****
IT SERVICE MANAGEMENT NEWS - GIUGNO 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- Standardizzazione - Andamento delle norme della famiglia ISO/IEC 270xx
02- Standardizzazione - ISO 22301 sui Business continuity management systems
03- Standardizzazione - Common Criteria 3.1
04- Attacchi - Furto delle password da LinkedIn
05- Attacchi - Flame
06- Normativa - Privacy & telecomunicazioni: pubblicati i Dlgs 69 e 70 del 2012
07- Normativa - Obbligo di aggiornamento delle notizie pubblicate online
08- Articolo "Everyone Has Been Hacked. Now What?"
09- Come scrivere i documenti
10- Usare il cloud in sicurezza - Una mia presentazione
11- VERA 3.0 ITA

****
01- Andamento delle norme della famiglia ISO/IEC 270xx

Ecco qui la situazione delle norme della famiglia ISO/IEC 270xx dopo l'incontro di Stoccolma del SC 27 di metà ottobre 2012:
- ISO/IEC 27000: è attualmente allo stadio di DIS
- ISO/IEC 27001: rimarrà allo stadio di CD; si suppone di rilasciarla in stadio di DIS a ottobre, poi in aprile 2013 come FDIS, per pubblicare la nuova versione della ISO/IEC 27001 a ottobre 2013
- ISO/IEC 27004 (misurazione dei controlli): ne è stata lanciata la revisione
- ISO/IEC 27006 (norma per gli Organismi di Certificazione ISO/IEC 27001):
ne è stata lanciata la revisione
- ISO/IEC 27013 (relazioni tra ISO/IEC 27001 e ISO/IEC 20000-1): è ora in stato di FDIS e dovrebbe quindi essere rilasciata ad ottobre
- ISO/IEC 27014 (Governance of information security): è ora in stato di FDIS e dovrebbe quindi essere rilasciata ad ottobre
- ISO/IEC TR 27015 (linee guida per i Financial Services): è ora in stato di DTR (corrispondente allo stadio DIS)
- ISO/IEC 27036 (gestione fornitori): è allo stato di CD; questa norma è in
3 parti, la seconda delle quali mi pare essere certificabile
- ISO/IEC 27037 (digital evidence): è allo stato di Final Draft, dovrebbe essere quindi pubblicata entro fine 2012
- ISO/IEC 27041, 27042 e 27043 (sulla computer forensics): sono allo stadio di Committee Draft
- ISO/IEC 24762 (linee guida sul DR): è stata avviata la revisione

Sono attualmente in corsi degli studi per le norme su: Capability Maturity Framework for Information Security Management, Privacy / Personal Information Management Systems, Information Security within Smart Grid Environments, International Certification of Information Security Management Specialists.

Al di fuori delle norme della famiglia ISO/IEC 270xx, anche se di pertinenza del SC27, ho notato che sono in corso i lavori (ora allo stadio di Working
Draft) per la ISO TS 30104, dal titolo "Physical security attacks, mitigation techniques and security requirements". Pare interessante, viste alcune richieste del mercato in tal senso.

Fabio Guasconi, Presidente del comitato SC 27 di Uninfo, mi ha fatto notare che lo stato delle norme sopra indicato, per quanto sembri corretto, sarà da verificare quando sarà emessa la roadmap aggiornata.

****

02- Standardizzazione - ISO 22301 sui Business continuity management systems

Il 15 maggio 2012, l'ISO ha pubblicato la ISO 22301 dal titolo "Business Continuity management systems – Requirements".

Si tratta di uno standard certificabile, che sostituisce la BS 25999-2:2007. Ricordo che questo standard riguarda i Sistemi di gestione per la continuità operativa, applicabile ad ogni tipologia di attività e non solo all'IT.

Per chi fosse completamente a digiuno sulla materia, posso segnalare il "BCM statement" del BCI:
- http://www.thebci.org/index.php?option=com_content&view=article&id=62&Itemid=105

Altre norme correlate, ma non certificabili, sono:
- ISO/PAS 22399:2007 "Societal security - Guideline for incident preparedness and operational continuity management".
- BS 25777: 2008 "Information and communications technology continuity management - Code of Practice" (solo per l'IT, quindi)
- ISO/IEC 24762: 2008 "Guidelines for information and communications technology disaster recovery services" (sempre solo per l'IT)

Segnalo anche una pubblicazione correlata al BCM: la BSI PAS 200:2011 sul crisis management.

