Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS - NOVEMBRE 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

****
01- Legale: Privacy e 231 - Tutto annullato (ed errata corrige)

Nella newsletter del 16 di ottobre avevo riportato alcuni approfondimenti sul possibile inserimento dei delitti privacy nel Dlgs 231 del 2001. Ma non avevo verificato se quella notizia era ancora di attualità e ovviamente NON lo era: il Decreto Legge 93/2013 è stato convertito in Legge con modificazioni (Legge 119/2013) e i delitti privacy non saranno inclusi nel Dlgs 231.

Mi scuso con tutti i miei lettori. Posso giustificarmi dicendo che la Legge è datata 15 ottobre, ma la decisione era stata presa almeno settimane prima.

La prima ad avvisarmi è stata Paola Generali di GetSolution, seguita da Fabio Guasconi (mio Presidente all'SC 27) e da Massimo Cottafavi di Spike Reply.

Però, gli approfondimenti, anche se non di attualità, mi hanno permesso di capire la differenza tra "reati" e "delitti" e tra "sanzioni" e "contravvenzioni". Infine, Stefano Ramacciotti mi ha ricordato che la pena di morte è stata abolita da anni.

****

02- Pubblicata VERA 4.0

Ho pubblicato una nuova versione del mio Very Easy Risk Assessment, con i controlli della ISO/IEC 27001:2013, in versione bilingue e con qualche nuovo refuso. Ogni aiuto sarà il benvenuto!

Il link alla pagina da dove scaricare VERA:
- http://www.cesaregallotti.it/Pubblicazioni.html

****

03- Standardizzazione: Stato delle norme ISO/IEC 270xx (I lavori del ISO/IEC JTC1 SC27 WG1)

Venerdì 25 ottobre si è concluso a Songdo (Corea del Sud) il 47mo meeting dell'SC 27 dell'ISO/IEC JTC 1. Hanno partecipato circa 250 delegati, di cui 70 per il WG1 (ossia il gruppo che si occupa delle norme della famiglia ISO/IEC 27000 e collegate alla ISO/IEC 27001).

La delegazione italiana era composta da 4 persone: io per il WG 1, Stefano Ramacciotti per il WG 3, Dario Forte per il WG 4 e Andrea Caccia per i WG 1 e 4 e come rappresentante per ETSI.

Di seguito, le decisioni in merito alle norme del WG 1 affrontate in questo meeting.

ISO/IEC 27000 (Overview and vocabulary)
La norma sarà pubblicata a breve nell'edizione 2013. Si è discusso su come affrontare la prossima versione. Infatti, ciascun termine è "di proprietà" di uno standard e può essere ridefinito solo contestualmente all'elaborazione di quello standard. Purtroppo, questo ha ridotto l'impegno sui termini e definizioni, con risultati anche insoddisfacenti (per esempio, la definizione di "evento di sicurezza delle informazioni", non è collegata alla definizione di "evento"). Si farà sicuramente di meglio nel futuro.

ISO/IEC 27001 e 27002
Sarà pubblicato e reso disponibile gratuitamente il documento WG1 SD3 "Mapping Old to New Editions of ISO/IEC 27001 and ISO/IEC 27002". Ne parleremo poco oltre.

ISO/IEC 27003 (Guida all'attuazione di un ISMS)
Si è deciso di cambiarla totalmente e cambiarle il titolo (da "Implementation guidance" a "Guidance"). Diventerà una guida alla ISO/IEC 27001 e sarà suddivisa negli stessi capitoli della ISO/IEC 27001.

ISO/IEC 27004 (Misurazioni)
Tutti i partecipanti hanno concordato per un approccio non teorico. Sarà proposto un modello al prossimo meeting di aprile: bisognerà vedere come sarà e se presenterà un insieme minimo di indicatori. Si è anche deciso di scrivere un testo che non possa essere utilizzato come check list da auditor e utilizzatori, ma che sia veramente una linea guida. Cambierà titolo da "Measurements" a "Monitoring, measurement, analysis and evaluation".

ISO/IEC 27005 (Risk management)
Si è deciso di non limitare il testo ai soli risk assessment e risk treatment, ma di trattare di risk management, esattamente come nella versione attuale. Alcuni volevano ridurre lo scopo di questa norma per evitare sovrapposizioni con la 27001 e la 27003. La maggioranza ha voluto però evitare di pubblicare un testo troppo sintetico e forse incomprensibile alla maggioranza dei lettori (come, a mio parere, si è fatto per la 27001).

