****
IT SERVICE MANAGEMENT NEWS - OTTOBRE 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- Architetti e ingegneri

Nel contesto dell'organizzazione aziendale, negli anni '80 e '90 del XX secolo andava di moda l'ingegneria. Schiere di consulenti promuovevano la "reingegnerizzazione" dei processi (business process reengineering; BPR); ma tantissimi progetti fallirono o ebbero grossi problemi: troppe analisi, troppa complessità nella definizione delle soluzioni, troppe difficoltà nel realizzarle, troppi soldi per i consulenti. Per tutto l'inizio degli anni 2000, non si è quasi più sentito parlare di questa materia.

In questi ultimi anni stanno prendendo la scena gli architetti e si sente parlare assai di "Enterprise architecture" (EA), soprattutto in ambito IT. I loro riferimenti sono principalmente il TOGAF e ArchiMate, ambedue mantenuti (e venduti) dal The Open Group (già dal nome, fanno capire che nel marketing sono bravi).

Ho guardato velocemente Wikipedia e quanto disponibile liberamente sul web. Mi pare che questi architetti non siano diversi dai precedenti ingegneri: tanti modelli, tanta astrazione, tanti nomi difficili, tanto approccio top-down (ossia: scrivere le procedure senza sapere cosa fa attualmente chi le dovrà applicare e, quindi, le difficoltà che avrà nell'adottarle). Immagino che ciò voglia anche dire tanti soldi per i consulenti. Consulenti che amano scrivere documenti, parlare con i dirigenti e non affaticarsi a capire cosa succede veramente tra gli operatori.

Io sono un matematico e già ho una naturale diffidenza per ingegneri e architetti. Ho anche avuto modo di imparare a fare consulenza scrivendo pochi e sintetici documenti, parlando e discutendo con gli operatori e cercando di capire visivamente i processi aziendali prima di proporre modifiche. Ho scoperto in un secondo tempo che si potrebbe apporre l'etichetta "Kaizen" a questo approccio (sarebbe comunque limitativo; il Kaizen è materia molto più complessa). E ho scoperto che i miei progetti durano poco tempo, lasciano dietro di sé qualcosa (non tutto) che dura qualche annetto, mi fanno fare delle amicizie che ancora durano.

Non è pubblicità a me stesso: ci sono anche altri che la pensano come me, da cui ho imparato molto e lavorano quasi sicuramente meglio di me. Chiamateci artigiani, se volete.

Perché scrivo tutto ciò? Per dire perché studio superficialmente i modelli BPR e EA e ne diffido. Forse sbaglio, forse molti non condividono il mio punto di vista. Meno male.

- Il TOGAF: http://pubs.opengroup.org/architecture/togaf9-doc/arch/index.html
- ArchiMate: http://www.opengroup.org/archimate/
- Il DoDAF, il modello EA del DoD USA: http://dodcio.defense.gov/dodaf20.aspx

Infine, segnalo l'articolo che mi ha spinto a scrivere questo, segnalato sul itSMF Italia Group di LinkedIn:
- http://www.twitlonger.com/show/j63qc9?goback=.gde_43531_member_159589784

****

02- Standardizzazione: approvata la ISO/IEC 27037 su digital forensics

Segnalo che è stata approvata, con voto concluso il 23 settembre, la norma ISO/IEC 27037 dal titolo "Guidelines for identification, collection, acquisition, and preservation of digital evidence".

Questa norma sarà poi seguita da altre norme ISO sulla digital forensics.

Da una presentazione di Alessandro Guarino del novembre 2011, segnalo che questa norma riguarda le fasi di identificazione, raccolta (collection), acquisizione e conservazione (preservation); non riguarda quindi le fasi di analisi, presentazione, eliminazione (disposal).

****

03- Standardizzazione: IRCA Briefing note: Annex SL

L'IRCA ha pubblicato una piccola guida sull'Annex SL ossia dell'Allegato SL al "ISO/IEC Directives, Part 1: Consolidated ISO Supplement – Procedures specific to ISO". Precedentemente, questo Allegato aveva il nome di ISO Guide 83.

