****
IT SERVICE MANAGEMENT NEWS - MAGGIO 2012
****

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

****
01- Standardizzazione: Lavori sulla futura ISO/IEC 27001 e 27006

Come già detto in altro articolo, ho partecipato all'incontro del WG1 dell'SC27 della ISO del 7-11 a Stoccolma per scrivere la futura ISO/IEC 27001.

Tralascio il resoconto su come si è svolta la riunione e procedo a dare notizie sui punti tecnici più rilevanti.

Alcuni punti relativi alla futura ISO/IEC 27001.

- Uso del Common Text for Management Systems: la ISO ha emesso la ISO Guide 83, in cui sono specificate le regole per la scrittura degli standard sui sistemi di gestione (inclusa la 27001) e l'SC 27 ha confermato che la userà con alcune modifiche; in effetti, il testo proposto dalla ISO Guide 83 presenta alcuni punti che sono difficili da unire con la 27001 (presenta anche alcuni errori nell'inglese, per la verità).
- Risk Assessment: uno dei problemi della ISO Guide 83 è che richiede una gestione dei rischi dell'organizzazione (la troveremo quindi anche nella ISO 9001), che presenta difficoltà di unione con il risk assessment per la sicurezza delle informazioni; molto dibattito si è fatto sulla distinzione tra "risk assessment per il sistema di gestione" e "risk assessment per la sicurezza delle informazioni"; per me, l'Italia e altri Paesi non ci dovrebbe essere distinzione, per altri sì; alla fine ha prevalso la prima posizione
- Risk Assessment 2: nella bozza iniziale i requisiti sul R.A. erano veramente ridotti, ora sembra che si sia arrivati ad una giusta via di mezzo tra quello troppo prescrittivo della ISO/IEC 27001:2005 e quello troppo vago della bozza iniziale
- Riferimenti ad altri documenti: saranno tolti i riferimenti ad altri documenti e sarà fatta un'operazione simile alla ISO 9001, in cui i riferimenti ad altri standard saranno limitati ad una specifica sezione

- Uso dello Statement of Applicability: è stato deciso di continuare a richiedere lo Statement of Applicability con riferimento all'Annex A
- è stato chiarito che non si richiederanno misurazioni di efficacia di tutti i controlli, ma si richiederà di individuare per quali misurare e misurare
- è stato chiarito che il piano di trattamento del rischio deve riportare tutti i rischi, anche quelli per cui non è richiesta nessuna azione (meglio: per cui l'azione è la accettazione).

Purtroppo, non ho avuto l'occasione di assistere alla discussione sulla ISO/IEC 27002.

Ho anche avuto l'occasione di discutere di ISO/IEC 27006. Da questo punto di vista non ci saranno grosse novità, se non la necessità di allinearla alla attuale ISO/IEC 17021. Il punto più "caldo" riguarda l'Annex C, ossia la tabella con le giornate uomo da prevedere per gli audit. L'Italia ha espresso l'opinione che la tabella ha valori troppo elevati (cioè, richiede troppe giornate di audit) e ha fatto una prima proposta di eliminazione.
Attualmente si è deciso di mantenere l'Annex C ed è stato richiesto all'Italia di presentare una tabella alternativa.

Altre norme sono state discusse, ma la delegazione italiana (vedere altro articolo) era troppo ridotta per poterne seguire i lavori.

****

02- Standardizzazione: Chi partecipa ai comitati ISO (Lamentazione)

Dal 7 al 15 maggio 2012 si è tenuto l'incontro dell'SC 27 a Stoccolma per scrivere, tra le altre, le future ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27006 (requisiti per gli organismi di certificazione), norme sulla computer forensics, norme sulla certificazione di prodotti (queste ultime, in Italia, anche richiamate in alcuni dispositivi di legge o norme).

In tutto, la delegazione italiana era composta da 3 persone: me stesso (ho seguito le attività su 27001, 27002 e 27006), Stefano Ramacciotti (Ce.Va. Difesa, che si è occupato dei criteri di valutazione della sicurezza, che generalmente hanno a che fare con la valutazione dei prodotti ai fini della loro certificazione, dei sistemi, dell'implementazione di algoritmi crittografici e di processi di "security engineering") e Fabio Guasconi (di @mediaservice.net, ha seguito il comitato principale in qualità di Capo delegazione). Aggiungo anche Dario Forte che però ha partecipato solo per poche ore via Skype sulle norme di computer forensics. C'era un altro italiano, in rappresentanza della Commissione Europea, Pasquale Stirparo (JRC di Ispra e DFA, che ha seguite le norme sulla forensics).