ISO/IEC 27006 (Requisiti per gli organismi di certificazione)
Si è discusso se mantenere la tabella di riferimento per le giornate di audit basata sulle persone impiegate nell'ISMS, oppure se seguire un'altra strada. Malgrado né in questo meeting né nel precedente siano state individuate strade alternative, metà dei delegati ha votato per questa seconda opzione; vedremo cosa succederà al prossimo meeting. Si è anche deciso di riportare la versione del SoA sui "documenti di certificazione" e non sul certificato, contrariamente a quanto previsto dalla versione della 27006 attualmente in vigore.

ISO/IEC 27016 (Organizational economics)
Sarà pubblicata a breve.

Process reference model e Process assessment model
Di questo ne parlai già in precedenza (http://blog.cesaregallotti.it/2013/09/spice-modelli-di-maturita-e-isoiec-27001.html). Le proposte sono state sostanzialmente bocciate. Attualmente queste due proposte di standard sono di competenza del SC 7, ma si è chiesto di assegnarle al SC 27.

Si è anche discusso di ISO/IEC 27009 (cambierà titolo il "Sector specific application of ISO/IEC 27001 – Requirements), 27011 (requisiti per telecomunicazioni), 27013 (rapporti tra 27001 e 20000-1) e 27017 (cloud), senza notizie da segnalare.

ISMS professionals
Si sta studiando da tempo una norma sulle certificazioni delle competenze dei professionisti degli ISMS. Si è deciso di creare uno schema a cui dovranno adeguarsi gli organismi di certificazione del personale.

****

04- Standardizzazione: i lavori del ISO/IEC JTC1 SC27 WG3

Stefano Ramacciotti mi ha inviato un aggiornamento sui lavori del WG3 del Sub Commitee 27 di ISO/IEC JTC1.

Esso si occupa dello sviluppo di Security Evaluation Assurance criteria, ovvero dei criteri di valutazione dei sistemi informatici (compresi quelli crypto) per mezzo dei quali verificare la fiducia, in termini di sicurezza, che può essere accordata ai prodotti in esame.

Tra i principali standard vi sono i Common Criteria (standard ISO/IEC 15408), con la relativa metodologia (ISO/IEC 18045), gli standard a essi collegati (come l'ISO/IEC 15292 sulle procedure di registrazione dei Protection profile e l'ISO/IEC TR 15446, per le linee guida relative alla costruzione di Protection Profiles (PP) e Security Targets (ST)), più altri standard come l'ISO/IEC 19790 Security requirements for cryptographic modules che rappresenta l'edizione internazionale dello standard americano-canadese FIPS 140-2.

Nel corso della conferenza svoltasi a Incheon (Corea del Sud) dal 21 al 25 ottobre, si è parlato soprattutto di:
- ISO/IEC 15408-1:2009 "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model": ne è stata chiesta la pubblicazione.
- ISO/IEC 17825 "Testing methods for the mitigation of non-invasive attack classes against cryptographic modules": è stata chiesta la votazione per il passaggio a CD.
- ISO/IEC 18045:2008 "Information technology - Security techniques - Methodology for IT security evaluation": è stata chiesta la pubblicazione.
- ISO/IEC TR 19791:2010 "Information technology - Security techniques - Security assessment of operational systems": dovrà essere preparato il primo Working Draft entro fine anno.
- ISO/IEC TR 20004 "Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045": rimodulata in modo da diventare la prima parte della futura ISO/IEC 20004 e la 30127 "Detailing software penetration testing under ISO/IEC 15408 and ISO/IEC 18045 vulnerability analysis" ne è divenuta la seconda parte;
- ISO/IEC 24759:2008 "Information technology -- Security techniques -- Test requirements for cryptographic modules": è stata chiesta la votazione per il passaggio a CD.
- "Study Period on High-assurance evaluation under ISO/IEC 15408/18045": prolungato il periodo di studio.
- "Joint ISO/IEC JTC 1/SC 27/WG 3 and ISO/IEC JTC 1/SC 27/WG 5 Study Period on security evaluation of anti spoofing techniques for biometrics": prolungato il periodo di studio.
- SC 27 N13022 "Competence requirements for security evaluators, testers, and validators": stabilito un periodo di studio.
- SC 27 N13026 "Guidance for developing security and privacy functional requirements based on ISO/IEC 15408": richiesto un New Work Item Proposal.

