Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – DICEMBRE 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

****

00 - Editoriale

Con un po' di ritardo rispetto al previsto, invio la newsletter di dicembre e ne approfitto per augurare buone feste a tutti i lettori.

****

01- Standardizzazione: ISO 31004 - Guida alla ISO 31000

Franco Ferrari mi ha segnalato l'uscita della ISO/TR 31004 dal titolo "Risk management — Guidance for the implementation of ISO 31000".

Francamente, mi sembra strano che esista una guida per una linea guida (la ISO 31000 ha titolo " Risk management — Principles and guidelines") e, in effetti, la sua lettura non mi sembra illuminante.

Gran parte di essa (10 pagine su 36) è dedicata a riflessioni sugli 11 principi del risk management e un'altra parte rilevante (8 pagine) è
dedicata al monitoraggio e al riesame del rischio.

****

02- Standardizzazione: Prassi UNI sulle Infrastrutture Critiche

Franco Ferrari del DNV Italia mi ha segnalato questo articolo dell'UNI dal titolo " Prassi di riferimento sulle Infrastrutture Critiche: al via la consultazione pubblica":
- http://www.uni.com/index.php?option=com_content&view=article&id=2528:prassi-di-riferimento-sulle-infrastrutture-critiche-al-via-la-consultazione-pubblica&catid=111:generale&Itemid=546

Riporto, per comodità, questo breve estratto: "Il documento è strutturato per essere applicato a organizzazioni, siano esse titolari o gestori di Infrastrutture Critiche che operano nel settore dell'energia e dei suoi sottosettori (elettricità, petrolio, gas) e nel settore trasporti e nei suo sottosettori, così come indicati nella Direttiva 2008/114/CE del Consiglio Europeo, ma può essere altresì applicato ad altri settori in cui l'Infrastruttura Critica potrebbe trovarsi a operare".

Visto che l'IT è un'infrastruttura critica, anche se non (ancora) riconosciuto come tale dal Dlgs 61 del 2011, la lettura di questo documento potrebbe essere interessante.

La bozza è scaricabile (per ora):
- http://www.uni.com/index.php?option=com_content&view=article&id=1354:le-prassi-di-riferimento&catid=149&Itemid=1439&showall=&limitstart=8

****

03- Standardizzazione: ISO/IEC 20000 parte 5 e 10

Franco Ferrari del DNV Italia mi ha segnalato la pubblicazione della ISO/IEC TR 20000-5 dal titolo " Exemplar implementation plan for ISO/IEC 20000-1".

Propone un approccio a fasi per attuare i requisiti della ISO/IEC 20000-1. Può essere una lettura interessante, anche se ciascuno dovrebbe sviluppare un approccio adatto alle caratteristiche dell'organizzazione in cui si vuole attuare la ISO/IEC 20000-1.

Per chi dovesse avere già la versione del 2011, l'introduzione della nuova versione dice che l'aggiornamento ha riguardato solo l'allineamento alla versione del 2011 della ISO/IEC 20000-1. Ho notato però che è stata aggiunta un'appendice di 12 pagine dal titolo "Templates".

La ISO/IEC 20000-10 dal titolo "Concepts and terminology" è invece alla prima edizione e riporta le definizioni comuni delle norme della serie ISO/IEC 20000, alcune considerazioni in merito, una descrizione degli altri standard della stessa famiglia, oltre a quelli ad essi collegati (tra cui la 27001).

****

04- ISO Survey 2012

L'ISO ha pubblicato la survey delle certificazioni 2012. Riguarda 9001, 14001, 27001, 13485, 22000, 50001 e 16949. Non ci sono proprio tutti (avrei voluto avere dei dati anche sulla ISO/IEC 20000), ma già così è interessante:
- http://www.iso.org/iso/home/standards/certification/iso-survey.htm

La notizia è arrivata via newsletter del DNV (ma senza il link alla pagina ufficiale dell'ISO!), di cui potete leggere il commento in italiano:
- http://www.dnvba.com/it/information-resources/news/Pages/ISO-Survey-2012.aspx

****

05- Legale: Privacy e call center extra-UE (riflessioni)

A fine ottobre avevo segnalato il Provvedimento del Garante relativo ai call center siti in Paesi extra-UE:
- http://blog.cesaregallotti.it/2013/10/privacy-e-call-center-extra-ue.html

Alessandro Alberici di Econocomm mi ha però fatto notare che questo Provvedimento pone dei problemi. In particolare, esso si applica "a tutti i soggetti [...]che svolgono in qualità di titolare del trattamento [...]un'attività di call center [...] in maniera prevalente". Quindi, se una società vende pc e l'assistenza telefonica è offerta da personale extra-UE, questo Provvedimento non si applica?