L'ho letta velocemente e, ovviamente, non l'ho ancora mai applicata. Tenendo conto di queste premesse, non mi pare ci siano importanti modifiche sostanziali a quanto già previsto dalla precedente BS 25999.

Grazie anche al documento "Moving from BS 25999-2 to ISO 22301" del BSI e alla presentazione fatta dal BSI Italia il 24 maggio a Milano (grazie a Max Cottafavi di Reply per la condivisione della conoscenza), provo ad elencare nel seguito i punti di interesse, con alcuni miei commenti:
- il testo si basa sulla ISO Guide 83, ossia su uno schema comune a tutte le norme dei sistemi di gestione (bisognerà poi vedere come sarà recepito dalla ISO 9001, ISO/IEC 27001, eccetera)
- l'adozione alla ISO Guide 83 implica che non si parli più di procedure documentate o registrazioni, ma di informazioni documentate
- l'adozione alla ISO Guide 83 implica che i requisiti per il miglioramento siano drasticamente ridotti; su questo punto credo ci sarà necessità di approfondimenti nei prossimi anni, anche dopo l'uscita della futura ISO 9001 tra qualche anno; si potranno comunque trovare le azioni preventive nelle "azioni volte ad affrontare rischi e opportunità"
- l'adozione alla ISO Guide 83 implica che vi sia un chiaro obbligo di prendere in considerazione le parti interessate e non solo l'organizzazione (azienda)
- l'interpretazione dei requisiti della ISO Guide 83 da parte del Technical Committee ISO/TC 223 (che non condivido) ha portato all'introduzione di due risk assessment: uno nella parte di pianificazione dove si parla di "issues" e uno propriamente detto; ci sarà da discutere nei prossimi anni
- l'adozione alla ISO Guide 83 implica che la norma non sia più impostata sul concetto di "BCM programme", ma sul concetto di "Sistema di gestione" e sul ciclo PDCA

- fornisce due definizioni per la stessa cosa: "Maximum acceptable outage (MAO)" e "Maximum tolerable period of disruption (MTPD)"; poi, nel corpo del testo, non ne usa neanche una (stranezze della standardizzazione)
- esplicita il concetto di "Minimum business continuity objective (MBCO)", ossia di livelli minimo di servizi da ripristinare a seguito di un'interruzione delle attività
- esplicita la necessità di dare delle priorità alle diverse attività di ripristino (Prioritized timeframes), simile ma non uguale al ben noto termine di RTO
- approfondisce alcune aree quali: valutazione dei rischi, comunicazione, gestione degli incidenti (costruendo così un collegamento tra eventi "ordinari" e straordinari)
- introduce il concetto di "ritorno alla normalità",

Il documento del BSI si trova al seguente link:
- shop.bsigroup.com/upload/Shop/22301-Transition-Guide.pdf

La ISO ha in programma per "fine 2012 o inizio 2013" la pubblicazione della ISO 22313, guida alla realizzazione di un BCMS. Immagino che anche il The BCI modificherà le sue GPG.

Per la transizione: gli audit sulla ISO 22301 potranno essere condotti dal 1 novembre 2012 (anche per garantire la disponibilità di tempo per modificare le procedure e la formazione di tutte le parti coinvolte), non potranno più essere effettuati audit sulla BS 25999 dopo il 31 dicembre 2013 e tutti i BCMS certificati dovranno essere conformi alla ISO 22301:2012 ento fine 2014.

Ringrazio quanti, nei giorni scorsi, mi hanno preannunciato l'uscita di questa norma; ho preferito comunque darne notizia solo quando disponibile sul sito della ISO (www.iso.org).

****

03- Standardizzazione - Common Criteria 3.1

I Common Criteria, detta in pochissime parole, sono uno standard internazionale (ISO/IEC 15408, dal 2009 alla versione 3.1) per la valutazione della sicurezza dei prodotti e sistemi IT.

La materia non è banalissima, anche perché, come tutte le certificazioni, si basa su dei concetti non facili da capire ad un primo approccio.

