Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – MAGGIO 2014

****

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- Prossimi appuntamenti: DFA Open Day 2014 - 5 giugno 2014 - Milano

Il 5 giugno si terrà l'Open Day dell'associazione DFA, di cui sono consigliere.

Sono molto orgoglioso del programma, che sarà pubblicato in forma completa su:
- http://www.perfezionisti.it/proposte-formative/dfa-open-day-2014/.

Gli argomenti saranno soprattutto relativi a "OSINT e Investigazioni Digitali" e "Security e Incident Response aziendale".

La partecipazione è gratuita. Programma in sintesi e modulo di registrazione:
- http://dfaopenday2014.eventbrite.it/

****

02- Standardizzazione: stato delle norme ISO/IEC 270xx

Venerdì 11 aprile si è concluso a Hong Kong il 48mo meeting dell'SC 27 dell'ISO/IEC JTC 1. Come nel precedente meeting di ottobre 2013 hanno partecipato circa 250 delegati, di cui 100 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: Fabio Guasconi (Presidente SC 27 italiano), io per seguir i lavori del WG 1 insieme a Fabio, Dario Forte per il WG 4 e Andrea Caccia per i WG 1 e 4 e come rappresentante per ETSI.

In questo meeting del WG sono proseguiti i lavori sulle nuove ISO/IEC 27003, 27004, 27005, 27006, 27009, 27010, 27011, 27013 e 27017. Si è anche lavorato sulle future edizioni della ISO/IEC 27000. Sono stati avviati i lavori preliminari per le nuove edizioni delle ISO/IEC 27007, 27008, 27019 e per la nuova ISO/IEC 27021 sulle competenze dei professionisti di sistemi di gestione per la sicurezza delle informazioni.

Questo arido elenco di norme non rende giustizia di quanto successo: si è discusso molto in un clima decisamente costruttivo e in modo che le esigenze dei rappresentanti dei diversi Paesi e delle diverse parti interessate alle norme (auditor, consulenti e organizzazioni) fossero ben espresse.

****

03- Standardizzazione: Presentazione ISO/IEC JTC 1/SC 27

Il ISO/IEC JTC 1/SC 27 è il comitato che si occupa, tra le altre cose, della scrittura della ISO/IEC 27001.

E' stata predisposta una presentazione per illustrarne l'organizzazione, i partecipanti, i progetti in corso e altro ancora. Il link è il seguente:
- http://www.jtc1sc27.din.de/cmd?level=tpl-bereich&languageid=en&cmsareaid=sc27slides

****

04- Standardizzazione: Ancora su HLS, Annex SL e Annex SC

A gennaio avevo scritto un breve articolo (ora modificato) sulla nuova edizione delle Direttive ISO/IEC:
- http://blog.cesaregallotti.it/2014/01/annex-sl-o-annex-jc-o-mss-hls.html

L'articolo segnalava che l'HLS (ossia il testo base da utilizzare per tutte le norme relative ai sistemi di gestione, su cui è basata la ISO/IEC 27001:2013 e su cui si baserà la futura versione della ISO 9001) si trovava nell'Annex SC, mentre sulla ISO/IEC 27001 si fa riferimento a questo testo come "Annex SL". Io ora penso sia meglio chiamarlo MSS HLS (management system standards high level structure) per evitare confusioni.

In realtà ho fatto un errore: la ISO/IEC pubblica Direttive specifiche per l'ISO e Direttive specifiche per il JTC 1 (il comitato dedicato alle attività congiunte ISO e IEC, tra le quali vi è la scrittura della ISO/IEC 27001) e probabilmente altre Direttive specifiche per altri organismi.

Bene... nelle Direttive specifiche per l'ISO, di cui è stato pubblicato recentemente l'aggiornamento, continua a riportare il MSS HLS in Annex SL, mentre le Direttive specifiche per il JTC 1 lo riporta in Annex SC.

A complicare ulteriormente le cose, i due testi sono ora disallineati. In particolare, nelle nuove direttive specifiche per l'ISO è stata eliminata la definizione di "correzione" perché, in effetti, non presente nel

resto del testo (anche se è molto utile distinguere tra "correzione" e "azione correttiva" e ricordare che la ISO 9001, come la ISO/IEC 27001, non richiede assolutamente di attuare azioni correttive per ogni non conformità rilevata, né confonde tra correzione e azione correttiva).

