Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – MAGGIO 2015

****

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- Stato delle norme ISO/IEC 27000

Venerdì 8 maggio si è concluso a Kuching (Malesia) il meeting semestrale del WG1 dell'ISO/IEC JTC1 SC27 che ha, tra le altre cose, la responsabilità di redigere le norme della serie ISO/IEC 27000. A questo incontro hanno partecipato circa 127 esperti in rappresentanza di circa 27 Paesi. Oltre ai lavori del WG1, si sono svolti i lavori degli altri gruppi di lavoro dedicati agli standard di sicurezza delle informazioni e sicurezza informatica.

La delegazione italiana, per tutti i 5 gruppi di lavoro, era composta da 3 persone, incluso me e il Presidente dell'SC 27 italiano Fabio Guasconi (di Bl4ckSwan).

Passo quindi in rassegna rapidamente cosa è successo.

ISO/IEC 27001: è stata apportata una correzione marginale al testo.

ISO/IEC 27003 ("interpretazione" della ISO/IEC 27001): c'è stata una lunga discussione per avere un testo "di qualità". Io ho partecipato attivamente alle discussioni e sono emerse cose interessanti. Purtroppo, la ricerca di qualità rallenterà la pubblicazione della norma (che ora prevedo sarà a metà o fine 2016).

ISO/IEC 27004 (sulla misurazione di un sistema di gestione per la sicurezza delle informazioni): hanno cercato di rendere il testo sempre più "pratico" e meno "teorico". Come italiani siamo riusciti ad inserire molti esempi di misurazioni e a bloccare alcune idee molto belle in teoria ma irrealizzabili nella pratica.

ISO/IEC 27005 (sulla gestione del rischio): la norma avanzava molto lentamente perché si cercava di aggiornarla con troppe idee (ahinoi, spesso troppo teoriche ma non rigorose). È stato deciso di ritornare all'edizione del 2011 e apportare solo le modifiche necessarie ad allinearla alla nuova ISO/IEC 27001:2013 dove necessario. Questo comunque non velocizzerà i tempi e la nuova edizione della ISO/IEC 27005, forse, uscirà nel 2017.

ISO/IEC 27006 (regole per la certificazione ISO/IEC 27001): la discussione ha riguardato soprattutto il numero minimo di giornate di audit, osservando che la nuova tabella di riferimento per questo calcolo diventerà "normativa" e non più "informativa". Come spesso succede, interessi diversi partivano da esigenze diverse e si è cercato di raggiungere un compromesso. Le discussioni più accese sono state tra auditor, ossia tra quelli molto scrupolosi che vorrebbero avere sempre più tempo per gli audit e quelli che non ritengono necessario verificare sul campo l'attuazione delle misure di sicurezza che non ritengono utile un audit lungo, avendo in effetti non molte cose da vedere. Come al solito, il giusto starebbe nel mezzo; speriamo di averlo trovato.

Delle altre norme oggetto di questo meeting (ISO/IEC 27007, 27008, 27010, 27013, 27017, 27019, 27021) non ho seguito le discussioni.

Ho seguito anche una breve riunione in merito ad un possibile futuro e ulteriore standard sul cloud. Ormai il numero di standard sul cloud è così elevato che è quasi ridicolo (se poi pensiamo che per gli "altri" fornitori non sono quasi disponibili delle buone linee guida). Una delegata ha chiesto di presentare, per il prossimo incontro di ottobre, dei casi pratici che non possono essere affrontati con gli standard attualmente disponibili. Ho apprezzato molto questa richiesta, soprattutto perché ci aspettiamo che non ne sarà presentato nessuno.

****

02- Certificazione e bandi di gara

Sandro Sanna mi ha segnalato la "Linee Guida ACCREDIA per i bandi di gara". È un documento molto sintetico in cui sono riportati dei suggerimenti e degli esempi per richiedere ad un fornitore o potenziale fornitore prova di una certificazione:
- http://www.accredia.it/news_detail.jsp?ID_NEWS=1711&areaNews=94&GTemplate=default.jsp

Il documento riporta ulteriori e utili informazioni per esempio su come richiedere un'offerta per un servizio di certificazione.