Per chi fosse interessato, raccomando la lettura di questo articolo (segnalatomi da Stefano Ramacciotti del Ce.Va. Difesa), in cui sono descritte le caratteristiche dello schema, insieme alle critiche che sollevano:
- http://www.difesa.it/SMD/Staff/Reparti/II-reparto/CeVa/pubblicazioni/estere/Documents/CommonCriteria_ISSA%20Journal_0411.pdf

Stefano mi ha anche segnalato una sua presentazione del 2009. Si trova nello zip del seminario tecnico "Le novità nel campo degli standard per la sicurezza It" tenuto al Security Summit 2009; il file di interesse è "10.06.09_Ramacciotti.pdf" con la presentazione dal titolo "I Common Criteria 3.1 ad un anno di distanza dalla loro entrata in vigore. Cosa è cambiato dalla versione 2.3 alla 3.1R2".
- http://roma.securitysummit.it/upload/file/Seminari/Seminario-Clusit-10-giugno.zip

Per saperne ancora di più, segnalo il portale dedicato proprio ai Common Criteria:
- http://www.commoncriteriaportal.org/

****

04- Attacchi - Furto delle password da LinkedIn

La notizia è nota: è stato dichiarato che sono state compromesse 6 milioni e mezzo di password di utenti di LinkedIn. Io ho modificato la mia non appena avuta la notizia:
- https://mashable.com/2012/06/06/6-5-million-linkedin-passwords/ <https://mashable.com/2012/06/06/6-5-million-linkedin-passwords/>

Poco dopo, LinkedIn ha pubblicato un post, spiegando cosa è successo e come ha reagito:
- http://blog.linkedin.com/2012/06/06/linkedin-member-passwords-compromised/
<http://blog.linkedin.com/2012/06/06/linkedin-member-passwords-compromised/>

In pochissime parole: hanno confermato, hanno spiegato che stanno ancora investigando il caso, hanno spiegato agli utenti con password compromessa che il loro account è stato bloccato e che riceveranno una mail con la procedura per la riattivazione, hanno informato tutti che hanno realizzato un miglioramento alla sicurezza, si scusano con gli utenti.

Un comunicato di 242 parole che mi è sembrato ben fatto: un ottimo esempio di gestione della crisi.

Mi hanno però fatto notare che questo comunicato non è stato inviato a tutti gli utenti di LinkedIn, ma solo quelli con le password compromesse. Un errore evitabile.

Un ulteriore articolo con alcuni approfondimenti (nella prima parte; poi c'è un insieme di nozioni teoriche forse non interessantissime):
- http://securityaffairs.co/wordpress/6205/hacking/linkedin-passwords-compromised-social-network-poisoning-other-risks.html

Ringrazio Vito Losacco per le segnalazioni.

****
05- Attacchi - Flame

In questi giorni, l'ambiente della sicurezza informatica è emozionato per il virus Flame. Non ho molto da dire in proposito, se non dare il link ad un ottimo articolo (segnalazione di Vito Losacco) e fare solo commento riassuntivo:
- http://www.wired.com/threatlevel/2012/05/flame/

Se ho capito bene, si tratta in realtà di un virus associato ad un toolkit: di per se, non è una grande notizia. La cosa interessante è che nessuno aveva ancora visto né il virus (e infatti, al 28 maggio, l'articolo dice che "Researchers aren't certain how Flame infects its initial target"; sembra però che sfrutti alcune vulnerabilità già note e forse altre non ancora note), né il toolkit (anche se il web ne è pieno; vuol dire che è stato appositamente programmato da zero). Per questi motivi, i ricercatori credono si tratti di uno strumento di spionaggio sviluppato da qualche Nazione.

Una cosa l'ho capita bene: questo virus è in circolazione dal 2007 o dal 2010 ed è stato scoperto solo oggi. Ancora una volta, un argomento per la mia piccola battaglia contro certi indicatori di sicurezza: le misure quantitative misurano quello che sappiamo, mentre l'elemento fondamentale, in questo campo, è quello che non abbiamo ancora visto.

Nota: i commenti all'articolo sono solo di tipo politico, sulla situazione in Medio-Oriente.

****

06- Normativa - Privacy & telecomunicazioni: pubblicati i Dlgs 69 e 70 del 2012

A fine maggio sono stati approvati e pubblicati i Dlgs 69/2012 e 70/2012, di recepimento delle Direttive 2009/136/CE e 2009/140/CE e con modifiche al Codice privacy (Dlgs 196/2003) e al Codice delle comunicazioni elettroniche (Dlgs 259/2003).

Le novità riguardano i "fornitori di servizi di comunicazione elettronica".

