****
IT SERVICE MANAGEMENT NEWS – OTTOBRE 2010
****

Newsletter mensile con novità in materia di sicurezza delle informazioni, IT Service Management, Qualità.

E' possibile iscriversi o disiscriversi
- scrivendo a cesaregallotti@cesaregallotti.it
- seguendo le istruzioni riportate nella pagina http://www.cesaregallotti.it/newsletter.htm

Sulla stessa pagina è possibile consultare l'informativa sul trattamento dei dati personali.

****
Indice

****
01- Novità standard famiglia ISO/IEC 27000

Da Fabio Guasconi, Presidente Commissione SC27 di Uninfo.

Lunedì 11 novembre si è concluso il meeting del SC27 (comitato internazionale incaricato della revisione delle norme della famiglia ISO/IEC 27000) a Berlino.

In anteprima ed in estrema sintesi, i punti salienti emersi nel meeting:

- i commenti a 27001 e 27002 sono stati così numerosi che nessuno dei due gruppi è riuscito a visionarli tutti. Nel primo caso si è proceduto per priorità e nel secondo per ordine
- l'annex A della 27001 rimane al suo posto nonostante i continui tentativi di spostarlo
- la 27001 adotterà il nuovo formato del JTC per i sistemi di gestione (che poi diventerà comune a tutte gli standard ISO sui sistemi di gestione)
- ci sarà una nuova norma sul Cloud Computing
- avrà inizio la revisione della ISO/IEC 27006 (quella applicabile agli Organismi di Certificazione)
- la 27007 (sull'auditing degli ISMS) avanza a FCD
- la neo uscita IEC 62443 (SCADA) verrà revisionata per essere allineata con la 27001
- la revisione della 27005 (Linee guida per il risk assessment) per allinearne i termini alla 31000 è allo stato di FDIS (final draft, quasi la versione finale tranne errori editoriali)
- la 27016 sugli elementi economici della gestione della sicurezza è partita

****

02- Standardizzazione: Business Continuity

Dalla newsletter del Disaster Recovery Institute, segnalo l'articolo "The shifting sands of business continuity management": http://www.continuitycentral.com/feature0812.html

Questo articolo confronta le norme
- BS 25999 e NFPA 1600 (basate sul solo "ripristino del business"),
- SPC.1-2009 (che richiede anche di prevenire gli incidenti e di mitigarne gli effetti)
- la nuova AS/NZS 5050:2010 (basata sul risk management).

Sembra ci sia molto dibattito in materia.

Per leggerle:
- SPC.1-2009 (free): http://www.asisonline.org/guidelines/ASIS_SPC.1-2009_Item_No._1842.pdf
- NFPA (free): http://www.nfpa.org/assets/files//PDF/NFPA16002010.pdf
- BS 25999-2 (a pagamento): http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030169700&t=r
- AS/NZS 5050:2010 (a pagamento): http://www.standards.co.nz/web-shop/?action=viewSearchProduct&pid=5050%3A2010%28AS%7CNZ%29&mod=catalog
- AS/NZS 5050:2010 DRAFT (free): http://www.calamityprevention.com/links/AS-NZS-5050-Part-1-Specification.pdf

****

03- An Excel Based Risk Assessment Methodology

Ho trovato interessante questa metodologia basata su Excel. In alcuni punti, più complicata del necessario, in altri troppo semplicistica (io terrei conto delle vulnerabilità e i parametri di riservatezza e integrità sembrano sottovalutati). La soluzione è comunque interessante.
http://www.17799.com/modules.php?name=Papers&pa=showpage&pid=6

****

04- Attacchi IT e perdite economiche

Da SANS NewsBites Vol. 12 Num 76: la Corte Suprema dello Stato del Maine ha stabilito che l'azienda Hannaford Bros (la cui banca-dati con i numeri di carte di credito dei clienti è stata violata) non deve riconoscere alcunché ai clienti che non hanno subito alcun danno diretto (cioè, perdite economiche a causa di uso fraudolento del numero della propria carta).

Ovviamente, tali clienti hanno subito danni indiretti, visto che hanno dovuto impiegare un po' del loro tempo per chiedere la sostituzione della propria carta. Ma questi non dovranno essere riconosciuti.

http://www.computerworld.com/s/article/9187340/Maine_court_limits_damage_claims_in_data_breach_cases?source=rss_news

La sentenza mi lascia perplesso. Inoltre, deduco che uno dei messaggi più utilizzati per vendere sicurezza ("negli USA eventuali attacchi possono costare molti soldi") non potrà più essere utilizzati.

****

05- Tecnologia Microsoft: EMET

Sul forum di discussione del Clusit su LinkedIn è stata data la notizia che il 14 settembre la Microsoft ha pubblicato un tool di hardening dei sistemi denominato EMET.

