Cesare Gallotti

From: Cesare Gallotti [cesaregallotti@cesaregallotti.it]
Sent: Saturday, 16 January, 2010 10:25
To: cesaregallotti@cesaregallotti.it
Subject: IT Service Management News del 16 gennaio 2010

****
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 o disiscriversi o scrivendo a cesaregallotti@cesaregallotti.it o seguendo le istruzioni riportate nella pagina http://www.cesaregallotti.it/newsletter.htm. L'informativa sul trattamento dei dati personali è alla pagina http://www.cesaregallotti.it/newsletter.htm.

****
Indice

****
00- Miei interventi futuri

Il 17 febbraio a Milano e il 3 marzo a Roma presenterò per l'AIEA (www.aiea.it <outbind://82-00000000B5ADC49B8CF0E64D8B298394C693433DE4FE2E00/www.aiea.it>) la metodologia VERA. Sarà più un'occasione per discutere sullo stato dell'arte dei risk assessment per la sicurezza delle informazioni. Cercherò di fare un intervento più interessante e sostanzioso di quelli che normalmente sentiamo quando sono presentate le survey annuali di varie società su questo tema.

****
01- Standard e framework

ISO/IEC 31010

La ISO/IEC 31010:2009 "Risk management – Risk assessment techniques" è lo sforzo di ricondurre ad un massimo comun denominatore le tecniche di risk assessment utilizzate in contesti diversi (sicurezza delle informazioni, sicurezza degli impianti, sicurezza delle persone, eccetera).

Presenta più di 30 tecniche di risk assessment: ce ne sono di utilizzabili in tutte le fasi del risk assessment o solo in alcune e ci sono tecniche utilizzabili in tutti i contesti (per esempio il "brainstorming") o solo in uno specifico (per esempio l'HACCP).

Comprendere altre tecniche, seppure tradizionalmente non utilizzate per la sicurezza delle inoformazioni, può essere utile per evitare di riproporre un'unica metodologia (spesso basata su questionari e interviste one-to-one) anche dove questa risulterebbe inefficace.

Bisogna sforzarsi di essere creativi e non aver paura di introdurre cose nuove. Racconto sempre del mio stupore quando un'azienda mi illustrò il proprio metodo di risk assessment basato su tecniche Delphi, mai vista nel contesto della sicurezza delle informazioni; però i risultati sono risultati convincenti e la metodologia più che adeguata alla cultura aziendale in cui si inseriva. (L'esempio è anonimo, a meno che l'autore mi autorizzi a citarlo).

ISACA RiskIT

E' stata pubblicata la versione definitiva del Risk IT dell'ISACA.
http://www.isaca.org/Template.cfm?Section=Risk_IT&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=79&ContentID=48749
<http://www.isaca.org/Template.cfm?

Section=Risk_IT&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=79&ContentID=48749>

Attualmente, si compone di più documenti, spesso tra loro ridondanti. Io consiglierei di iniziare dal "Risk IT Framework", in cui sono descritti i 9 processi (suddivisi a loro volta in attività) del risk management. L'approccio è un po' più pragmatico di altri documenti di questo genere. Purtroppo, la terminologia è sottilmente diversa da quella usata dalle norme ISO, ma sappiamo bene che è pratica comune delle associazioni adottare una terminologia lievemente diversa dalle altre.

****

02- Novità Privacy

Dalla newsletter del Garante della Privacy dell'11 gennaio 2010, segnalo 2 notizie. A cui dovrei aggiungere che finalmente la newsletter ha dato conto (seppure in fondo e con 2 righe ciascuna) anche di notizie su provvedimenti "importanti".

Il Garante ha rinnovato le autorizzazioni generali per i dati sensibili. Per ora, non le ho ancora trovate sul sito del Garante, ma non dovrebbero differire da quelle di inizio 2008
http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Normativa%2FItaliana%2FAutorizzazioni+del+Garante%2F2008 <http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Normativa%2FItaliana%2FAutorizzazioni+del+Garante%2F2008>

Sono state pubblicate le Linee guida in tema di referti on-line
http://www.garanteprivacy.it/garante/doc.jsp?ID=1679033 <http://www.garanteprivacy.it/garante/doc.jsp?ID=1679033>

****

03- Computer Forensics

Sequestro di siti web

Dalla Newsletter di Filodiritto: la Cassazione ha ritenuto legittimo il sequestro preventivo del sito web Privatebay.
http://www.filodiritto.com/index.php?azione=archivionews&idnotizia=2231 <http://www.filodiritto.com/index.php?azione=archivionews&idnotizia=2231>

Prospettive del digital forensics

Due articoli di Marco Mattiucci:
- Prospettive del digital forensics: http://www.marcomattiucci.it/htc.php <http://www.marcomattiucci.it/htc.php>
- Copia forense dei dati: http://www.marcomattiucci.it/copy.php <http://www.marcomattiucci.it/copy.php>

****

04- Incident Management

Sul magazine "ENISA Quarterly Review, 4th Quarter 2009" (https://www.enisa.europa.eu/publications/eqr/issues <https://www.enisa.europa.eu/publications/eqr/issues>) si discute di incident management per le reti di comunicazioni.
Qui, "incident management" viene riduttivamente inteso come "major incident management" o "business continuity management". Una volta capito l'ambito, però, si vorrano scaricare le good practices dell'ENISA per studiarle ed estenderne i concetti a tutti i tipi di business.

