****
IT SERVICE MANAGEMENT NEWS - Settembre 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 (sulle proposte senza successo)

Nella newsletter del 16 luglio 2011 avevo proposto di organizzare a gennaio-febbraio 2012 un incontro di studio tra quanti volevano discutere di sicurezza delle informazioni, gestione dei servizi IT e qualità senza fronzoli e senza vaghezze (no sponsor, no interventi generici, eccetera).

Ho ricevuto 6 adesioni (con me, arriviamo a 7). Direi molto poche.

Però non demordo e vi chiedo:
- se siete interessati
- se qualcuno ha delle proposte di intervento (casi reali, riflessioni su novità legali o su nuovi standard, elementi di dibattito su varie interpretazioni)
- se avete proposte per il titolo ("Gallotti & friends" è già stata bocciata...)

Poi, vedremo se e come andare avanti. Intanto, ringrazio Paolo Carcano per la disponibilità.

****

01- Novità Legali - Legge 106 del 2011 con modifiche al Codice Privacy

A maggio era stato emesso il DL 70 del 2011 che (all'articolo 6, comma 2), tra le altre cose, presentava alcune semplificazioni in materia di privacy. Ora il DL è stato definitivamente approvato (come mi ha segnalato Franco Ferrari del DNV) con la Legge 106 del 2011.

Anche con l'aiuto della circolare 19439 di Confindustria (disponibile solo agli iscritti di Confindustria e altri siti), provo a riassumere i punti rilevanti:

1. fornita una nuova definizione di "trattamenti effettuati per finalità amministrativo-contabili", che semplifica gli adempimenti di gestione del personale; osservo però che molti comportamenti di "buona condotta" del datore di lavoro (applicazione di misure di sicurezza e non diffusione dei dati) rimangono attivi.

2. esclusi dall'ambito di applicazione del Codice i trattamenti di dati effettuati nei rapporti business to business (B2B) per finalità amministrativo-contabili, con semplificazioni nella gestione dei clienti e fornitori quando non sono persone fisiche, eliminando la necessità di informative e raccolte di consenso (peraltro già molto ridotte nel testo originale del 2003); si potrebbe anche vedere ridotti gli oneri sull'applicazione delle misure minime e sulle nomine dei responsabili, ma questo rappresenterebbe una cattiva pratica gestionale, oltre che introdurre complicazioni quando si deve analizzare gli impatti di ogni misura minima sui dati personali oggetto del Codice e quelli esclusi

3. esonerate dal consenso le comunicazioni di dati nell'ambito di gruppi d'impresa, con ovvi benefici per le realtà di gruppo

4. esteso l'ambito di applicazione dell'autocertificazione sostituiva del DPS; ma, abbiamo visto, in alcuni casi è più "facile" fare il DPS che seguire le istruzioni per l'autocertificazione, oltre che più produttivo, se fatto correttamente

5. esclusione dell'obbligo di informativa e consenso per i curricula vitae trasmessi spontaneamente dall'interessato; con altri ovvi benefici

6. l'estensione del regime di opt-out previsto per le telefonate commerciali anche al marketing mediante posta cartacea, perché hanno impatto sulle persone fisiche

Il testo del DL 70 del 2011 consolidato con la Legge 106 del 2011 e il testo aggiornato del Codice Privacy si trovano su www.normattiva.it (cercando il solo DL 70 del 2011).

****

02- Novità Legali - Regole tecniche documento informatico

Segnalazione ricevuta da Uninfo: DigitPA ha pubblicato la bozza delle regole tecniche documento informatico e gestione documentale, protocollo informatico e sistema conservazione di documenti.

Queste regole dovrebbero sostituire la Circolare CNIPA 11/2004 e AIPA 28/2001 e prendere in carico i requisiti del CAD dopo le modifiche apportate dal Dlgs 235 del 2010.

La bozza è stata pubblicata il 5 agosto e i commenti possono essere inviati entro il 10 settembre. Non commento i tempi.