Alcuni dettagli li ho dati in un altro articolo e spero di riceve contributi dagli altri.

Perché "Lamentazione"? Perché 3 sono troppo poche persone. Il problema è che per partecipare a queste iniziative bisogna pagarsi il viaggio e l'hotel. Ma mi sorprende che dall'Italia non c'era:

- nessuno da Organismi di Certificazione accreditati per la ISO/IEC 27001 (si capisce: o era a Stoccolma o era a fare audit fatturabili; la scelta è facile da capire, non da giustificare)
- nessuno da Accredia (quelli che controllano gli Organismi di Certificazione ISO/IEC 27001, apparentenemente e inspiegabilmente non interessati ad una norma come la 27006; ma in ottima compagnia nel loro disinteresse, visto che a parlare di 27006 eravamo 3 auditor di OdC e 2 rappresentanti degli organismi di accreditamento),
- nessuno delle società di consulenza (anche loro hanno il problema di pagare le spese e non fatturare 7-8 giornate, però si presentano lo stesso sul mercato come "espertissimi" e applicano tariffe coerenti; facciamo eccezione Fabio e io... e io non riesco ad applicare le tariffe che vorrei! (non so nulla di Fabio)),
- nessuno dalla Pubblica Amministrazione o Autorità collegate (anche se poi emettono schemi "conformi" alla 27001, o chiedono la certificazione 27001 nei contratti; forse su suggerimento dei consulenti di cui sopra; solo i francesi e tedeschi avevano referenti dei loro Garanti Privacy), con l'eccezione del Ce.Va. Difesa
- nessuno dalle nostre imprese più rappresentative (anche se dicono di applicare la 27001 o norme collegate e chiedono di avere fornitori certificati)
- nessuno dalle forze dell'ordine (che pur fanno computer forensics)

- nessuno dai laboratori di valutazione della sicurezza dei prodotti informatici (ad eccezione di Stefano Ramacciotti)

Le ragioni sono sicuramente tante e non credo che sia interessante un ulteriore approfondimento in questa sede. Ma non riesco a capire perché non sia ritenuto né utile né interessante un investimento di spesa sulla 27001 variabile dai 4 ai 10mila Euro annui (ci sono 2 incontri all'anno, in posti anche lontani) da TUTTE le aziende italiane che si vantano di fare sicurezza delle informazioni (con la dovuta eccezione di @mediaservice).

(Rimane sempre il problema che per scrivere le norme devo pagare per iscrivermi a UNINFO e per il viaggio e poi per leggere la versione definitiva devo pagare per averla).

PS: ringrazio Stefano Ramacciotti per avermi segnalato refusi e imprecisioni e futuri potenziali articoli di approfondimento sugli ultimi due paragrafi

****

03- Articolo sul caso Wikileaks

Segnalo questo articolo di Stefano Ramacciotti dal titolo "La sicurezza delle informazioni al tempo di Wikileaks".

Il caso è ormai vecchio e l'articolo è di inizio 2011. Però mi sembra interessante per i seguenti punti:

- pone molto bene il problema che c'è nella percezione di "sicurezza delle informazioni" e "sicurezza informatica"
- introduce molto bene i paradigmi di need-to-know e need-to-share
- parla della "Sindrome di Fort Apache" che non conoscevo; è "quell'atteggiamento secondo il quale si pensa che i "cattivi" stiano tutti fuori, e dentro il forte ci siano solo i buoni"; per saperne di più dovrei leggere il libro di Giustozzi, ma già il nome è interessante
- propone alcune misure di sicurezza che non sono normalmente trattate nell'ambito civile e che potrebbero essere mutuate intelligentemente dall'ambito militare
- segnala un attacco ovvio, ma di cui non sapevo il nome ("Pod slurping") e a cui raramente si pensa

L'articolo:
- http://www.difesa.it/Pubblicistica/info-difesa/Infodifesa140/2011/Documents/Rivista%203-2011/3_Articolo3.pdf

****

04- Approccio al change management

Segnalo questo interessante articolo sul change management postato su ITSM Portal.

L'autore è Glen Taylor, dirigente IT della Walt Disney Parks & Resorts (sempre che non si tratti di un furto di identità).

Glen Taylor dice che un processo di approvazione e gestione dei change troppo rigido è un errore. In modo simile, afferma che il classico processo "andiamo avanti senza regole" è altrettanto sbagliato.