Per quanto riguarda il Codice Privacy, il Dlgs 69/2012 prescrive quanto segue:
- esplicita richiesta di protezione dei dati relativi al traffico ed all'ubicazione e degli altri dati personali archiviati o trasmessi dalla distruzione anche accidentale, da perdita o alterazione anche accidentale e da archiviazione, trattamento, accesso o divulgazione non autorizzati o illeciti
- limitazione agli accessi del fornitore ai dati e ai dispositivi dei propri clienti
- richiesta di segnalare al Garante ogni violazione di dati personali
- richiesta di segnalare agli interessati ogni violazione di dati personali che possa arrecare pregiudizio ai dati personali (se capisco correttamente, questo caso si differenzia dal primo nel caso in cui i dati compromessi non siano intellegibili dai non autorizzati)
- richiesta di mantenere un registro delle violazioni di dati personali
- i subfornitori dovranno comunicare gli eventi al fornitore, in modo che poi segnali l'evento al Garante e, ove necessario, agli interessati (tra l'altro, qui accenno solo al fatto che questa misura conferma la mia interpretazione sul fatto che i fornitori non devono essere necessariamente Responsabili esterni; ma questa è un'altra storia)

Per quanto riguarda il Codice delle comunicazioni elettronico, il Dlgs 70/2012 prescrive quanto segue:
- misure di controllo del mercato, incluse richieste di interoperabilità
- l'adozione di specifiche misure di sicurezza (saranno stabilite dal Ministero dello sviluppo economico)
- la comunicazione al Ministero di violazioni della sicurezza o perdita dell'integrità significative ai fini del corretto funzionamento delle reti o dei servizi
- la creazione di un CERT nazionale
- la necessità di sottostare a verifiche della sicurezza da parte del Ministero dello sviluppo economico
- argomenti da inserire nei contratti

Il Dlgs 69/2012 introduce anche una misura per quanto riguarda le comunicazioni indesiderate, richiedendo che il mittente o il chiamante sia riconoscibile e che eventuali riferimenti a siti web devono essere a siti conformi alle prescrizioni del Dlgs 70 del 2003.

Una riflessione finale: questi Decreti valgono per i "fornitori di servizi di comunicazione elettronica", ossia per i fornitori di "servizi consistenti... nella trasmissione di segnali su reti di comunicazioni elettroniche...". Mi pare siano quindi esclusi i fornitori di servizi applicativi quali email o simili. Dovrei pensare a lungo se si tratta di un peccato o di una fortuna.

Ringrazio Fabrizio Monteleone per una prima segnalazione (auspicando l'adozione della 27001 dagli operatori di TLC, con un mio corollario anche alla ISO/IEC 27011), Max Cottafavi di Reply per una seconda segnalazione e Daniela Quetti della DFA per avermi dato i riferimenti precisi dai due Decreti Legislativi.

****

07- Normativa - Obbligo di aggiornamento delle notizie pubblicate online

Dalla newsletter della DFA, segnalo questo interessante articolo dal titolo "Diritto all'oblio: Cassazione ne conferma il riconoscimento", sulla Corte di Cassazione che ha imposto l'obbligo per gli editori di aggiornare gli archivi online delle notizie pubblicate.

Il caso è semplice: una persona accusata negli anni '90 di corruzione è stata successivamente prosciolta. Purtroppo per lei, sul web e sui motori di ricerca sono ancora facilmente reperibili i vecchi articoli, senza che questi siano accompagnati da un aggiornamento della vicenda.

La Cassazione ha appoggiato la lamentela: è necessaria una misura che consenta l'effettiva fruizione della notizia aggiornata, non essendo sufficiente la mera generica possibilità di rinvenire all'interno del «mare di internet» ulteriori notizie concernenti il caso di specie, ma richiedendosi la predisposizione di sistema idoneo a segnalare (nel corpo o a margine) la sussistenza nel caso di un seguito e di uno sviluppo della notizia.

La notizia
-
http://www.altalex.com/index.php?idu=193118&cmd5=21b8ec335692c54d0cada421fb338bae&idnot=56769

****
08- Articolo "Everyone Has Been Hacked. Now What?"

Simone Tomirotti mi segnala questo articolo di Wired che suggerisce di: "learning to live with the threat, rather than trying to eradicate it, is the new normal. Just detecting attacks and mitigating against them is the best that many companies can hope to do. (...) We have to manage the way we assess the risk".
- http://www.wired.com/threatlevel/2012/05/everyone-hacked/
<http://www.wired.com/threatlevel/2012/05/everyone-hacked/>

