Cesare Gallotti

From: it_service_management-news-bounces@mailman.cesaregallotti.it on behalf of IT Service Management NewsLetter [it_service_management-news@mailman.cesaregallotti.it]

Sent: Sunday, 18 October, 2009 11:20

To: it_service_management-news@mailman.cesaregallotti.it

Subject: [IT Service Management] Newsletter del 18 ottobre 2009

Attachments: ATT00159.txt

****
IT SERVICE MANAGEMENT NEWS
****

Newsletter mensile con novità in materia di sicurezza delle informazioni, IT Service Management, Qualità.
E' possibile dare il proprio contributo e diffonderla a chiunque secondo la licenza http://creativecommons.org/licenses/by-nc/2.5/it/.
E' possibile iscriversi, disiscriversi e modificare le proprie opzioni, oltre a vedere l'informativa sul trattamento dei dati personali, all'indirizzo
http://mailman.ipnext.it/mailman/listinfo/it_service_management-news

****
Indice

****
01- VERA

Sul numero di settembre 2009, ICT Security ha pubblicato un mio articolo su VERA. Devo dire che è stato impaginato proprio male!
E' possibile scaricarlo da
http://www.cesaregallotti.it/art_pres/20090915-Articolo-VERA.pdf

****
02- Novità normative - Siti web

E' stata introdotta una nuova e importante disposizione per i siti web delle aziende.

L'articolo 42 della Legge 88 del 2009 (http://www.parlamento.it/parlam/leggi/09088l.htm) dice che le società per azioni, le società in accomandita per azioni e le società a responsabilità limitata devono indicare sul sito web quanto prescritto dall'articolo 2250 del Codice Civile (http://www.studiocataldi.it/codicecivile/codice_civile_V_titolo_V.asp); in particolare:
- sede sociale, ufficio del registro delle imprese di iscrizione e numero di iscrizione,
- capitale sociale,
- eventuale stato di liquidazione.

La norma parla di "spazio elettronico destinato alla comunicazione", non di sito web. E' quindi immaginabile che dovranno anche essere considerati oggetto di questo provvedimento anche i social network.

Ricordo che sul sito web di tutte le imprese, secondo un'interpretazione del DPR 633 del 1972, deve essere indicata nella home page la Partita Iva.

(Notizia tratta dalla newsletter dell'Ordine dei Dottori Commercialisti e degli esperti contabili del 1 ottobre 2009)

****

03- ITIL - Una nuova edizione?

Dal gruppo di LinkedIn "ITIL v2 / v3 Service Management (ITSM) and ISO 20000" viene segnalato un articolo sul mandato di OGC per una revisione di ITILv3
http://www.itpreport.com/default.asp?Mode=Show&A=2086&R=GL

Sembra che il grosso del lavoro riguarderà il libro di Service Strategy, oltre che una revisione complessiva per rendere i 5 libri più omogenei e coerenti tra loro.

E' noto che ITILv3 è migliorabile, ma è anche vero che ITIL non è uno standard e non deve necessariamente presentare requisiti tra loro coerenti. In troppi invece pensano erroneamente che si possano dichiarare aziende o software conformi rispetto ad ITIL.

****

04- Tool per i Sistemi di Gestione dei Servizi IT

Dal Gruppo di LinkedIn "ITIL v2 / v3 Service Management (ITSM)", ho trovato due elenchi di tool per l'implementazione di un ITSM:
- www.toolselector.com
- https://www.pinkelephant.com/PinkVerify/PinkVERIFYTools.htm.

Intanto, l'OGC ha emesso lo schema di certificazione della conformità dei tool rispetto a ITIL. Io non ho ancora capito quali siano i requisiti rispetto a cui condurre le verifiche
http://www.itil-officialsite.com/SoftwareScheme/ITILSoftwareScheme.asp

Ho provato a fare una piccola software selection per un'azienda, ma questi siti si limitano solo a dire per quali processi è utilizzabile un certo tool. Sicuramente questa solo informazione è insufficiente per determinare la possibile adeguatezza di un tool ad una specifica realtà. Sembrano quindi più iniziative pubblicitarie che iniziative di supporto alle aziende.

****

05- Tool per un assessment ISO/IEC 20000

Dal sito dell'itSMF segnalo uno strumento di assessment per la ISO/IEC 20000. Sembra un buon punto di partenza, ma ha troppi errori per poter essere utilizzato così come è.
http://www.itsmf.it/index.php?method=section&action=zoom&id=1137

****

06- ITSMS e Modelli di maturità

La SEI-CMU ha pubblicato ormai da tempo il CMMI for Services. Ora siamo alla versione 1.2. (Segnalazione di Tony Coletta)

Il modello, a differenza di ITIL, è un insieme coerente di requisiti e come tale dovrebbe essere letto. Si potrebbe paragonare alla ISO/IEC 20000, che, come noto, presenta molte lacune. In particolare, il modello del CMMI-SRV affronta con compiutezza la fase di progettazione e sviluppo.
http://www.sei.cmu.edu/cmmi/tools/svc/index.cfm

****

07- Sistemi Qualità - ISO 9004

La ISO 9004 sarà emessa tra poco tempo. Al momento, per comprendere la nuova norma, può essere utile questo articolo.
http://www.irca.org/inform/issue23/DHoyle.html?dm_i=4VM,1RE3,HZSOT,5MGC,1

****

08- Businnes Continuity

Clusit

Il 24 settembre il Clusit ha organizzato una lezione su "Introduzione alla BS 25999" presentata da Mauro Cicognini. Una mezza giornata sicuramente interessante.

Potete trovare le slides su http://www.clusit.it/download/index.htm (al momento in cui scrivo non sono ancora disponibili).