L'Annex SL stabilisce lo schema comune che dovranno avere tutte le norme di requisiti per i sistemi di gestione. In altre parole, stabilisce lo schema che dovranno avere le future edizioni di ISO 9001, ISO 14001, ISO/IEC 20000-1, ISO/IEC 27001 e non solo. Questo schema è già stato adottato, anche se in una versione precedente, dalla ISO 22301 sulla business continuity.

Il testo si può trovare all'appendice 3 dell'allegato SL del supplemento consolidato dell'ISO della parte 1 delle direttive ISO/IEC. In poche parole: da pagina 143 a pagina 152 del documento che si può scaricare da qui:
- http://isotc.iso.org/livelink/livelink?func=ll&objId=4230452&objAction=browse&sort=subtype

La guida dell'IRCA illustra i punti più significativi delle modifiche che saranno introdotte negli standard dei sistemi di gestione:
- http://www.irca.org/en-gb/resources/Guidance-notes/Annex-SL-previously-ISO-Guide-83/

****

04- Standardizzazione: le regole del gioco

La UNI ha pubblicato il libro "Le regole del gioco", in cui sono spiegati in modo chiaro e scorrevole i processi che portano alla definizione degli standard nazionali e internazionali. Sono descritti quasi tutti i termini gergali e gli acronimi che non sempre sono facili da capire.

L'ho letto con piacere e con gusto. Ho trovato spiegate le relazioni tra UNI, UNINFO, EN, CEI e ISO; la definizione di PAS, TS e IS; la storia della normazione internazionale. Non sono neanche nascoste le difficoltà che ogni tanto emergono e le limitazioni della normazione.

La pagina ufficiale al libro "Le regole del gioco", scaricabile in pdf:
http://www.uni.com/index.php?option=com_content&view=article&id=1555

Le mie critiche ai processi di normazione:
http://blog.cesaregallotti.it/2012/05/chi-partecipa-ai-comitati-iso_10.html

****
05- NISTIR 7874: "Guidelines for Access Control System Evaluation Metrics"

Il NIST, a settembre 2012, ha pubblicato il report "Guidelines for Access Control System Evaluation Metrics".

Lo segnalo per due motivi: uno tecnico e uno terminologico.

Il motivo tecnico è presto detto: il rapporto presenta un elenco di requisiti che dovrebbe avere un sistema di controllo accessi. E' evidentemente rivolta agli sviluppatori e richiede un buon livello di preparazione tecnica.

Il motivo terminologico riguarda l'uso del termine "metrica". Il documento presenta soprattutto "metriche" i cui valori possibili sono "sì" o "no". Qui si pone un primo problema: si può parlare di "metriche", e quindi di "misurazione" come da ISO/IEC 27004, se la scala è composta da due valori discreti? A rigore, ovviamente, la risposta è sì. Tutto ciò, nel mondo non scientifico, porta al rischio di vedere inclusi nelle metriche anche valori soggettivi ("è adeguato?"; "sì"), fino a perdere di vista la differenza tra "metriche", "valutazioni su parametri oggettivi" e "valutazioni su parametri soggettivi".

Tutto ciò può portare (e sta già portando) a errori potenzialmente dannosi, come l'idea che si possa fare un'analisi dei rischi quantitativa o che il livello di sicurezza sia misurabile sulla base di valori oggettivi.

Concludo, anche se salto logico potrebbe apparire eccessivamente ampio: è un errore cercare di riportare la sicurezza a schemi rigorosamente logico-analitici: c'è anche la psicologia, di cui tenere conto. Oltre al fatto che un approccio troppo rigoroso dovrebbe tenere conto di un elevatissimo livello di complessità che mal si sposa con il fatto che la sicurezza deve essere applicata da organizzazioni fatte di persone. Quindi, promuovo il ritorno a termini meno ambiziosi di "metriche": "criteri di valutazione" andrebbe benissimo.