Le Direttive ISO/IEC sono disponibili a questo link:
- http://www.iso.org/iso/home/standards_development/resources-for-technical-work/iso_iec_directives_and_iso_supplement.htm

Sono previste delle linee guida per l'uso del MSS HLS al seguente link, ma al momento non ve ne sono (altra cosa che trovo ironica):
- http://isotc.iso.org/livelink/livelink?func=ll&objId=16347818&objAction=browse&viewType=1

****

05- Standardizzazione: Storia e futuro della ISO 9001

Segnalo questo white paper del BSI dal titolo " The history and future of ISO 9001 - Approaching change":
- http://www.bsigroup.com/LocalFiles/en-GB/iso-9001/Revisions/ISO%209001%20Whitepaper%20-%20the%20history%20and%20future%20of%20ISO%209001.pdf

Il motivo per l'interesse è la storia, che avevo dimenticato: nata come BS 5750 e appoggiata dal Ministero della difesa UK, si occuapava della gestione dei processi manifatturieri. Nel 1987 la BS 5750 fu recepita dall'ISO con il codice 9001 e modificata per coprire più tipologie di business. L'edizione ISO 9001:1994 era più orientata all'assicurazione qualità, con l'introduzione delle azioni preventive. La successiva edizione ISO 9001:2000 introdusse l'approccio per processi e la loro misurazione. La ISO 9001:2008 è un raffinamento della versione del 2000.

Il white paper si dilunga sulle novità della futura versione prevista per il 2015. Questa è pura operazione di marketing sulla cui completa onestà ho molto dubbi (il BSI promuove convegni a pagamento e l'acquisto dei draft dello standard) . Infatti la norma si trova in stato di Committee Draft e potrebbe subire consistenti cambiamenti da qui alla sua pubblicazione (come peraltro ho sperimentato personalmente durante i lavori dell'SC 27 e in particolare con la ISO/IEC 27001 e la ISO/IEC 27006). Pertanto, a meno che non partecipiate ai lavori della futura ISO 9001 (in Italia è possibile farlo attraverso l'UNI), il mio consiglio è di non far nulla.

****

06- Legale: accreditamento conservazione digitale

Sandro Sanna e Vincenzo Mondelli mi hanno segnalato la pubblicazione della Circolare 65 del 10 aprile 2014 dell'Agenzia per l'Italia digitale (AgID) che riporta le modalità per l'accreditamento dei conservatori dei documenti informatici.

Avevo accennato a suo tempo alla pubblicazione delle regole tecniche:
- http://blog.cesaregallotti.it/2014/04/regole-tecniche-protocollo-e.html

Mi era sfuggito però che tra le richieste fatte ai conservatori vi fosse la certificazione ISO/IEC 27001. In realtà è divertente vedere come nelle regole tecniche stabilite dal DPCM del 3 dicembre 2013 la richiesta è esposta come possibilità ("il responsabile della conservazione può chiedere di certificare la conformità..."), mentre nella documentazione richiesta dall'AgID vi è il certificato ISO/IEC 27001 senza prevederne l'assenza.

Ho notato inoltre che la richiesta è fatta molto bene: richiedono la certificazione rispetto all'edizione 2013 della norma, con riferimento anche all'edizione precedente, specificano che deve includere la conservazione e che il certificato deve essere rilasciato da un organismo di certificazione accreditato (poco prima delle mail di Sandro e Vincenzo avevo ricevuto un'altra e-mail che mi riferiva che un'Autorità europea aveva, ahimè, chiesto le certificazioni ISO/IEC 27002 e 27005, come se esistessero...).

****

07- Fondi ai progetti open source

Dal SANS NewsBites segnalo questa notizia: le più grandi società tecnologiche hanno comunicato che contribuiranno economicamente alla Linux Foundation's Core Infrastructure Initiative per aiutare i progetti open source. Il bug Heartbleed ha portato alla ribalta la situazione di OpenSSL: il codice è diffusissimo, ma il progetto riceve donazioni per circa 2.000 dollari all'anno ed è seguito da un addetto a tempo pieno:
- http://arstechnica.com/information-technology/2014/04/tech-giants-chastened-by-heartbleed-finally-agree-to-fund-openssl/

Trovo tutto questo stupendo: un tizio mantiene quasi gratuitamente un codice che è utilizzato da tantissime società per guadagnare tanti tanti milioni di dollari, senza che gliene diano neanche una briciola... fino al pasticcio, ovviamente!