Può essere comunque utile leggere il materiale proposto:
http://www.digitpa.gov.it/altre-attivit/pubblicata-bozza-regole-tecniche-documento-informatico-protocollo-informatico-conserva

****

03- Novità Legali - Schema di regolamento su Diritto d'Autore su Internet

Giovanni Francescutti (DNV Italia) segnala l'iniziativa dell'Autorità per le Garanzie nelle Telecomunicazioni sul Diritto d'Autore. In particolare, l'AGCOM ha presentato uno "schema di regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica".

Riguarda soprattutto il ruolo e le responsabilità degli ISP nel pubblicare contenuti non rispettosi del Diritto d'Autore e le modalità che dovranno seguire.

E' possibile leggere il Comunicato Stampa del 6 luglio 2011:
http://www.agcom.it/Default.aspx?message=visualizzadocument&DocID=6663

Lo schema di regolamento in consultazione pubblica per 60 giorni:
http://www.agcom.it/Default.aspx?DocID=6694

La delibera 398 del 2011 dell'AGCOM con indicati i diversi contributi ricevuti per la redazione dello schema di regolamento:
http://www.agcom.it/Default.aspx?DocID=5413
Nota: quello che qui è chiamato "schema", altri chiamerebbero "bozza".

Sarà ovviamente interessante vedere come andrà avanti l'iniziativa e i successivi commenti.

Intanto segnalo già i primi due commenti di Simone Tomirotti che gentilmente me l'ha segnalato:
- http://italianjam.blogspot.com/2011/07/lagcom-e-il-diritto-dautore-la-mia.html
- http://italianjam.blogspot.com/2011/08/la-proposta-dellagcom-e-blanda.html

****
04- Novità Legali - Sentenza: Accessi abusivi e 231

Dalla newsletter di Filodiritto segnalo questa sentenza della Cassazione Penale.
http://www.cortedicassazione.it/Notizie/GiurisprudenzaPenale/SezioniSemplici/SchedaNews.asp?ID=1698

La sentenza tratta di diverse cose. Quelle di rilievo per questa newsletter sono:
- Punto 9.3: "commette il reato di cui all'articolo 615ter Codice Penale non solo chi si introduca abusivamente nel sistema informatico protetto, ma anche chi si intrattenga al suo interno [Nota di Cesare: pur essendo un utente autorizzato del sistema], contro la volontà espressa o tacita di chi abbia diritto di escluderlo, per finalità diverse da quella per le quali l'abilitazione era stata concessa."; in altre parole: gli utenti autorizzati che usano il sistema informatico per raccogliere dati, senza averne il permesso esplicito o tacito, commette reato perché abusano della propria posizione
- Punto 11.3: la società capogruppo può essere chiamata a rispondere, ai sensi del d. lgs. n. 231 del 2001, per il reato commesso nell'ambito dell'attività di altra società del gruppo, purchè nella sua consumazione concorra una persona fisica che agisca per conto della holding perseguendo anche l'interesse di quest'ultima.

L'articolo su Filodiritto:
http://www.filodiritto.com/index.php?azione=archivionews&idnotizia=3258

****

05- Novità Legali - Firma digitale, questa sconosciuta

Luca De Grazia mi segnala un articolo che lo riguarda in merito alle sue disavventure nel fare accettare dalla Pubblica Amministrazione dei documenti firmati digitalmente.
http://affaritaliani.libero.it/mediatech/firma_digitale130711.html

Mi sono ricordato anche che, in forza dell'articolo 16 del DL 185 del 2008) il 29 novembre tutte le imprese dovranno avere la Posta Elettronica Certificata per comunicare con la Pubblica Amministrazione. Luca De Grazia mi ha ricordato che la PEC è strumento diverso dalla sottoscrizione con firma digitale. Se però oggi siamo a questo punto, sicuramente ne vedremo delle belle.

****

06- Novità Legali - Garante Privacy: Cloud e smartphones

Il 23 giugno, il Garante ha pubblicato due "schede di documentazione":
- "Cloud computing: indicazioni per l'utilizzo consapevole dei servizi":
http://www.garanteprivacy.it/garante/document?ID=1819933
- "Smartphone e tablet: scenari attuali e prospettive operative":
http://www.garanteprivacy.it/garante/document?ID=1819937

Mi viene da notare che il Garante sta ora espandendo la propria area di azione alla informazione sulla sicurezza informatica, oltre al trattamento dei dati personali.