****

03- Standardizzazione - ISO/IEC 20000 e informatica

Stanno girando da tempo post e articoli sul fatto che forse la ISO/IEC 20000 non riguarda solo i servizi di tipo informatico, ma tutti i servizi.

Ne ho avuto conferma al meeting dell'SC27 e un po' ne sono rimasto sorpreso.

Di questa possibilità ne parlai, assolutamente casualmente, nel 2005 con Tony Coletta. Ci eravamo messi a discutere sul perché nella norma non apparisse mai "IT" e se quindi, forse, poteva essere generalizzata. Mi ricordo che, in effetti, convenimmo sulla sua possibile generalizzazione, ma non pensavo che questa idea potesse diffondersi.

Ora la cosa è ufficiale o quasi ufficiale.

****

04- Privacy e profilazione on-line

Sono state pubblicate le "Linee guida in materia di trattamento di dati personali per profilazione on line". Sono applicabili da chiunque faccia profilazione on line:
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3881513

Francamente, non mi pare ci sia nulla di nuovo. D'altra parte, un richiamo su informativa, consenso e diritto di opposizione è sempre benvenuto.

****

05- Privacy e lavoratori

Il Garante privacy ha pubblicato il Vademecum 2015 su "Privacy e lavoro" (grazie a Ivo Trotti di TNS per la segnalazione):
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3890025

Oltre a questo, il Consiglio d'Europa in data 1° aprile 2015 ha adottato la Raccomandazione CM/Rec(2015)5 sul trattamento dei dati personali nel contesto dell'occupazione. I datori di lavoro dovrebbero ridurre al minimo i rischi di violazione dei diritti dei lavoratori e delle libertà fondamentali:
- https://wcd.coe.int/ViewDoc.jsp?id=2306625

Questa seconda notizia mi è stata fornita da Enzo Ascione di Intesa Sanpaolo. Enzo si chiede anche come agiranno le imprese che hanno già emesso delle policy interne in conformità al Provvedimento del Garante in materia di utilizzo della posta elettronica e della rete internet (delibera n. 13 del 1° Marzo 2007).

Inoltre si chiede:
- Quanto differiscono queste Recommendation "europee" dalla delibera "italiana" di cui sopra?
- Questa analisi sarà affrontata e pubblicata dal Garante o dovremo farla da soli?
- Come tenere conto delle eventuali differenze?

****

06- Sito di confronto delle normative privacy

Stefano Ramacciotti, che ringrazio moltissimo, mi ha segnalato questo sito che permette di confrontare tra loro le normative privacy di due Paesi:
- http://www.dlapiperdataprotection.com/#handbook/registration-section/c1_IT/c2_NO

Ci ho fatto un breve test e mi è sembrato molto bello.

****

07- Linee guida del CERT sulla codifica

Vi segnalo i "CERT Coding Standards" per C, C++, Java, Perl e Android:
- https://www.securecoding.cert.org/confluence/display/seccode/CERT+Coding+Standards

Il un'altra pagina, sono a disposizione le "Java Coding Guidelines":
- https://www.securecoding.cert.org/confluence/display/java/Java+Coding+Guidelines

La differenza tra gli "standard" e le "linee guida" al momento mi sfugge.

****

08- CSSLP (libro) - Sviluppo sicuro

Da tempo volevo approfondire il tema dello sviluppo sicuro. Ho cercato un libro e ho trovato questo:
- Mano Paul. "Official (ISC)2 Guide to the CSSLP". USA: CRC Press, 2011.

È il libro per la preparazione all'esame CSSLP del (ISC)2 e quindi soffre di qualche limite, il primo dei quali è che un manuale per preparare ad un esame non è la stessa cosa di un libro scritto per altri scopi.