A questo proposito segnalo anche questo interessante articolo:
- http://www.theregister.co.uk/2014/04/11/openssl_heartbleed_robin_seggelmann/

Ovviamente, per disperdere energie, qualcuno ha pensato bene di aprire un nuovo progetto: LibreSSL. Non posso fare a meno di riflettere sulle similitudini con i nostri partiti politici...
- http://threatpost.com/libressl-sticks-a-fork-in-openssl/105653

****

08- Electronic Evidence Guide

E' stata recentemente pubblicata la "Guida alla prova digitale", traduzione italiana della "Electronic Evidence Guide" del Council of Europe. Per scaricare la guida dovete compilare il form online disponibile a questo indirizzo:
- https://docs.google.com/forms/d/1gwHSgAjlyKWT10FEh8JNIAt_OQBRaCV4Jgt_-SLUWhU/viewform

La versione italiana nasce dallo sforzo congiunto delle associazioni Digital Forensics Alumni, Tech and Law Center e DEFT Association. La guida è stata presentata ieri a Deftcon 2014 e sarà nuovamente illustrata il prossimo 5 Giugno 2014 in occasione del DFA Open Day alla Statale di Milano.

La versione in inglese si trova a questo indirizzo:
-
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp

La lettura è molto interessante anche per chi vuole capire meglio cos'è la digital forensics e presenta numerosi casi ed esempi.

****

09- Le frodi nella rete (una guida)

Enrico Toso di DB Consorzio mi ha segnalato un interessante lavoro presentato a Milano, al Security Summit 2014. Il titolo è "Le frodi nella rete" e si trova a questo indirizzo:
- http://frodi.clusit.it/views/Homepage.html

La presentazione fatta al Security Summit si trova tra gli atti del 19 marzo:
- https://www.securitysummit.it/milano-2014/atti/atti-19-marzo/

Nel documento ho trovato interessante soprattutto la seconda parte, dove sono analizzate le frodi tipiche di ogni settore (banche, telco, assicurazioni, gaming, pagamenti on-line, mobile, carte di credito e proprietà intelletuale) e sono indicate delle modalità per prevenirle e/o rilevarle.

****

10- Guida rapida Scrum

Stefano Ramacciotti mi ha segnalato l'interessante pubblicazione "Scrum Primer 2.0" e la sua traduzione in italiano:
- http://www.greengegneria.it/index.php?option=com_content&view=article&id=135

Copio e incollo dalla breve presentazione: "Scrum è il modello di Sviluppo Software Agile più diffuso al mondo. The Scrum Primer 2.0 è una delle guide rapide su Scrum più note a chi si è avvicinato a questo modello di Sviluppo Agile".

****

11- AdS che chiedono la password agli utenti

Segnalo questo articolo sul blog di Achab:
- http://www.achab.it/blog/index.cfm/2014/4/chiedere-la-password-in-modo-sicuro.htm

In poche parole, Achab ha condotto un sondaggio da cui emerge che solo il 24% degli amministratori di sistema non chiede mai la password agli utenti dei sistemi che amministrano.

Provo a fare una lista del perché il restante 76% fa male:
- perché se gli utenti comunicano la propria password agli amministratori di sistema, allora si sentono autorizzati a comunicarla ai colleghi, agli amici, ai parenti...;
- perché se gli utenti sono abituati a comunicare la propria password agli amministratori di sistema, allora non sembrerà loro strano inviargliela se gliela richiedono via mail (e poi ci si chiede perché gli utenti abboccano alle e-mail di phishing);
- perché se la password non è più segreta, si riduce il livello di certezza con cui si riconosce chi ha fatto cosa sui sistemi informatici;
- perché spesso le password sono usate per accedere a dati personali e la normativa vigente in materia di privacy richiede di mantenerla segreta;
- perché se la password non è più segreta, allora forse accedono persone non autorizzate ai sistemi informatici aziendali.

Nell'ultimo punto ho scritto "forse", ma solo perché sono un ottimista.

Evito di commentare per iscritto, ma confermo che ho fatto qualche riflessione sulle competenze di certi amministratori di sistema e sulle configurazioni di certe reti aziendali.

L'articolo, tra le altre cose, ricorda una misura compensativa nel caso vengano comunicate le password dagli AdS: tenere traccia dell'evento e modificarle appena il lavoro è stato finito.

