolare (commento di Cesare: si osservi che vigeva la Legge 675/1996)
- il 8 giugno 1999 [doc. web n. 42260] il Garante ha stabilito che le società fornitrici non possono essere nominate "incaricate esterne", ma "Responsabili" (commento Cesare: faccio notare che nulla viene detto sulla possibilità o impossibilità di autonoma titolarità)

Altre sentenze di interesse:
- Garante 7 luglio 1998: doc. web n. 40377
- Garante 24 gennaio 2003: doc. web n. 1067875
- Garante 23 marzo 1998: doc. web n. 40999
- Garante 10 giugno 2003: doc. web n. 1132569

Simone Tomirotti, avendomi segnalato il "Provvedimento banche" (doc. web n. 1813953), segnala la frase: "la posizione di Titolare del trattamento, pur astrattamente riconoscibile anche in capo all'outsourcer, risulta, tuttavia, ascrivibile solo alla banca nei casi in cui la stessa abbia il potere di:
1. assumere decisioni relative alle finalità del trattamento;
2. impartire istruzioni e direttive vincolanti nei confronti delle società di gestione dei sistemi informativi, sostanzialmente corrispondenti alle istruzioni che il titolare del trattamento deve impartire al responsabile;
3. svolgere funzioni di controllo rispetto all'operato delle medesime e degli incaricati delle stesse."

Ho avuto modo di leggere una noticina (quindi da non considerare come definitiva) di AbiLab che traduce così "E' stata confermata la possibilità di qualificare l'outsourcer, sia esso interno od esterno al gruppo bancario, quale autonomo titolare del trattamento qualora i poteri riconosciuti dal Codice della Privacy al titolare del trattamento risultino *in concreto* in capo all'outsourcer e non alla banca."

Ringrazio Fabrizio e Simone per il contributo.

****

02- Privacy: dei Titolari e dei Responsabili esterni - Parte 4

Il 15 giugno, il Garante ha emesso un Provvedimento dal titolo "Titolarità del trattamento di dati personali in capo ai soggetti che si avvalgono di agenti per attività promozionali".

In questo caso, invita le aziende che danno mandato ad agenti per le attività promozionali a nominare tali agenti "Responsabili del trattamento".

Questo pare contraddire alcune riflessioni fatte in post precedenti:
- http://blog.cesaregallotti.it/2011/06/privacy-dei-titolari-e-dei-responsabili.html
- http://blog.cesaregallotti.it/2011/04/privacy-dei-titolari-e-dei-responsabili_04.html
- http://blog.cesaregallotti.it/2011/06/privacy-dei-titolari-e-dei-responsabili.html

Aggiungo queste riflessioni:
- in questo caso specifico, si tratta di contratti di agenzia e il Garante evidenzia che gli agenti agiscono già nei fatti come responsabili (perché controllati dal cliente, perché agiscono in suo nome, eccetera)
- nel Provvedimento si cita la definizione di Titolare "cui competono, anche unitamente ad altro titolare, le decisioni...", ma furbescamente si omette la parte "anche unitamente ad altro titolare" e ancora una volta si evita di darne un'interpretazione
- il Provvedimento asserisce che il Titolare esercita già nei fatti il "controllo" sugli agenti, ma non cita neanche una modalità con cui questo viene effettuato, laddove ogni dizionario equipara il termine "controllo" con quello di "verifica" e non con quello di "fornire indicazioni"; anche qui, ancora una volta, si evita di darne un esempio (mi ricorda molto le non definite modalità di "verifica" delle attività degli Amministratori di Sistema).

Ecco qui il link al Provvedimento:
http://www.garanteprivacy.it/garante/doc.jsp?ID=1821257

****
03- Novità su ITIL v3.1

Un post di Luigi Buglione su LinkedIn fornisce il link al documento ufficiale sulle novità di ITIL v3.1.
http://www.best-management-practice.com/gempdf/ITIL_UPdate_FAQs_Summer_2011_June11.pdf

Innanzitutto il titolo ufficiale sarà "ITIL 2011" anche se tutti, quasi sicuramente, lo chiameremo ITIL v3.1.

La data di pubblicazione è il 29 luglio 2011, prima in formato cartaceo e poi in formato elettronico.

La novità più importante riguarderà la fase di Strategy. Per le altre fasi, ci saranno "chiarimenti". Il documento non sembra dare indicazioni sui tanti argomenti attualmente confusi.

Ultima cosa interessante è che "chi è già in possesso di certificati ITIL, non avrà la necessità di ri-certificarsi": se capisco bene, le qualifiche ITIL 2007 e ITIL 2011 saranno uguali quindi indistinguibili tra loro.

Il commento di IT Skeptic fornisce ulteriori spunti di riflessione:
http://www.itskeptic.org/itil-v3-2011-new-book-and-four-new-processes

****

04- Cobit 5: il draft

L'ISACA ha pubblicato il draft del Cobit5 e chiede commenti. A inizio 2012 dovrebbe pubblicare la versione finale.

Non sono un esperto di Cobit e quindi mi guardo bene dal commentarlo. Ritengo però sia necessario conoscerlo perché propone dei modelli molto interessanti, con carte RACI e un elenco di misure tra cui scegliere.

Mi pare di notare che in questa edizione non siano più utilizzati i modelli di maturità come nel passato, preferendo un modello generale descritto una volta per tutte nel documento di descrizion del framework.

http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-5-Initiative-Status-Update.aspx

****

05- Sulla formazione sulla sicurezza

In molti mi chiedono "quale corso seguire" sulla sicurezza. A questo proposito, copio, traduco con qualche modifica e incollo l'editoriale di Hervé Schauer sulla newsletter della sua società di consulenza HSC (sito web www.hsc.fr).