L'articolo in italiano: http://sicurezza.html.it/articoli/leggi/3475/aumentiamo-la-sicurezza-dei-programmi-windows-con-emet-20/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+HTML.it+-+Articoli

La pagina della Microsoft: http://www.microsoft.com/downloads/en/details.aspx?FamilyID=c6f0a6ee-05ac-4eb6-acd0-362559fd2f04

****

06- Novità legali

Il 30 luglio, il Consiglio dei Ministri ha approvato il Dlgs di modifica del Codice della Proprietà Industriale. Per ora non è stato ancora pubblicato in Gazzetta Ufficiale, ma può essere utile comprenderne le novità con questo articolo:
http://www.filodiritto.com/index.php?azione=visualizza&iddoc=1955

Da Filodiritto, segnalo l'articolo "Fine del telefax nell'èra della PEC?", dove è ribadita l'importanza della PEC anche per il miglioramento dell'efficienza della Pubblica Amministrazione.
http://www.filodiritto.com/index.php?azione=visualizza&iddoc=1964

Intanto, aziende private continuano a chiedermi di inviare moduli firmati e scannerizzati via mail. Chi dice che il privato è sempre più avanti della PA?

In materia di Privacy, il 10 Giugno il Garante ha vietato ad una società di utilizzare i file pornografici memorizzati sul pc di un proprio dipendente per avallare la decisione di licenziamento. Ancora una volta, perché l'informativa non è risultata ben scritta.
http://www.filodiritto.com/index.php?azione=visualizza&iddoc=1962&newsfrom=2634

****
07- Verifica sull'operato degli Amministratori di Sistema

Dopo una interessante discussione con Vito Losacco di Engineering, ho elaborato la mia proposta di check list per la verifica dell'operato degli AdS secondo quanto richiesto dal Provvedimento del Garante.

Secondo Vito, è troppo lunga.

Se avete proposte di migliorie, comunicatecele!

http://www.cesaregallotti.it/art_pres/20100920-Checklist-AdS.pdf

****
08- Gestione progetti

Su Computer World è stato pubblicato un interessante articolo dal titolo "Progetti di CRM, qualche suggerimento per ridurre le perdite di tempo". Non è applicabile ai soli progetti CRM e quindi molto interessante.

http://www.cwi.it/knowledge-center/2010/07/01/progetti-di-crm-qualche-suggerimento-per-ridurre-le-perdite-di-tempo/

****
09- Sicurezza delle applicazioni

Quasi sempre è difficile trovare correttamente documentati i requisiti di sicurezza delle applicazioni. Lungi il voler imporre il modello waterfall, ma troppe volte in fase di analisi non si sa "quali requisiti considerare". E' quindi improbabile che siano documentati in maniera coerente.

Alcuni standard (come la ISO/IEC 15408 "Common Criteria") presentano metodologie e specifiche molto dettagliate. La ISO/IEC 15408 è una norma divisa in 3 parti per un totale di circa 650 pagine. Sicuramente, in molte situazioni è troppo onerosa.

La metodologia OWASP (www.owasp.org) è invece orientata alle applicazioni e ai servizi web. E' comunque consigliabile la sua lettura anche a chi si occupa di altre tipologie di applicazioni.

Io mi sono permesso di elaborare un ulteriore elenco di requisiti da consierare, basati sui punti dell'allegato A della ISO/IEC 27001:
- i requisiti legali applicabili
- considerazioni sulla capacity (quanti utenti utilizzeranno l'applicazioni? quanto spazio disco sarà utilizzato? ...)
- considerazioni sulla disponibilità

- quali meccanismi crittografici per la connessione degli utenti e degli amministratori e come configurarli
- quali meccanismi di sicurezza per la connessione dell'applicazione con altre applicazioni
- quali meccanismi di identificazione e autenticazione per utenti e amministratori (userid e password? con quali regole di complessità, scadenza, modalità di modifica da parte degli utenti, ripristino, eccetera?)
- quali meccanismi di autorizzazione per gli accessi ai dati (controllo accessi, gestione dei ruoli e profili utente)
- quali meccanismi di log (login, logout, azioni degli utenti)
- come validare gli input e gli output e avere la garanzia che i dati siano elaborati correttamente (anche in considerazione delle potenziali vulnerabilità)
- come gestire il patching
- gli impatti sui sistemi di backup e sul Business Continuity Management (impatti sui sistemi del sito di Disaster Recovery e sulle procedure di gestione degli incidenti)
- gli impatti sul service desk (è necessario aggiornare gli operatori?)
- gli impatti sulla configurazione dei firewall
- gli impatti sui sistemi di monitoraggio e discovery (per esempio, se è necessario riconfigurarli)
- il ruolo dei fornitori

Ovviamente l'elenco è migliorabile, ma da qualche parte bisogna iniziare (se avete idee...).

****

10- Interventi di Cesare Gallotti

Il 5 ottobre ho tenuto un'intervista per Salotto Tecnologico su "Sicurezza delle informazioni, privacy e organizzazione: che deve fare una PMI per ottenere risultati concreti?". Sono quasi 50 minuti...
http://www.salottotecnologico.it/video.cfm?idVideo=19&id=2

Il 30 novembre interverrò ai GS Days di Parigi (http://www.club-27001.fr/) su "Appréciation conjointe ISO 27001 et ISO 20000-1"