Il processo giusto dovrebbe considerare il livello di rischio di ciascun change e richiedere il corrispondente livello di documentazi e attività. Ovviamente, il livello di rischio non potrà essere calcolato solo con "dati, regole e punteggi", ma con "informazioni, linee guida, esperienza" e, soprattutto, non deve essere fatto in un modo qualunque "tanto per soddisfare un requisito".

Il passaggio però al change management basato sul rischio deve passare inesorabilmente per il change management basato sulle regole, in caso contrario non è possibile costruire le linee guida e le esperienze necessarie.

L'articolo:
- http://www.itsmportal.com/news/why-%E2%80%9Crules-based%E2%80%9D-approach-change-management-always-fails

****
05- Privacy: Cloud & Mobile

Alessandro Vallega di Oracle mi segnala un lavoro fatto a più a mani e in ambito Clusit sulla privacy sul cloud e in ambito mobile (cellulari, smartphone, tavolette, BYOD, eccetera). In entrambi i documenti si assume il punto di vista di un'azienda italiana titolare dei trattamenti relativi a dati personali.

Gli argomenti sono ormai noti, ma la lettura è comunque interessante per chi non avesse avuto ancora la possibilità di affrontare questi argomenti. Per chi invece li dovesse già conoscere, se ha un po' di pazienza potrebbe trovare alcuni spunti originali.

Ecco il link:
- https://privacycloudmobile.clusit.it/

****
06- Privacy: Controllo dei conti correnti

Riporto tale e quale la segnalazione di Daniela Quetti della DFA e di Lispa.

Il 18 aprile è comparsa sul sito del Garante la seguente notizia: "Fisco: sí del Garante agli schemi di provvedimento dell'Agenzia delle entrate sui conti correnti dei cittadini e sulla partecipazione dei Comuni alla lotta all'evasione fiscale. Necessaria una rigorosa protezione dei dati".

Il Garante ha richiesto, tra le misure di sicurezza, la cifratura di tutti i passaggi interni (interessante pensare che a livello di dato sanitario, per il dato non genetico, questo non sia richiesto).

http://www.garanteprivacy.it/garante/doc.jsp?ID=1886812

****

07- Privacy: Videosorveglianza, eliminati alcuni vincoli per l'autorizzazione

Copio e incollo (con qualche modifica) quanto riportato alla pagina
http://www.consulentidellavoro.it/browse.php?mod=article&opt=view&id=10522

Il Ministero del lavoro è intervenuto con la nota n. 7162 del 16 aprile 2012 per semplificare l'installazione dei sistemi di controllo a distanza, soprattutto in quegli esercizi commerciali (ricevitorie, tabaccherie, oreficerie, farmacie, edicole, distributori di carburante) dove non ci sono rappresentanze sindacali.

Finora la procedura di istallazione richiedeva che personale ispettivo, prima di procedere al rilascio dell'autorizzazione, procedesse con un accertamento tecnico dello stato dei luoghi (planimetria dei locali, numero impianti da installare ecc..).

Il Ministero ha riconosciuto sufficiente la richiesta espressa del datore di lavoro e, per il rilascio dell'autorizzazione, sarà sufficiente la sola documentazione tecnica prodotta.

Ringrazio Max Cottafavi di Reply per la segnalazione.

****

08- Privacy: Responsabilità dell'acquirente di liste di contatti

Il Garante della Privacy, il 5 aprile, ha emesso un Provvedimento su "responsabilità dell'acquirente di liste di contatti":
- http://www.garanteprivacy.it/garante/doc.jsp?ID=1891156

Il Provvedimento è molto lungo e di difficile lettura. Questo articolo riassuntivo è più semplice:
http://www.filodiritto.com/index.php?azione=archivionews&idnotizia=3739

Considerazione 1: nella lunga premessa si evince quanto vado a dire da tempo (e non sono un legale), ossia che non è sempre corretto nominare le altre aziende come "Responsabili esterni". In questo Provvedimento è chiaro come le diverse aziende coinvolte si siano nominate reciprocamente "Responsabili" seguendo l'interpretazione più diffusa, senza considerare gli impatti e gli obblighi reciproci derivanti.

Considerazione 2: la lamentela è stata sollevata da una persona iscritta al Registro delle Opposizioni, ma poi questo particolare viene dimenticato nel corso del Provvedimento.

Considerazione 3: credo che il discorso si faccia ora complesso per coloro che vogliono utilizzare elenchi non pubblici di nominativi per fare telemarketing, visto che "chi acquisisce la banca dati deve accertare che ciascun interessato abbia validamente acconsentito all'invio di materiale pubblicitario". Come può farlo se le garanzie contrattuali, così come richiamate dal Provvedomento, non sono ritenute sufficienti?