Il libro ha altri limiti, tra cui: errori di inglese (li ho trovati io!) e ripetitività di alcuni argomenti in diversi capitoli (e non sempre presentati in modo allineato). Drammaticamente ci sono anche errori tecnici (mi chiedo cosa abbia letto della ISO/IEC 27006, visto che la considera una norma per la "certificazione" del software e non per gli organismi che certificano secondo ISO 9001, 14001 e altri standard per i sistemi di gestione).

Però, in questi tempi in cui parlo con gli sviluppatori di "politiche di sviluppo sicuro" o, più banalmente, di "accorgimenti di sviluppo sicuro", vedo solo: a) sguardo di mucca quando passa il treno; b) i risultati di un vulnerability assessment; c) documenti in cui la parola "sicurezza" è nominata per sbaglio una o due volte senza ulteriori dettagli.

Allora è benvenuto un libro, per quanto mal fatto, che parla di sviluppo sicuro o, in inglese, di secure software development lifecycle (SSDLC).

In questo libro si parte dal "solito" risk management, per poi trattare del ciclo di vita: requisiti, progettazione, codifica, testing (tecnico), accettazione, messa in produzione, conduzione, manutenzione e eliminazione. Ci sono anche capitoli sulla catena di fornitura e sull'acquisizione di software da parti esterne.

Ovviamente, chiunque voglia segnalare altri testi è il benvenuto.

****

09- Supply Chain Resilience report

Il Business continuity institute mi ha comunicato la pubblicazione del Supply Chain Resilience report 2014:
- http://www.thebci.org/index.php/about/news-room#/pressreleases/businesses-facing-high-costs-of-supply-chain-disruption-1078655

Per scaricarlo chiedono di registrarsi, ma credo che anche fornendo dati falsi si possa accedere al link.

Detto questo, per pigrizia mi sono accontentato di leggere la sintesi, consapevole che ogni report segnala (più o meno) quello che vuole, solitamente per spingere da qualche parte (non mi sorprende infatti che un report sulla "supply chain" inizi dicendo che l'80% degli intervistati hanno avuto, l'anno precedente, dei problemi di filiera di fornitura, né che un report realizzato con il contributo delle assicurazioni Zurich riporti perdite ingenti per questi problemi e sottolinei che il 40% degli intervistati ha dichiarato di non avere stipulato polizze specifiche).

Però qualcosa fa riflettere, soprattutto se ci fermiamo a parlare di informatica: il 53% dei problemi di fornitura è dovuto a interruzioni dei sistemi informatici. Questo mi riporta ad uno dei miei cavalli di battaglia: forse anche questi hanno pensato troppo ai potenziali problemi di sicurezza del cloud e non hanno pensato a quelli posti dai fornitori, anche di informatica, "tradizionali".

Questo report ci ricorda la necessità di analizzare il più possibile l'intera filiera di fornitura e non fermarsi solo al fornitore primario.

****

10- NIST SP 800-161 su supply chain risk management

Il NIST ha pubblicato la Special Publication 800-161, Supply Chain Risk Management Practices. Essa è indirizzata agli enti federali degli USA ma potrebbe essere interessante per tutti:
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

Io sono un fan delle pubblicazioni del NIST, ma questa non mi ha soddisfatto. Infatti spende 36 pagine per illustrare un metodo di risk assessment (come se il NIST non avesse già un'altra pubblicazione dedicata a questo o come se gli autori di questa pubblicazione volessero dire la loro sulla materia) per poi elencare lungamente dei controlli di sicurezza non sempre applicabili a tutti i fornitori. Anche l'elenco delle minacce non mi sembra particolarmente illuminante.

Mi sarebbe piaciuto infatti trovare considerazioni sui rischi relativi ai fornitori e alla filiera di fornitura, mentre invece non si trova quasi nulla di tutto ciò. E così pure sui controlli di sicurezza.