<< Presso HSC un consulente su due ha fatto un master sulla sicurezza. Con questo, hanno imparato, non sempre benissimo, cose che si imparano facilmente in azienda o con la formazione continua. Sono formati a rispondere bene durante i colloqui, ma non a fare quello che oggi non si insegna più nelle aziende: dai fondamentali dell'informatica alla corretta scrittura in francese, oltre a qualche qualità umana.

20 dopo alcune mie iniziative di promozione di corsi specialistici e in un altro contesto, penso che la moltiplicazione dei corsi sulla sicurezza sia nefasta e inutile. Si basa solo sul profitto. Solo la crittologia giustifica pienamente un insegnamento universitario superiore. La scuola deve insegnare a pianificare, amministrare, sintetizzare, essere disciplinati e imparare a imparare e non tecniche di intrusione o le tecniche di risk assessment. >>

Credo che quando Hervé Schauer nomina la "formazione continua" intenda anche i corsi specialistici di poche giornate, per differenziare questi corsi dai master universitari o simili. In questo caso l'avrei scritto in modo diverso, ma condivido appieno.

****

06- Top 25 Most Dangerous Software Errors

Agli americani piace fare classifiche e non sempre significative. Questa del SANS però è interessante e importante perché allinea gli errori di sviluppo più comuni e pericolosi e fornisce linee guida per evitarli.

- la pagina di introduzione del SANS: http://www.sans.org/top25-software-errors/
- il report: http://cwe.mitre.org/top25/

****

07- Sicurezza iPhones e Android

Sul gruppo Clusit di LinkedIn, Aldo Ceccarelli segnala questo articolo della Symantec sulla sicurezza di iPhone e Android:
- l'articolo su Networkworld: http://www.networkworld.com/news/2011/062811-symantec-mobile-report.html
- il rapporto della Symantec:
http://www.symantec.com/content/en/us/about/media/pdfs/symc_mobile_device_security_june2011.pdf

Non si parla di Blackberry, l'unico per il quale il NIST ha prodotto una check list di sicurezza:
http://web.nvd.nist.gov/view/ncp/repository/checklistDetail?id=252

Segnalo quindi la guida 800-124 del NIST sulla sicurezza di cellulari e PDA:
http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf

****

08- NIST SP 800-82 sulla sicurezza dei sistemi informatici industriali

Il NIST ha pubblicato la propria guida per la sicurezza dei sistemi SCADA, DCS e PLC.

Come sempre, la guida inizia con una ottima parte introduttiva che descrive compiutamente i sistemi oggetto del documento e poi via via descrive le minacce, le vulnerabilità e i controlli applicabili.

- La pagina con tutte le SP del NIST: http://csrc.nist.gov/publications/PubsSPs.html
- Il link diretto alla SP 800-82: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

****

09- Sulle survey sulla sicurezza

Aldo Ceccarelli, sul gruppo Clusit di LinkedIn, ha postato questo interessante articolo sulle survey sulla sicurezza:
http://www.technologyreview.com/business/37839/?ref=rss

Questo articolo mi ha ricordato un piccolo dibattito che abbiamo avuto qualche tempo fa su non-mi-ricordo-quale survey.

Io dicevo che mi lasciano sempre perplesso e, giustamente, Aldo rifletteva sul fatto che comunque forniscono qualche spunto interessante.

Questo articolo dice proprio che le survey sulla sicurezza forniscono "qualche spunto". Non di più.

****

10- Business Continuity e Incident Management (parte 3)

Sempre sul BCM (il post numero 2 è su http://blog.cesaregallotti.it/2011/05/un-contributo-su-business-continuity-e.html).

Dante Verona mi fa notare quanto segue.

"Ho un modo diverso di argomentare il mio punto di vista, ed è quello che considero più concreto ed efficace ed è in linea con standard BS25999.

Il BS25999-2:2007, al punto 4.1.1.2.c, dice: "The organization shall: establish the maximum tolerable period of disruption for each activity by identifing:....."

E, richiamando la definizione di Maximum Tolerable Period of Disruption presente nello standard stesso, troviamo: "duration after which an organization's viability will be irrevocably threatend if product and service delivery cannot be resumed"

Quindi io escluderei i piccoli incidenti se con piccoli intendiamo quelli che non minacciano la sopravvivenza della organizzazione. E il motivo di ciò per me è molto concreto. Confinare gli scenari BCM è una questione di successo del programma stesso."

Io credo che Dante parli della "parte di BCM per grandi eventi" (definizione mia). Per i piccoli incidenti c'è invece il "BCM per piccoli eventi" (dove la gestione degli incidenti è regolamentata da SLA basati anche sul termine di urgenza, proprio per evitare che un "normale incidente" diventi grande). Fanno parte tutti e due del BCM, ma sono affrontati con metodi e tecniche distinte.

Dante mi ha fatto notare che il "BCM per grandi eventi" e il "BCM per piccoli eventi" nelle grandi organizzazioni sono spesso seguiti da funzioni diverse con budget diversi. Il metterli insieme (come vuole un certo impianto teorico) può portare all'insuccesso del programma di BCM.

Quindi, concludendo, è importante distinguere bene, in fase di analisi, i confini di ciascuna area (si osservi che questa posizione non è scorretta, visto che applica la filosofia del problem solving "dividere un problema in sotto-problemi più facilmente risolvibili").