Sempre Simone fa alcuni commenti:
- Wired non è una rivista indirizzata verso la cultura del controllo, ma punta verso l'innovazione, eppure anche tra le loro colonne la soluzione è "valutare il rischio";
- negli USA c'è bisogno di un "FBI's former top cyber-cop", che sottolinei l'importanza del risk assessment;
- c'è vita dopo l'auditing

Dopo aver letto questa segnalazione di Simone, ho trovato una riflessione di Bruce Schneier molto simile nella newsletter Crypto-Gram a fronte di un articolo di Kelly Jackson Higgins (si tratta, in realtà, di una serie di articoli sullo stesso tema; quello segnalato è il secondo):
- http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/232800395/damage-mitigation-as-the-new-defense.html

****

09- Come scrivere i documenti

Le procedure non devono essere prodotti di alta letteratura, anche se alcuni redattori hanno velleità artistiche.

La scrittura di procedure deve rispondere ai criteri di chiarezza, precisione, uniformità, semplicità, economia.

Per questo ci sono delle regole che dovrebbero essere studiate e seguite: inizialmente con qualche sforzo, poi sempre più facilmente. L'individuazione di cosa scrivere costituisce il processo creativo del redattore di procedure, non la scelta di caratteri, colori e parole non diffuse.

Lungi dal propugnare la diffusione della neo-lingua di Orwell, condivido le premesse e le conclusioni di chi, in questi anni, ha scritto delle regole per la redazione dei testi normativi. Sappiamo bene che non sono stati molto seguiti, ma molti dei principi esposti sono applicabili alle nostre finalità:
- frasi brevi
- evitare la forma passiva dei verbi
- evitare frasi negative e non usare mai le doppie negazioni
- ripetere i termini senza paura
- evitare le maiuscole
- inserire prima le decisioni prese e poi la loro giustificazione
- eccetera

Duole dirlo, ma alcuni non dovrebbero solo studiare le regole di stile, ma tornare a studiare l'italiano, ad esempio l'uso dei congiuntivi e della virgola che non deve mai essere tra soggetto e verbo se non per inserire degli incisi.

Purtroppo, da nessuna parte viene riportato un principio fondamentale: avere un lettore spietato.

Sul web ho trovato queste interessanti e veloci letture, con utili esempi:
- "Progetto di semplificazione del linguaggio - Manuale di stile" (si trova con un qualsiasi motore di ricerca)
- "Regole e suggerimenti per la redazione dei testi normativi":
http://www.consiglio.regione.toscana.it/leggi-e-banche-dati/Oli/Manuale/man-ed-3.asp
- "Il progetto per la semplificazione del linguaggio amministrativo":
http://www.mef.gov.it/documenti/open.asp?idd=4500

Infine, segnalo il sito della Rete per l'eccellenza dell'italiano istituzionale (solo la prima lettera è in maiuscolo, come da regole):
- http://ec.europa.eu/dgs/translation/rei/

****

10- Usare il cloud in sicurezza - Una mia presentazione

Il 24 gennaio tenni un intervento dal titolo "Usare il Cloud in sicurezza: spunti tecnici" per il "Cloud seminar" organizzato da Assintel a Milano il 24 gennaio 2012.

E' un riassunto delle cose già dette in diversi contesti sulla materia, seguito da qualche mia riflessione in merito a tutto questo parlare di cloud e non parlare del resto.

La presentazione è ora pubblicata sul mio sito web:
- http://www.cesaregallotti.it/Pdf/Pubblicazioni/2012-Presentazione-Cloud.pdf

****

11- VERA 3.0 ITA

Dopo aver ricevuto qualche richiesta, ho tradotto VERA in italiano. Fanno eccezione i titoli dei controlli della 27001, perché la traduzione ufficiale in italiano non mi convince appieno.

Ho colto l'occasione anche per cambiare parecchie cose, tra cui:
- le istruzioni sono cambiate
- ora le caselle di incrocio tra controllo e minaccia non riportano solo la "X", ma il livello di rischio calcolato
- nel foglio principale, sull'estrema sinistra si trova il livello di rischio corrispondente ad ogni singolo controllo

Rimane sempre un metodo non user-friendly (o non stupid-proof, se volete...), ossia per persone abbastanza esperte della materia. Per renderlo più fruibile, è comunque possibile modificarlo un po' senza troppa fatica.

Lo potete scaricare da questo link:
- http://www.cesaregallotti.it/Pdf/Pubblicazioni/2012-VERA-3.0-ITA.xls