****
06- Novità legali: Call Center e privacy - Decreto crescita

Max Cottafavi di Spike Reply mi ha segnalato un aggiornamento privacy con impatto sui call center.

Il DL 83/2012, convertito dalla Legge 134/2012, ha visto l'aggiunta in fase di conversione dell'articolo 24, dal titolo "Misure a sostegno della tutela dei dati personali, della sicurezza nazionale, della concorrenza e dell'occupazione nelle attività svolte da call center".

Per quanto riguarda la privacy, l'articolo richiede (sintetizzo): Quando un cittadino effettua o riceve una chiamata a/da un call center deve essere informato preliminarmente, e se il caso, sul Paese estero in cui l'operatore con cui parla è fisicamente collocato.

Il DL è facilmente reperibile con la funzione di ricerca di www.normattiva.it.

Segnalo, su indicazione dello stesso Max Cottafavi, questo articolo dell'Istituto Italiano per la Privacy, con riflessioni critiche:
- http://www.istitutoitalianoprivacy.it/it/decreto-sviluppo-istituto-privacy-in-parlamento-norma-sbagliata-sui-call-center/

****

07- Novità legali: Agenzia per l'Italia Digitale

Il Decreto Legge 83 del 22 giugno 2012 ("Misure urgenti per la crescita del Paese") ha sancito la chiusura di DigitPA per passarne le funzioni alle neonata Agenzia per l'Italia Digitale. Il Decreto Legge è stato convertito con modificazioni dalla Legge 134 del 7 agosto 2012.

Ricordo che DigitPA era nata a dicembre 2009 come erede del CNIPA, a sua volta erede dell'AIPA. Chissà se la catena si fermerà per un po' di tempo.

L'operazione è ovviamente lodevole, visto che promuove l'accentramento delle funzioni della Pubblica Amministrazione sull'informatizzazione.

L'articolo 20 del DL afferma che l'Agenzia prenderà le funzioni di DigitPA, eccetto "ogni altra funzione prevista da leggi e regolamenti già attribuita al CNIPA, nell'ambito delle direttive del Presidente del Consiglio dei Ministri o del Ministro delegato". Mi chiedo allora quali siano queste funzioni e chi le svolgerà.

Ho notato con dispiacere che il sito di DigitPA non dà la notiza (cita le attività dell'Agenzia per l'Italia Digitale, ma nulla più) e non ho ancora capito se esite un sito web dell'Agenzia per l'Italia Digitale. Capisco che non ci sia, visto che è appena nata; se qualcuno avrà notizie, prego di fornirle.

Comunque, l'Agenzia ha già iniziato a lavorare sui servizi di Disaster Recovery nelle Pubbliche Amministrazioni (la pubblicazione è sul sito di DigitPA):
http://www.digitpa.gov.it/sites/default/files/Raccomandazioni_PROFILI%20MINIMI%20SERVIZI%20DI%20DR_v_2_4_0.pdf

****

08- Novità legali: Certificati digitali invalidati? - 2a puntata

Il 14 febbraio avevo postato la notizia sulla possibile non validità delle firme digitali rilasciate da quasi tutte le autorità di certificazione. Questo perché non avevano dei dispositivi di generazione delle chiavi certificati opportunamente:
- http://blog.cesaregallotti.it/2012/02/certificati-digitali-invalidati.html

Dal sito dell'Agenzia per l'Italia Digitale, ho avuto notizia del DPCM del 19 luglio 2012 con un'ulteriore deroga alle deroghe precedenti (una del 14 ottobre del 2011, che a sua volta prorogava la deroga data il 10 febbraio 2010, che poi a sua volta prorogava una misura del 1999).

