****
IT SERVICE MANAGEMENT NEWS - NOVEMBRE 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

****
01- Normativa: Segreto di Stato

Sulla Gazzetta Ufficiale n. 203 del 1 settembre 2011 è stato pubblicato il DPCM 22 luglio 2011 n.4 "Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate".

Il DPCM è molto focalizzato nella descrizione delle misure di sicurezza fisica. Sulle misure di sicurezza informatica, mi pare sia molto limitato.

Ad ogni modo, il tema merita di essere conosciuto anche da chi non si occupa di sicurezza delle informazioni in ambito militare o del Segreto di Stato. La mia personale biografia è la seguente:
- Legge 124 del 2007 sulla disciplina del Segreto di Stato
- DPCM 7 del 12 giugno 2009 "Determinazione dell'ambito dei singoli livelli di segretezza, dei soggetti con potere di classifica, dei criteri d'individuazione delle materie oggetto di classifica nonché dei modi di accesso nei luoghi militari o definiti di interesse per la sicurezza della Repubblica" (questo è anche sulla classificazione delle informazioni)
- DPCM 4 del 22 luglio 2011 "Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate" (cioè, disposizioni sulle misure di sicurezza)
- Legge 241 del 1990 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi"
- DPR 184 del 2006 "Regolamento recante disciplina in materia di accesso ai documenti amministrativi."
- DPCM 11 aprile 2002 sulla certificazione dei prodotti e sistemi IT coinvolti nel Segreto di Stato

Segnalo quindi la pagina del Comitato parlamentare per la sicurezza della Repubblica che riporta alcune di queste normative:
http://www.parlamento.it/bicamerali/43775/43777/43783/44440/88129/sommario.htm

Infine, segnalo questa pagina della Presidenza del Consiglio dei Ministri:
http://www.sicurezzanazionale.gov.it/web.nsf/pagine/segreto_di_stato

****

02- Normativa: DPS Addio?

Attilio Rampazzo di segnala un articolo su Italia Oggi sulle ulteriori semplificazioni alla normativa privacy.
http://www.italiaoggi.it/news/dettaglio_news.asp?id=20111021120400758 8&chkAgenzie=ITALIAOGGI&sez=newsPP&titolo=Privacy,%20Dps%20addio

Attilio si chiede: "A questo punto, anche se è una nuova proposta per superare la crisi, invece di tutte queste semplificazioni ovvero mutilazioni, non è meglio a questo punto abrogare tutta la legge visto che,se sarà vero, non rimane quasi più nulla di tutela dei dati personali?"

Convengo che la cosa mi inquieta.

Un pochino per quei pochi euro che mi portava "l'aggiornamento del DPS", ma tanto per la mia sensibilità in materia di sicurezza.

Purtroppo, alcune pessime disposizioni dell'Allegato B (ereditate dal 318/1999, e ampliate da amenità quali la "data certa" e altri Provvedimenti del Garante) e un nugolo di cani affamati di soldi (i consulenti), hanno reso l'esercizio del DPS molto oneroso e incomprensibile, ridotto alla produzione di plichi di centinaia di pagine anche in piccole realtà (li ho visti! lo giuro!).

Se a questo aggiungiamo che il Governo attualmente in carica non è molto sensibile alla materia (vedere Registro delle Opposizioni, che inverte il precedente principio di opt-in nel principio di opt-out), il gioco è fatto.

Non ci rimane che guardare cosa succede: una nostra manifestazione sotto il Parlamento richiamerebbe al massimo una decina di persone ;-)

****

03- Glossario ITIL 2011

Sul sito ufficiale di ITIL è stato pubblicato il glossario 2011, anche in italiano (può anche far riflettere il fatto che ci sia un glossario spagnolo per la Spagna e uno spagnolo per l'America Latina).

E' noto che non tutte le definizioni di ITIL sono condivisibili (pensate a quella di known error, per cui non basta avere il workaround, ma anche la causa documentata, mentre nella realtà si hanno spesso workaround senza causa documentata e sono comunque denominati known error) e alcuni termini rimangono confinati a ITIL e non usati nella maggioranza dei casi ("operation bridge" su tutti).

E' anche noto che alcune traduzioni in italiano dei termini informatici possono sembrare forzate.