****

07- Standardizzazione - ITIL 2011

Il 29 luglio è stata pubblicata la versione 2011 di ITIL. Come già detto, non si tratta di una versione 4, ma di una versione 3.1.

Faccio un breve riassunto delle novità, affidandomi alla newsletter del 3 agosto di itSMF Italia (i commenti sono miei, ovviamente):
- le nuove pubblicazioni sono acquistabili da itSMF Italia (www.itsmf.it) o da www.best-management-practice.com; il costo è di non poche 360 sterline inglesi (410 Euro);
- se già le pubblicazioni del 2007 vi sembravano corpose (un totale di 1.344 pagine), sappiate che le cose non sono migliorate: ora il numero totale di pagine è di 1.888:
- buona notizia: non sono previsti aggiornamenti (o "bridge") delle certificazioni ottenute negli anni scorsi su ITILv3; in altre parole, se avete già un certificato ITILv3 Foundation o Intermediate o Expert, è ancora valido;
- non è stato ridotto il numero di processi: ora la Service Strategy ne prevede 5 e al Service Design è stato aggiunto il processo di Design Coordination (che in effetti mancava... come era facilmente intuibile); gli altri rimangono dove sono: i redattori di ITIL2011 hanno dimostrato di non voler buttare via nulla e hanno lasciato dei "processi" che sono evidentemente delle "attività".

Ad ogni modo, i nuovi esami sono disponibili dal 8 agosto.

Per chi se la sente: buona lettura!

****

08- Standardizzazione - ISO/IEC 27035:2011 su Incident management

Il 1 settembre è stata pubblicata la ISO/IEC 27035:2011 dal titolo "Information technology — Security techniques — Information security incident management". Questa norma della famiglia ISO/IEC 270xx sostituisce la ISO/IEC TR 18044:2004.

Oltre alle cose già note e ripetute in mille altri contesti (scrivere politica, registrare gli incidenti, eccetera), sono sviluppati i seguenti argomenti:
- istituzione di un ISIRT (o CERT)
- un'appendice con degli esempi di incidente
- un'appendice con esempi di categorizzazione degli incidenti (in molti, in questi anni, mi hanno chiesto se c'era uno standard con questi esempi; la ISO/IEC TR 18044 non li aveva, ora ci sono)
- esempi di reportistica (già presenti nella ISO/IEC TR 18044)

Ovviamente, non mancano riflessioni su escalation, analisi approfondite dopo aver superato l'emergenza, computer forensics, gestione delle comunicazioni, eccetera.

Il tutto è molto orientato al trattamento di attacchi o di gravi incidenti, ma nell'incident management è necessario includere anche la gestione di eventi meno significativi. Ovviamente, chi seguirà questo standard farà in modo di implementarlo in modo corretto.

Le norme ISO costano (www.iso.org). Per chi vuole risorse autorevoli e gratuite, segnalo la guida del NIST (http://csrc.nist.gov/publications/PubsSPs.html), SP 800-61 "Computer Security Incident Handling Guide" del 2008:
http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

Grazie a Franco Ferrari del DNV Italia per la segnalazione.

****
09- Standardizzazione - ISO 29110: Software Life Cycle Profiles and Guidelines for Very Small Entities

Nel 2011 è stata pubblicata la ISO 29110 sul ciclo di vita del software per le piccole imprese (fino a 25 persone). Si tratta di uno standard diviso in 5 parti.

Per saperne di più:
https://secure.wikimedia.org/wikipedia/en/wiki/ISO_29110:Software_Life_Cycle_Profiles_and_Guidelines_for_Very_Small_Entities_%28VSEs%29

La notizia mi arriva dal gruppo di LinkedIn "ISO/IEC JTC 1/SC7 Software and Systems Engineering".

Alla fine dell'articolo, ci sono i link per procurarsele. Tre delle 5 parti sono gratis:
http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.

****

10- Standardizzazione - BS 10008:2008 sulle prove informatiche

Max Cottafavi (Spike Reply) mi segnala che è da tempo pubblicata la BS 10008:2008 dal titolo "Evidential weight and legal admissibility of electronic information. Specification".