Un mio anonimizzato lettore ha fatto i seguenti commenti:
- ho sempre visto le deroghe come una diminuzione "almeno momentanea" della sicurezza e pertanto non mi piacciono. Poi si sa che in Italia niente è più definitivo di ciò che è momentaneo;
- il decreto, è scritto veramente male

Io aggiungo che tutto ciò mi ricorda le brutte deroghe per il DPS.

Infine, ho chiesto sempre al mio anonimizzato lettore alcuni chiarimenti sui tempi di certificazione di un prodotto rispetto ai Common Criteria (ISO/IEC 15408):
- normalmente, la valutazione di un Security target (cioè la fase denominata ASE) la si fa in 30/40 giorni;
- se per "adeguatezza" si intende "una veloce lettura del ST per vedere se il TOE è adeguato per essere sottoposto ad una valutazione", che è la prima azione che fa per Legge un direttore di un CEVA prima ancora di accettare il contratto per evitare di perdere tempo e soldi del contribuente che paga il

certificatore, allora ci vuole una settimana lavorativa;
- per la valutazione del TOE (cioè del suo Security target, dei deliverable e del TOE stesso), per un EAL1 si va da 7/8 mesi a n-anni (con n=2 per un SO EAL4);
- il nostro schema nazionale non prevede, purtroppo, delle durate limite delle certificazioni, che invece sono previste in altri Paesi (dove, per esempio, per un EAL4 devono essere impiegati un massimo di 18 mesi).

Avvertenza: io e il mio lettore abbiamo utilizzato la terminologia inglese, anche perché le traduzioni italiane sono orrende.

Potete scaricare il nuovo DPCM del 19 luglio 2012 da
- www.digitpa.gov.it/sites/default/files/normativa/DPCM_19_luglio_2012.pdf

La pagina di DigitPA:
- http://www.digitpa.gov.it/notizie/firmato-decreto-ministro-profumo

Un commento sul sito dell'ANORC:
- http://www.anorc.it/notizia/354_Approvato_il_Decreto__Salva_-_HSM___ecco_le_novit_.html

****
09- Legale: Privacy e cookies

Enzo Ascione di Intesa Sanpaolo mi ha segnalato questa interessante serie di brevi articoli sull'interpretazione da dare al nuovo articolo 122 del Codice Privacy, così come modificato dal Dlgs 69 del 2012.

L'articolo, soprattutto nella terza parte, tratta delle modalità di gestione dei cookies dei siti web distinguendone le diverse funzionalità (user-input cookies, authentication cookies, multimedia player session cookies, social plug-in content sharing cookies):
- https://associazionecindi.wordpress.com/2012/06/29/cookies-privacy-d-lgs-69/

****
10- Legale: Quaderno UNINFO - sicurezza delle informazioni e privacy

Segnalo che è stato pubblicato il Quaderno UNINFO dal titolo "La gestione della sicurezza delle informazioni e della privacy nelle PMI".

Ho collaborato alla sua redazione con alcuni membri del Gruppo di Lavoro UNINFO sulla serie di norme ISO/IEC 27000. Si tratta infatti di una riflessione sui collegamenti tra ISO/IEC 27001 e normativa privacy. La seconda parte del quaderno presenta una tabella con i collegamenti tra i requisiti dello standard e quelli della normativa italiana.

Devo dire che è stato un lavoro molto interessante, che mi ha dato la possibilità di avere un bel confronto con professionisti preparati.

La home page di UNINFO:
- http://www.uninfo.polito.it/

La pagina delle pubblicazioni di UNINFO:
- http://www.uninfo.polito.it/Pubblicazioni.htm

Il link diretto al Quaderno:
-
http://www.uninfo.polito.it/SC27/SC27public/Quaderno%20UNINFO_La_gestione_dellaSicurezza_delleInformazioni_e_della_Privacy_v1_0.pdf

****

11- Legale: Di Internet e delle pene

Paolo Gasperi di Loogut mi ha segnalato il libro "Di Internet e delle pene" che ha scritto con Silvano Marchi.