****

12- Attacco a Orange

Fabrizio Monteleone di DNV GL mi ha segnalato questa notizia:
- http://www.bbc.com/news/technology-27322946

Dei malintenzionati hanno ottenuto accesso a dei database dell'operatore francese di TLC Orange e ai dati anagrafici dei clienti. Apparentemente, non sono stati compromessi dati critici come i numeri di carte di credito o le password di accesso ai servizi. Ciò non ostante il danno può essere consistente.

Non posso fare a meno di rilevare che Orange ha preferito aspettare del tempo prima di rendere pubblico l'incidente, causando molto malcontento tra i propri clienti. Inoltre, ho trovato molto inquietante che abbiano dichiarato di non sapere se i dati fossero cifrati o meno.

****

13- 2014 Data Breach Investigations Report

Anche quest'anno segnalo la pubblicazione del Data Breach Investigations Report di Verizon:
- http://www.verizonenterprise.com/DBIR/2014/

La segnalazione l'ho avuta dalla newsletter SANS NewsBites che riporta un link al seguente articolo (mi chiedo perché non riporti il link diretto al report):
- http://www.nextgov.com/cybersecurity/2014/04/government-employees-cause-nearly-60-public-sector-cyber-incidents/82933/

Riassumo il riassunto del SANS: almeno metà degli incidenti registrati nel settore pubblico sono dovuti al personale interno. Di questi, un terzo riguarda incidenti "vari", tra cui e-mail inviate a persone sbagliate.

Spionaggio e sfruttamento di vulnerabilità dei siti web costituiscono meno del 1% degli incidenti. I numeri delle imprese private sono diversi perché gli incidenti nel settore pubblico devono essere documentati e quindi piccoli errori molto frequenti predominano nella statistica.

Personalmente ritrovo le stesse difficoltà delle singole aziende che vogliono elaborare statistiche sulla sicurezza delle informazioni: i dati sono troppo eterogenei e variegati per ottenere qualcosa di realmente significativo e, quindi, piuttosto che "misurare" è necessario "monitorare" e "riferire"... ma di questo già scrissi a suo tempo (http://blog.cesaregallotti.it/2013/04/se-non-lo-misuri-non-lo-conosci.html).

****

14- Delle definizioni di rischio (approfondimento)

Dopo il mio post "Delle definizioni di rischio" (http://blog.cesaregallotti.it/2014/04/delle-definizioni-di-rischio.html), Andrea Veneziani di Data Management mi ha proposto un approfondimento che riporto di seguito (e lo ringrazio).

La definizione di rischio in seno al D. Lgs. 81/2008 può essere interpretato come "probabilità che si verifichino degli eventi per cui si hanno dei danni consistenti". In realtà si dovrebbe togliere la parola

"consistenti" a meno che non si voglia semplicemente dire "tangibili" ed in qualche modo "misurabili" e non come si dovrebbe intendere "di notevole entità", "ragguardevoli", "ricchi".

Infatti col D. Lgs. 81/2008 il focus è sulla salute e sicurezza dei lavoratori per cui il rischio e soprattutto il concetto di "danno" è legato alla salute misurabile in giorni di malattia o infortunio, che poi possono essere quantificati in punti di invalidità. Il caso peggiore (caso morte) non lo voglio contemplare, ma anche questo è configurabile come "misurabile" secondo parametri assicurativi.

In buona sostanza anche un giorno di assenza dal lavoro per infortunio causato potrebbe essere considerato un danno "consistente" ed andrebbe contemplato, anche se fino a 20 gg. non è punibile penalmente. Si eccettuano pertanto solo le piccole ferite guaribili senza grossi interventi da parte di medici. Colgo l'occasione per citare che eventuali lesioni personali colpose sopra i 20 gg. di calendario (causate da una non corretta valutazione del rischio e azioni per ridurlo da parte del datore di lavoro) potrebbero essere punibili con la reclusione fino a tre mesi….

In conclusione il "danno accettabile" spesso si riduce a "taglietti provocati dalla carta" per i rischi da ufficio, mentre tutto il resto ahimè andrebbe considerato come "consistente".

Da qui la differenza "logica" che deriva tra una definizione ISO del concetto di rischio e quella data dal D. Lgs. 81/08. In quest'ultimo caso l'asticella è tenuta ben focalizzata sui danni (anche minimi) anziché sulle semplici valutazioni di accettabilità del rischio.