Bisogna dire che mi sembra quindi un'occasione persa, soprattutto se consideriamo quanta letteratura (di qualità non sempre eccelsa...) è stata fatta sui servizi cloud (ossia su una tipologia specifica di fornitori) e quanta poca ve ne sia sugli altri fornitori. Poteva essere l'occasione per ricordare che gran parte delle questioni di sicurezza delle informazioni relative ai servizi cloud sono in realtà comuni a più tipologie di fornitori e che, pertanto, andrebbero affrontate.

****

11- Rapporto semestrale MELANI

Ogni sei mesi MELANI, la "Centrale d'annuncio e d'analisi per la sicurezza dell'informazione" svizzera pubblica un rapporto sulla sicurezza delle informazioni molto ben fatto.

Il 2014/II uscito a fine aprile 2015 riporta in parte i "soliti" attacchi di virus, intrusione, eccetera. In parte ci sono articoli su un attacco ad un impianto industriale in Germania, ad aziende norvegesi del settore petrolifero, alla navigazione aerea, eccetera. Il rapporto si trova a questo indirizzo:
- http://www.melani.admin.ch/dienstleistungen/archiv/01598/index.html?lang=it

La cosa interessante è che per ogni tipo di attacco sono riportate sinteticamente le misure di sicurezza da considerare. Per gli impianti industriali si fa anche riferimento ad una pubblicazione specifica dal titolo "Misure di protezione dei sistemi industriali di controllo (ICS)":
- http://www.melani.admin.ch/dienstleistungen/00132/01557/index.html?lang=it

****

12- I dieci rischi più importanti per le tecnologie sanitarie

Marco Fabbrini, esperto di dispositivi medicali, mi ha segnalato la pubblicazione "Top 10 Health Technology Hazards for 2015" dell'ECRI Institute:
- https://www.ecri.org/press/Pages/ECRI-Institute-Announces-Top-10-Health-Technology-Hazards-for-2015.aspx

Il rapporto è stato tradotto in italiano da AIIC.

I 10 rischi più importanti sono:
1. Policy e pratiche di configurazione degli allarmi inadeguate;
2. Dati errati o mancanti nella cartella clinica elettronica ed altri sistemi informatici;
3. Inversione di linee per terapia endovenosa e conseguente errata somministrazione di farmaci;
4. Rigenerazione inadeguata di endoscopi e strumenti chirurgici;
5. Mancata rilevazione di scollegamento dei ventilatori, a causa di allarmi mal-impostati o non avvertiti;
6. Errori nell'utilizzo e malfunzionamento di dispositivi per la movimentazione del paziente;
7. "Dose Creep": Insidiose variazioni nell'esposizione a radiazioni diagnostiche;
8. Complicazioni conseguenti a formazione inadeguata su chirurgia robotica;
9. Protezioni inadeguate per dispositivi e sistemi medicali da attacchi informatici;
10. Collassamento dei programmi per la gestione di richiami e avvisi di sicurezza.

Marco mi ha fatto notare che 3 su 10 sono di sicurezza informatica (il 2, il 9 e il 10). Tutto ciò è sintomo di un interesse degli operatori per questi temi (i rischi non sono stati rilevati da statistiche degli incidenti registrati, ma da altre fonti) e quindi da considerare.

****

13- Attacco ad una TV francese

Questa notizia la trovo strabiliante:
- http://arstechnica.com/security/2015/04/hacked-french-network-exposed-its-own-passwords-during-tv-interview/

Dal SANS NewsBites: in un'intervista video (peraltro relativa ad un hacking di un satellite), alle spalle dell'intervistato (un giornalista della rete francese TV5Monde) si trovavano dei foglietti con user-id e password. Come è andata a finire, potete immaginarlo (11 stazioni hanno avuto delle interruzioni di segnale).

Questo ci ricorda che ci vuole veramente poco per essere attaccati con successo.

****