Leggendo la presentazione sul sito del BSI Group, mi pare che non sia una anticipazione della ISO/IEC 27037 sulla computer forensics, bensì una norma sulla autenticità dei documenti e delle comunicazioni informatiche. Insomma, qualcosa di molto legata alla firma digitale, per la quale, in Italia, vige il Codice dell'Amministrazione Digitale (Dlgs 82 del 2005) e, quindi, forse questo standard non è utile per le nostre imprese.

Ad ogni modo, posso sempre sbagliarmi e lascio a voi la valutazione (nel caso, provvederò a pubblicare commenti):
http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030191165

****

11- Standardizzazione - Versione italiana della ISO 31000: 2009

Franco Ferrari del DNV Italia mi segnala che in novembre 2010 è stata pubblicata la versione italiana della ISO 31000:2009 "Risk management — Principles and guidelines".

E' quindi disponibile presso la UNI la UNI ISO 31000:2010 "Gestione del rischio - Principi e linee guida"

****

12- Standardizzazione - Versione italiana della ISO/IEC 17021:2011

Franco Ferrari mi segnala che a marzo 2011 è stata emessa la traduzione italiana della ISO/IEC 17021:2011 "Conformity assessment — Requirements for bodies providing audit and certification of management systems".

E' quindi disponibile la UNI CEI EN ISO/IEC 17021:2011 "Valutazione della conformità - Requisiti per gli organismi che forniscono audit e certificazione di sistemi di gestione".

Ricordo che questa norma è applicabile ai soli organismi di certificazione, sulla base della quale sono accreditati da orgnismi quali Accredia, UKAS, eccetera.

****

13- Certificazioni - Transizione da ISO/IEC 20000-1:2005 a ISO/IEC 20000-1:2011

Dal webinar di APMG "ISO/IEC 20000 - Part 1 Update Explained" del 3 agosto 2011, fornisco risposte a domande che mi sono state poste in questi mesi.

E' bene far notare che le risposte riguardano lo schema di APMG, dovremo vedere se saranno valide anche per le certificazioni gestite da altri organismi (Accredia, UKAS, etc):
- non sono previsti corsi di aggiornamento per Auditor e Lead Auditor (che dovranno comunque studiarsi autonomamanete la nuova norma)
- le certificazioni dal 1 giugno 2013 potranno essere condotti audit solo sulla ISO/IEC 20000-1:2011 (i nuovi certificati dovranno essere basati sulla nuova norma se emessi dopo il 1 giugno 2012)
- l'aggiornamento della ISO/IEC 20000-2 dovrebbe essere pubblicato a inizio 2012

La presentazione del webinar la trovate al link
http://www.apmg-international.com/nmsruntime/saveasdialog.asp?lID=4891&sID=4752

****

14- Certificazioni - APMG Ente di Accreditamento per la ISO/IEC 20000-1 (seconda puntata)

Il 27 maggio avevo pubblicato la notizia "APMG Ente di Accreditamento per la ISO/IEC 20000-1":
http://blog.cesaregallotti.it/2011/05/apmg-ente-di-accreditamento-per-la.html

Con il seguente commento: "Sarà interessante capire come saranno gestite le relazioni tra certificati aziendali accreditati APMG e quelli accreditati da altri organismi di certificazione quali Accredia (ex Sincert)".

Tony Coletta, al webinar di APMG "ISO/IEC 20000 - Part 1 Update Explained" del 3 agosto 2011 ha posto questa domanda, soprattutto facendo riferimento alla EC Regulation 765/08 che impone a ciascun stato della UE di avere un unico ente di accreditamento riconosciuto dagli altri stati membri attraverso gli accordi EA MLA (e, pertanto, non ci dovrebbe essere spazio per un ente quale APMG).

APMG ha risposto così (riassumo): "Un ente di accreditamento come UKAS in UK non è coinvolto nelle attività di itSMF e operano il proprio schema di certificazione ISO/IEC 20000 con 3 organismi accreditati, mentre APMG ne ha 50. Altro punto da considerare è che ci sono diversi schemi di certificazione accreditati (con la "a" minuscola) anche al di fuori degli accordi EA MLA, ma comunque riconosciuti dal mercato. E' intenzione di APMG lavorare a stretto contatto con gli organismi di Accreditamento nazionali per garantire l'efficacia dello schema".