Business Continuity Institute e GPG

L'istituto tecnico forse più coinvolto nella redazione della 25999 è il Business Continuity Institute (BCI), il cui sito è http://www.thebci.org

Il BCI offre programmi di certificazione delle competenze in materia di Business Continuity e il Clusit ne é licenziatario. Potete trovare informazioni su questo tema su:
http://www.clusit.it/bci/

Nel sito del BCI si trovano le Good Practce Guidelines del 2008, che possono essere viste come approfondimento della BS 25999. Sicuramente interessanti. (Grazie a Franco Ferrari del DNV per la segnalazione)
http://www.thebci.org/gpgdownloadpage.htm

Sempre grazie a Franco Ferrari, vi segnalo una versione italiana ferma però al 2005. Si può scaricare direttamente dal link
http://www.thebci.org/GPGItalian.pdf

ISO PAS 22399:2007

Franco Ferrari del DNV Italia mi segnala la norma ISO PAS 22399 "Societal security - Guideline for incident preparedness and operational continuity management".

Come si vede, la norma ha ormai 2 anni, ma può essere interessante vedere come anche qui si parli finalmente di BCM non solo legato all'IT.

****
09- Novità tecnologiche

Check list di sicurezza

Il NIST ha da tempo attivato un portale con le check list di sicurezza. Va detto che io trovo la navigazione di questo portale un po' ostica. Quando si parla di hardening, però, queste linee guida del NIST possono essere utili.
http://checklists.nist.gov/

Visto che il portale del NIST è ostico, è stata appena pubblicata una revisione della guida per la redazione e la lettura di queste checklist di sicurezza.
http://csrc.nist.gov/publications/PubsSPs.html#800-70

Acronimi

Sempre il NIST ha pubblicato un report sugli acronimi utilizzati nell'ambito della sicurezza informatica. Evidentemente, gli stessi statunitensi, maniaci degli acronimi in ogni circostanza, hanno dei problemi con questo loro modo di fare.
http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7581

Linee guida per i firewall

Sempre in ambirto NIST, segnalo la pubblicazione della revisione 1 della SP 800-41 "Guidelines on Firewalls and Firewall Policy". Un documento da leggere e studiare.
http://csrc.nist.gov/publications/PubsSPs.html#800-41

****
10- Notizie e storie

Da SANS Newsbyte segnalo l'interessante causa intentata negli USA dalla società Patco contro la banca Ocean Bank.

In pochissime parole, l'azienda, dopo aver perso quasi 600mila dollari a causa di transazioni fraudolente, accusa la banca di non aver previsto sufficienti misure di sicurezza per impedire questi eventi.

Non so se in Italia siamo messi così male da un punto di vista bancario, ma è sicuro che non tutti i fornitori di servizi forniscono sufficienti livelli di sicurezza.

http://voices.washingtonpost.com/securityfix/2009/09/construction_firm_sues_bank_af.html

Sempre da SansNewsbyte, segnalo la ricerca condotta sullo standard PCI DSS. In particolare, il 70% dei rispondenti vede la certificazione PCI DSS come un mero "mettere le crocette nelle caselle". Altre risposte sono interessanti, a mio parere non solo in ambito PCI, ma più in generale per tutte le certificazioni: è anche responsabilità degli auditor e degli Organismi di Certificazione e Accreditamento fare in modo di non ridurre gli audit alle sole check list. Purtroppo, in questo campo si passa da un eccesso all'altro: alcune volte sono richieste agli auditor delle competenze eccessive per il lavoro che fanno, altre volte si richiede loro solo di passare un esame e di compilare ogni anno 8 o 9 moduli inutili per mantenere la propria certificazione. Non è certo facile trovare una via di mezzo per garantire la presenza di auditor capaci di fare un buon lavoro, ma certamente oggi siamo ancora lontani.

http://www.darkreading.com/security/attacks/showArticle.jhtml;?articleID=220100919&subSection=Attacks/breaches
http://www.computerworld.com/s/article/9138427/PCI_survey_finds_some_merchants_don_t_use_antivirus_software?source=rss_security
http://www.theregister.co.uk/2009/09/23/data_security_survey/
http://lastwatchdog.com/pci-compliance-ineffective-stopping-data-thieves/

****

11- Statistiche

Segnalo questo interessante report sugli attacchi informatici. Come sempre, queste ricerche vanno lette con attenzione, visto che spesso sono più uno strumento di pubblicità per chi le pubblica che un vero e proprio elaborato scientifico (e infatti negli ultimi mesi ve ne ho già segnalate altre di ulteriori società di consulenza).
http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

****

12- Supply chain e qualifiche AEO

Questa segnalazione nasce da un articolo di Boselli, Jonathan, Paolino e Siciliano di KPMG Advisory su ICT Security del settembre 2009.

Per gli operatori di supply chain, è possibile richiedere la qualifica di AEO. Questa qualifica è come una certificazione di sicurezza e legalità dell'operatore. Lo schema è ufficiale e promosso dall'Unione Europea.

Come tutti gli schemi di certificazione, lo status è raggiungibile a seguito di un audit che include alcuni controlli della ISO/IEC 27001.

Per maggiori dettagli:
- http://www.agenziadogane.it/wps/wcm/connect/ed/Agenzia/Operatore+Economico+Autorizzato+AEO/
- http://ec.europa.eu/taxation_customs/customs/policy_issues/customs_security/aeo/index_en.htm

_____

Cesare Gallotti
Ripa Ticinese 75
20143 Milano (Italy)
Tel: +39.02.58.10.04.21
Mobile: +39.349.669.77.23
Web: http://www.cesaregallotti.it
Mail: cesaregallotti@cesaregallotti.it