Le guide le trovate all'indirizzo:
http://www.enisa.europa.eu/act/res/policies/good-practices-1/good-practices <http://www.enisa.europa.eu/act/res/policies/good-practices-1/good-practices>

Suggerisco di andare direttamente nella sezione "Prepardeness Exercises":
http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises <http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises>

****

05- Indicatori di sicurezza

Vista la recente pubblicazione della ISO 27004, la Newsletter HSC di gennaio 2010 dà alcuni link a presentazioni e documenti sugli indicatori di sicurezza. Alcuni degli indicatori risentono dell'origine "consulenziale": non sono interessanti e richiedono troppe risorse per raccoglierli. Ma ogni realtà ha le proprie esigenze e la propria cultura e un po' di esempi non fanno male.

Tutto in francese.

ANSSI : "Elaboration de tableaux de bord SSI", 02/04
http://www.ssi.gouv.fr/IMG/pdf/tdbssi-memento-2004-02-05.pdf <http://www.ssi.gouv.fr/IMG/pdf/tdbssi-memento-2004-02-05.pdf>

Cigref : "Guide pratique pour un tableau de bord sécurité stratégique et opérationnel", 10/07
http://cigref.typepad.fr/cigref_publications/RapportsContainer/Parus2007/tableau_bord_securite/Tableau_bord_Securite_2007.pdf <http://cigref.typepad.fr/cigref_publications/RapportsContainer/Parus2007/tableau_bord_securite/Tableau_bord_Securite_2007.pdf>

Clusif : "Les métriques dans le cadre de la série ISO 27000", 05/09

http://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-Metriques-dans-27000.pdf
<http://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-Metriques-dans-27000.pdf>

HSC/HS : "ISO 27004 : Métrage et métrique pour un SMSI", 04/06
http://www.hsc.fr/ressources/presentations/clusif-iso27004/ <http://www.hsc.fr/ressources/presentations/clusif-iso27004/>

****

06- Violato l'algoritmo A5/1

La notizia di violazione dell'algoritmo crittografico A5/1 utilizzato dalla rete GSM è riportata da molte newsletter. La prima a darmela è stata quella di perfezionisti.it (nella persona di Davide Fichera).

La notizia (in italiano):
http://www.ilsole24ore.com/art/SoleOnLine4/Mondo/2009/12/hacker-codice-gsm.shtml?uuid=8e09be06-f519-11de-ac8b-164065c89034&DocRulesView=Libero <http://www.ilsole24ore.com/art/SoleOnLine4/Mondo/2009/12/hacker-codice-gsm.shtml?uuid=8e09be06-f519-11de-ac8b-164065c89034&DocRulesView=Libero> .

Il sito del ricercatore
http://reflextor.com/trac/a51 <http://reflextor.com/trac/a51>

****

07- Tool di Project Management

Navigando un po' ho trovato questo sito sui tools di Project Management, con anche cose gratuite.

Per un consulente free-lance o per una piccola azienda, può essere conveniente presentare dei GANTT senza dover spendere i 139 Euro di licenza di MS Project. Ci sono anche soluzioni più ambiziose, che permettono di gestire grandi progetti non solo da un punto di vista organizzativo, ma anche economico.
http://airtodo.sourceforge.net/links.html#other_pm_tools <http://airtodo.sourceforge.net/links.html#other_pm_tools>

Ne approfitto per riportare una riflessione, sentita qualche mese fa durante una presentazione, che condivido: dopo un intervento dal pubblico finalizzato a presentare un tool super-sofisticato, il relatore rispose che secondo lui i migliori strumenti di analisi e gestione sono un programma di videoscrittura, uno di fogli di calcolo e... la propria testa.

****

08- Virus

Il mio antivirus mi ha segnalato questo trojan horse... qualcuno mi sa aiutare?
http://www.sampsonuk.net/B3TA/TrojanHorse.jpg <http://www.sampsonuk.net/B3TA/TrojanHorse.jpg>

(Da CRYPTO-GRAM, December 15, 2009)

****

09- Cybersecurity in USA

Su SANS NewsBites Vol. 11 Num. 100 viene segnalato un articolo di Melissa Hathaway, sui falsi miti sulla cybersecurity. La sua analisi, visto che è una collaboratrice di Barak Obama, benché non nuova per chi già si occupa della materia, merita una lettura.
http://blog.executivebiz.com/five-myths-about-cybersecurity/6102 <http://blog.executivebiz.com/five-myths-about-cybersecurity/6102>