Forse ho riassunto male e forse ho tradotto male, ma mi sembra che al momento la situazione sia ancora lacunosa.

Ad ogni modo, potete leggere la presentazione del webinar:
http://www.apmg-international.com/nmsruntime/saveasdialog.asp?lID=4891&sID=4752
e le risposte alle domande (tra cui quella di Tony Coletta):
http://www.apmg-international.com/nmsruntime/saveasdialog.asp?lID=4892&sID=4752

Alcuni punti sullo schema di certificazione su cui ho ricevuto domande nei mesi scorsi, nel post successivo.

****

15- Minacce e attacchi

In molti mi chiedono dove trovare una lista di attacchi per iniziare a fare un'analisi del rischio.

Da Crypto-Gram del 15 agosto, segnalo questo documento della Canergy Mellon University che può essere un ottimo inizio:
http://www.cert.org/archive/pdf/10tn028.pdf

Per chi volesse andare più in profondità, dai commenti a Crypto-Gram, segnalo il VERIS Framework:
https://verisframework.wiki.zoho.com/

Qui l'elenco è molto più dettagliato e forse di difficile utilizzo per un risk assessment generale. La web application messa a disposizione può essere di ulteriore aiuto: https://www2.icsalabs.com/veris/. Per chi volesse leggere un documento vero e proprio, segnalo il "Verizon Data Breach Investigations Report" con riportate anche le statistiche pertinenti (sempre da prendere con cautela).

****

16- ROSI v2

Il 16 maggio del 2010 avevo segnalato lo studio sul ROSI condotto da AIEA, CLUSIT, Deloitte, Ernst & Young, KPMG, Oracle, PricewaterhouseCoopers.

Ora ne è uscita la versione 2, liberamente scaricabile da http://rosi.clusit.it.

Ci sono alcuni spunti interessanti e la lettura è consigliata. Tra l'altro, avevo già segnalato che lo studio prende correttamente atto dell'impossibilità di calcolare il ritorno degli investimenti di sicurezza (dico io: se sono impossibili le analisi del rischio quantitative, sarà ovviamente impossibile valutare in modo esatto la bontà degli investimenti di sicurezza) e propone un approccio degno di attenzione.

****

17- I 20 controlli di sicurezza critici

Il SANS ha pubblicato la terza versione del suo elenco dei 20 controlli di sicurezza più importanti.
https://www.sans.org/critical-security-controls/

Il documento in pdf è di 76 pagine. Mi sembra interessante come sono descritte le modalità di implementazione, distinte in: quick wins, attività di monitoraggio, attività di riduzione delle vulnerabilità e controlli avanzati. Il tutto è preceduto da un rationale.

****

18- Sesso, bugie e ricerche sul cybercrime

Da sempre diffido delle ricerche e dei dati sugli attacchi informatici. E, conseguentemente, da sempre penso che le analisi di rischio quantitative siano impossibili da fare.

C'è chi ha raccolto le prove (come segnalato da Cryptogram di luglio):
http://research.microsoft.com/pubs/149886/SexLiesandCybercrimeSurveys.pdf

****

19- Tor Day

Il 28 giugno, alla Statale di Milano, si è tenuto un incontro con Giovanni Ziccardi, Pierluigi Perri, Andrea Trentini e Jan Reister, tutti dell'Università di Milano, dal titolo "TOR day".

Il TOR è un progetto per l'anonimità on line. Nella sua pagina web (https://www.torproject.org/) è possibile scaricare un browser Firefox con una configurazione specifica e altri software.

Altri miei appunti:
- i siti web per default spesso utilizzano pagine http, anche se sono disponibili quelle https. Il plug-in di Firefox HTTPS Everywhere permette invece di richiedere le pagine https di default
https://www.eff.org/https-everywhere
- per scaricare i video di youtube con TOR o da luoghi dove youtube è censurato: http://pwnyoutube.com o http://deturl.com/
- per creare utenti anonimi, con la possibilità di ricevere files in modo anonimo e per permettere ai mittenti di essere altrettanto anonimi (se usano, ovviamente, TOR): https://privacybox.de/
- via TOR sono poi disponibili diversi "hidden services" (non sempre eticamente accettabili). Per questo, si segnala la pagina http://tor2web.org