****

05- Standardizzazione: Corrispondenze tra ISO/IEC 27001:2005 e ISO/IEC 27001:2013

Alla seguente pagina è pubblicato il documento ufficiale dell'SC 27 "Mapping Old-New Editions of ISO/IEC 27001 and ISO/IEC 27002":
- http://www.jtc1sc27.din.de/sbe/wg1sd3

Ovviamente, questo documento non permetterà di escludere uno studio attento della nuova ISO/IEC 27001:2013. Come ho già ricordato più volte, molti requisiti presenti in precedenza sono ora impliciti e alcuni collegamenti sono meno evidenti, ma ci sono (per esempio, nel riesame di direzione non viene più richiesto di determinare il fabbisogno di risorse per l'ISMS, ma tale fabbisogno deve essere espresso quando si stabiliscono gli obiettivi).

Inoltre, non condivido la dicitura "deleted" per alcuni controlli della ISO/IEC 27002: se così fosse, vorrebbe dire che non erano utili per la sicurezza delle informazioni. In realtà, tutti i controlli "deleted" sono stati incorporati in alcuni degli attuali 114 controlli (per esempio, il "input data validation" è ora incorporato nel 14.1.1 Information security requirements analysis and specification.

****

06- Standardizzazione: Presentazione nuove norme ISO/IEC 27001 e 27002

Vi segnalo questa presentazione UNINFO sulle nuove ISO/IEC 27001 e 27002 e a cui ho contribuito:
- http://www.slideshare.net/guasconif/le-nuove-norme-della-famiglia-27000

****

07- Standardizzazione: Transizione dei certificati alla ISO/IEC 27001:2013

L'IAF, International Accreditation Forum, l'organizzazione che si occupa di dare le regole per gli organismi di accreditamento e quelli di certificazione, ha approvato la risoluzione 2013-13 che riporta le regole per la transizione delle certificazioni dalla alla ISO/IEC 27001:2005 alla ISO/IEC 27013.

La risoluzione è molto succinta e stabilisce che i certificati ISO/IEC 27001:2005 non saranno più validi dal 1 ottobre 2015. Non sono date ulteriori regole sulla formazione degli auditor o su altri aspetti. Trovo sia un peccato.

Le organizzazioni certificate dovranno comunque ricevere nei prossimi mesi una comunicazione del proprio organismo di certificazione con indicate le regole per la transizione.

****

08- Standardizzazione: UNI 11506:2013 - Figure professionali ICT

Franco Ferrari del DNV Italia e Giovanni Ghidoni mi hanno segnalato la pubblicazione della norma UNI 11506:2013 dal titolo "Attività professionali non regolamentate - Figure professionali operanti nel settore ICT - Definizione dei requisiti di conoscenza, abilità e competenze".

E' possibile leggere l'articolo di presentazione di UNI:
- http://www.uni.com/index.php?option=com_content&view=article&id=2486:la-nuova-uni-11506-definisce-la-figura-professionale-dell-informatico

Questa norma UNI si basa sul European e-Competence Framework e sui tre documenti del European e-Competence Framework 2.0 il cui sito web di riferimento è:
- http://www.ecompetences.eu/1386,Home.html

Questi 3 documenti corrispondono alle CWA 16234-1, 2 e 3 del CEN, il cui sito di riferimento è:
- http://www.cen.eu/cen/Sectors/Sectors/ISSS/CWAdownload/Pages/ICT-Skills.aspx

Confesso che non ho capito cosa offra in più la UNI 11506 e quindi come dovrebbe essere applicata. Ogni indicazione sarà benvenuta (e pubblicata, se ne sarò autorizzato).

****

09- Legale: Privacy, audit e videosorveglianza

Dalla newsletter del Garante del 31 ottobre 2013 segnalo la notizia " Sicurezza nei supermercati senza ledere la dignità dei lavoratori - Nel mirino del Garante le società della grande distribuzione con sistemi di videosorveglianza non a norma":
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2726619#2

In realtà nulla di nuovo: il Garante ha svolto delle ispezioni e ne ha fatto un resoconto.

Segnalo però la seguente frase: "Il legale rappresentante di un supermercato aveva addirittura dichiarato al nucleo ispettivo che l'impianto di videosorveglianza non era in funzione, salvo poi doversi smentire di fronte alle evidenze raccolte". Magnifico! Cercano di prendere in giro anche gli ispettori del Garante, non solo gli auditor ISO. Mi sento in buona compagnia.