Io direi di sì (ossia: non si applica), ma vorrei capire se ci sono posizioni diverse.

****

06- Minacce e attacchi: ENISA Threat Landscape 2013

Dal gruppo LinkedIn Italian Security Professional, ricevo notizia della pubblicazione del "ENISA Threat Landscape 2013 - Overview of current and emerging cyber-threats":
- https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats

La segnalazione è accompagnata dal seguente articolo riassuntivo:
- http://securityaffairs.co/wordpress/20423/cyber-crime/enisa-threat-landscape-2013.html

Lettura decisamente interessante, che suggerisco.

****

07- Minacce e attacchi: 2013 Horizon Scan Report

Un'altra ricerca sulle minacce. Questa è proposta dal The Business Continuity Institute con il BSI:
- http://www.thebci.org/index.php/download-the-2013-horizon-scan-report

Essa è basata sulle percezioni dei partecipanti ed è possibile parteciparvi accedendo dalla home page del BCI (http://www.thebci.org/)

****

08- Minacce e attacchi: Attaccata la wi-fi del Parlamento Europeo

Dal SANS NewsBites giro la seguente notizia. La wi-fi del Parlamento Europeo è stata attaccata in modo da intercettare le comunicazioni:
- http://www.zdnet.com/european-parliaments-network-hacked-public-wi-fi-network-shutdown-7000023733/
- http://news.techworld.com/security/3491268/european-parliament-cuts-wi-fi-after-french-researcher-breaks-into-email-accounts/

Questo per ricordarci quanto le wi-fi siano insicure.

****

09- Contromisure: Studi sicurezza apps

Contromisure: Studi sicurezza apps

Più o meno in contemporanea ho ricevuto notizia di due studi sulla sicurezza dei sistemi di pagamento delle app per dispositivi mobili.

Il primo è stato segnalato da Enzo Ascione di Intesa Sanpaolo e riguarda la bozza di raccomandazioni della Banca Centrale Europea dal titolo "Recommendations for the security of mobile payments". Riguarda i pagamenti in mobilità in generale, ma le app sono ovviamente il tema più approfondito.

La pagina da dove si può scaricare la bozza sembra nascondere il documento; si trova a destra piccino piccino e ha il titolo "Draft recommendation":
- http://www.ecb.europa.eu/press/pr/date/2013/html/pr131120.en.html

Il secondo, segnalato dal Clusit Group di LinkedIn, è uno studio del Joint Research Centre of European Commission (JRC) dal titolo The MobiLeak. Segnalo la tesi di Pasquale Stirparo, collegata allo studio, dal titolo "MobiLeak: A System for Detecting and Preventing Security and Privacy Violations in Mobile Applications":
- http://kth.diva-portal.org/smash/record.jsf?searchId=1&pid=diva2:664617

L'intervista a Pasquale è decisamente interessante:
http://www.agendadigitale.eu/ecommerce/574_quanti-buchi-nelle-app-delle-banche-lo-studio-ue.htm

****

10- Contromisure: Linee guida 2013 Agid per il Disaster Recovery

L'Agenzia per l'Italia digitale ha pubblicato l'edizione 2013 delle "Linee guida per il disaster recovery delle pubbliche amministrazioni". Si trovano a questo indirizzo:
- http://www.digitpa.gov.it/fruibilita-del-dato/continuita-operativa

Il documento è notevole e contiene molte informazioni interessanti Certamente è discutibile l'impaginazione e l'ordinamento degli argomenti. In generale, si trovano molte riflessioni sulle normative in vigore e sono assenti delle linee guida su come effettuare una Business impact analysis e/o un Risk assessment. Ci sono però molte altre cose interessanti, anche se frutto ci copia-incolla o sintesi da altri documenti.