Però, in questo glossario ci sono anche cose interessanti e che meritano di essere capite e utilizzate.

La pagina dei glossari: http://www.itil-officialsite.com/InternationalActivities/ITILGlossaries_2.aspx

****

04- Standardizzazione: Pubblicata la ISO/IEC TR 27008 - Tecniche di audit

Attilio Rampazzo mi informa della pubblicazione, il 6 ottobre 2011, della ISO/IEC TR 27008:2011 - Information technology -- Security techniques -- Guidelines for auditors on information security controls.

E' una linea guida, quindi non è necessario seguirla. Come tutte le norme di questo tipo, ci sono cose interessante e altre risapute.

****

05- Tecnologia: iOS 5

La Apple ha pubblicato la nuova versione dell'iOS per iPhone, iPod e iPad. Oltre al servizio di iCloud, la nuova versione corregge alcune vulnerabilità.

Perché do io questo annuncio, visto che normalmente non tratto questi argomenti? Per denunciare, nel mio piccolo, il fatto che questa nuova versione, con correzione di vulnerabilità, è disponibile per iPhone 3GS e superiori. Per chi ha comprato un iPhone 3G (solo 3 anni fa, non molti), nulla!

E' ovvio, scrivo perché sono persona interessata al problema (ho un iPhone 3G), ma trovo scorretta questa politica di non fornire più alcun supporto giusto giusto 2 anni dopo l'uscita di una nuova versione dell'hardware (il 3GS è uscito nel giugno 2009), quando la garanzia non è più valida. E poi ci lamentiamo della Microsoft!

****

06- Tecnologia: Attacco a SSL/TLS

Un interessante articolo da "Minded Security Early Warning" segnala il nuovo attacco al protocollo SSL/TLS 1.0 che permette di intercettare le comunicazioni.

Gli sviluppatori dovrebbero passare alle versioni successive.

Segnalo questi link in materia:
- http://www.mindedsecurity.com/fileshare/early_warning/Early_Warning_Ott11.pdf
- http://www.theinquirer.net/inquirer/news/2110508/ssl-tls-attack-secure-communications-risk
- http://vnhacker.blogspot.com/2011/09/beast.html

****

07- Tecnologia: Incidente al Blackberry

Il 10 ottobre, i servizi Blackberry hanno subito un crash con conseguente indisponibilità di 3-4 giorni.

Clienti arrabbiati, investitori infastiditi e altre amenità di questo genere:
- http://www.bbc.co.uk/news/technology-15287072
- http://money.cnn.com/2011/10/13/technology/blackberry_outage/index.htm

La Blackberry ha detto che condurrà una "root cause analysis" su un "problema hardware". Spero che non diventi una "caccia al colpevole per punire un innocente", ma sia una roba seria (mi chiedo quale possa essere stato il guasto che ha colpito un'infrastruttura forse in non-così-alta-affidabilità).

Detto questo, l'incidente ci deve ricordare che l'e-mail (come la posta tradizionale, come gli SMS) è basata su un protocollo "inaffidabile". Se volete essere certi che il destinatario riceva una vostra comunicazione, dovete telefonargli!

****

08- Voucher per la valutazione dei rischi informatici

La Regione Lombardia e le Camere di Commercio di alcune Province, in accordo con Assintel, intendono finanziare tramite l'utilizzo di voucher a fondo perduto, nominativi e non trasferibili, l'acquisto di un servizio tecnico di valutazione dei rischi informatici.
http://www.assintel.it/eventi/810.jsp

La notizia mi è stata segnalata da Simone Tomirotti e potrebbe essere interessante capirne i dettagli. Soprattutto le procedure tecniche che saranno seguite. Sui siti web relativi, non ho trovato nulla in merito. Si accettano ulteriori informazioni.

****

09- Dilbert sugli standard

Da Crypto-Gram del 15 ottobre 2011, segnalo questa vignetta di Dilbert:
http://dilbert.com/fast/2011-08-02/

In inglese. Ma mi ha ricordato cose italiane...

****

10- Mia presentazione ISO/IEC 27001

Il 10 novembre ho tenuto un intervento per la DFA sulla "Famiglia delle norme ISO/IEC 270xx".

E' pubblicato su www.cesaregallotti.it/Pubblicazioni.html