****

10- Legale: Privacy e call center extra-UE

Dalla newsletter del Garante privacy, segnalo il recente Provvedimento relativo ai call center siti in Paesi extra-UE:
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2724806

Apparentemente non dice nulla di nuovo, ma in realtà la newsletter segnala le seguenti novità:
- i call center dovranno dichiarare la nazione dalla quale chiamano o rispondono;
- per le chiamate fatte da un cliente (spesso, se il call center è un help desk), dovrà essere data all'utente la possibilità di scegliere un operatore collocato sul territorio nazionale;
- dovrà essere segnalato preventivamente al Garante l'affidamento delle attività in Paesi extra-UE.

Non sono un protezionista, ma sono contento che finalmente il Garante si sia accorto di questo fenomeno e cerchi di controllarlo, anche perché era ingiusto imporre certe regole solo agli italiani.

****

11- Legale: Stato avanzamento Regolamento EU Privacy

Alberto Piamonte mi ha segnalato questo link:
- www.federprivacy.it/informazione/ultime-news-privacy/988-via-libera-al-nuovo-regolamento-ue-sulla-privacy.html

La notizia è che la Commissione Libertà civili e giustizia (LIBE) del Parlamento Ue ha dato voto positivo alla proposta di Regolamento Europeo privacy di cui ho parlato in altri post:
- http://blog.cesaregallotti.it/2013/09/articolo-sullo-stato-del-regolamento-ue.html

L'articolo di Federprivacy è decisamente entusiasta, ma rimane ancora almeno un ulteriore passaggio, ossia il negoziato a tre di Consiglio, Commissione e Parlamento europei.

Max Cottafavi di Reply mi ha invece segnalato questo link, dove si dice che l'UK sta lavorando per posporre il tutto al 2015:
- http://www.euractiv.com/specialreport-digital-single-mar/france-germany-form-anti-spy-pac-news-531306

Il Garante, nella sua newsletter del 31 ottobre, riassume le principali novità:
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2726619#3

Credo rimanga valida la regola di base: finché non sarà approvato definitivamente, eviterei di dedicare troppo tempo a questo possibile Regolamento (che già faccio troppe errata corrige...).

****

12- Notizie: Facebook e i profili segreti

Massimo Cottafavi di Reply mi ha segnalato un po' preoccupato che Facebook ha comunicato ai propri utenti che potrà condividere le loro informazioni con altri soggetti, a scopi pubblicitari e di marketing:
- http://www.lastampa.it/2013/10/14/tecnologia/addio-ai-profili-segreti-su-facebook-HdLcdF3CdeRrKjESHSiD3J/pagina.html

Sono sorpreso: pensavo lo facesse già da tempo ;-)

****

13- Legale: Le condizioni di contratto del cloud computing

Segnalo questo articolo su CINDI dal titolo "Le condizioni di contratto del cloud computing". Ovviamente molto di più si potrebbe dire sul cloud, ma trovo inquietanti i risultati dell'analisi... basati solo su 3 elementi contrattuali:
www.cindi.it/le-condizioni-di-contratto-del-cloud-computing

Visto che le linee guida suggeriscono di prevedere più di 3 elementi sul contratto, non oso immaginare se e come sono gli altri.

****

14- Legale: Diffamazione sul web

Segnalo questo interessante articolo su CINDI dal titolo "Riforma della diffamazione via web (e tramite Facebook)"
- http://www.cindi.it/diffamazione-via-web-tramite-facebook

Personalmente, non sono interessato a studiare i disegni di legge, a meno che non mi chiamino a collaborare (cosa mai successa, per la verità), perché poi cambiano continuamente (vedere Regolamento UE privacy e, in precedenza, il DPS o la privacy nella 231).

Però l'articolo descrive bene come interpretare il reato di diffamazione (diffamazione semplice, tentativo di diffamazione, circostanze attenuanti, permanenza del reato, eccetera) e le pene previste.

****

15- Minacce e attacchi: Rapporti semestrali Clusit e MELANI

Segnalo la pubblicazione dei due rapporti sulla sicurezza informatica tra i più interessanti in circolazione.

Per avere il rapporto Clusit, aggiornato al primo semestre 2013, è necessario scrivere a rapporti@clusit.it.

Quello MELANI (svizzero) si trova a questo indirizzo:
- http://www.melani.admin.ch/dienstleistungen/archiv/01558/index.html?lang=it

****

16- Minacce e attacchi: Frodi sui dispositivi mobili

Dalla newsletter del Clusit del 31 ottobre segnalo un documento dell'APWG dal titolo "Mobile Financial Fraud & The Underground Marketplace - Overview – an APWG White Paper". Si trova a questo link:
- http://apwg.org/resources/mobile

Sono riportate le tante minacce e vulnerabilità relative ai dispositivi mobili, utili per capire il fenomeno a chi non dovesse averlo ancora capito.