L'ho trovato interessante perché spiega in modo chiaro 5 sentenze corrispondenti ad altrettanti reati:
- diffamazione su social network
- cyberstalking
- pubblicazione di un numero telefonico su social network
- scambio video con protagonisti non consenzienti
- uso di e-mail intestata ad altro

Il libro, gratuito e di sole 47 pagine, è scaricabile da:
- http://www.ladige.it/articoli/2012/02/06/sicurezza-line-questione-cultura

****
12- Legale: Modifiche al CAD (commento)

A settembre 2012 avevo scritto un articolo sulle modifiche al Codice dell'Amministrazione Digitale:
- http://blog.cesaregallotti.it/2012/07/modifiche-al-codice-dellamministrazione.html

Io avevo scritto che "la Pubblica Amministrazione è invitata ad acquisire software freeware e non solo open source". Andrea Rui mi ha scritto la precisazione che segue e lo ringrazio.

Il CAD vuole specificare meglio, rispetto alla precedente edizione, che è d'obbligo (a meno di motivatissime ragioni) l'utilizzo di software che viene tecnicamente (non nel testo) identificato come FLOSS (Free/Libre Open Source Software).

Faccio questa precisazione perché il termine 'open source' non sempre implica gratuità, ed in generale il freeware è software a codice chiuso, ma disponibile gratuitamente.

****
13- CERT-EU

Non sapevo che esistesse, ma la notizia sul SANS Newsbyte dice che dopo un anno di sperimentazione il CERT europeo è stato confermato in modo permanente.

Il sito mi sembra molto ricco di informazioni, forse fin troppe.

Per chi fosse interessato: http://cert.europa.eu

****
14- European Cyber Security Month

Mi segnala Simone Tomirotti che "una volta c'era il mese della prevenzione dentale; oggi c'è l'European Cyber Security Month!"

Si tratta di ottobre 2012. Il materiale è in inglese, francese, tedesco e spagnolo. Manca l'italiano e ho un sospetto del perché non ne ho ancora sentito parlare.

Ad ogni modo, il materiale (poster, video, illustrazioni) è interessante anche per chi vuole cominciare una campagna di sensibilizzazione sulla sicurezza informatica nella propria azienda.

Il sito: http://www.enisa.europa.eu/activities/cert/security-month

****

15- Assicurazioni e sicurezza informatica (commenti)

A settembre ho scritto un articolo sul mercato delle assicurazioni nell'ambito della sicurezza informatica:
- http://blog.cesaregallotti.it/2012/08/assicurazioni-e-sicurezza-informatica.html

Ho ricevuto questo commento da Fabrizio Monteleone del DNV Italia: "ci sono articoli del codici civile che trattano i rischi nelle assicurazioni; in particolare il 1897 "Diminuzione del rischio". Esso afferma che se il contraente comunica all'assicuratore mutamenti che producono una diminuzione del rischio (perchè ha fatto l'analisi dei rischi, si è certificato, ...), l'assicuratore deve abbassare il premio corrispondente. Quante aziende certificate ISO/IEC 27001 o BS 25999 (ora ISO 22301) lo usano coi loro broker assicurativi? Come potremmo aiutarli?"

Le mie risposte sono facili:
- non so quante aziende certificate ISO/IEC 27001 o BS 25999 usano questo articolo coi loro broker assicurativi. Ho delle supposizioni, ma preferirei avere prima dei dati (se i miei lettori vorranno contribuire, ne sarò ben lieto)
- potremmo aiutarli segnalando loro proprio l'articolo 1897 del CC.

Per leggere l'articolo del CC: http://www.studiocataldi.it/codicecivile/assicurazione.asp

Stefano Ramacciotti ha trovato interessante il fatto che qualcuno orienti le assicurazioni a riconoscere la bontà del prodotto se sottoposto a 2700x e/o Common Criteria. Infine ragiona: "Forse... dove non poté la politica, poté il dio denaro".