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

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

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.htm

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

****
Indice

****
01- Blog della newsletter

E' attivo il blog della newsletter su http://blog.cesaregallotti.it

Ogni suggerimento su come migliorarlo è benvenuto.

Inoltre, lancio una domanda: a qualcuno interessa la pubblicazione della newsletter in formato epub, oppure il formato email è più che sufficiente?

****
02- Risk Assessment: Mehari 2010

Dalla Newsletter del Clusit si apprende che è stata pubblicata la versione 2010 della metodologia Mehari. La precedente era del 2007.

Mehari è una metodologia "classica" di risk assessment e segue completamente i passi previsti dalla teoria, espressa ufficialmente anche dalla ISO/IEC 27005.

La sua implementazione può risultare eccessivamente onerosa per motivi che ho già espresso altrove.

D'altro canto, la metodologia è intesa come "operativa" e presenta delle scelte ben precise e degli esempi rispetto al modello necessariamente astratto delle norme ISO. Sono ben definite le vulnerabilità e cosa si intende con questo termine, è proposto un elenco di circa 800 minacce di dettaglio da affiancare alle 40 "generali", i controlli di sicurezza della ISO/IEC 27002 sono rinominati "servizi di sicurezza" e riclassificati fino ad arrivare al numero di circa 350 (la 27002 ne propone 133, variamente aggregati), a loro volta ulteriormente dettagliati nelle tabelle di analisi e ben spiegati in uno specifico documento.

Accanto a tutto ciò, è messo a disposizione un foglio di calcolo di supporto.

La lettura è dunque interessante e istruttiva. Oltre ad essere gratuita.

Tutta la documentazione è disponibile in francese ed inglese su
https://www.clusif.asso.fr/fr/production/ouvrages/type.asp?id=METHODES.
L'introduzione alla metodologia, in italiano, è disponibile su
https://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Introduzione-Italiano.pdf

****

03- Sicurezza: Il trasferimento dei rischi

La Newsletter del Clusit del 31 ottobre 2010 segnala un articolo di Riccardo Salici sui rischi trasferibili al mercato assicurativo.

L'articolo presenta una premessa generale di 2 pagine, in cui sono riepilogate le caratteristiche del mercato assicurativo collegato ai rischi informatici. E' interessante rilevare come sia suggerita, come attività di risk assessment, una "valutazione tecnico-assicurativa proveniente da un settore che di eventi imponderabili se ne intende, al contrario di altri".

Certo mi fa riflettere come in tutti questi anni non abbia mai assistito a presentazioni da parte delle assicurazioni per illustrare, anche brevemente, i metodi utilizzati. Salici giustifica la cosa scrivendo: "In genere gli assicuratori tengono riservati i loro calcoli e le stime dei rischi residuali nei confronti dei clienti per evitare di passare per i "giona" della situazione". Io rimango con il dubbio (sempre pronto ad essere contraddetto) che questi attori non abbiano strumenti sufficientemente maturi da essere esposti ed, eventualmente, criticati. Rimane il fatto che, sicuramente, una valutazione tecnico-assicurativa svolta da persone con una sensibilità diversa rispetto a consulenti, personale interno o tecnici informatici, possa portare elementi utili alla valutazione del rischio e alle conseguenti scelte di trattamento.

Al termine del documento, sono riportati i "Rischi tipicamente trasferiti al mercato assicurativo". Qui l'elenco può confondere chi è attaccato alla terminologia ISO/IEC 27000 perché confonde rischi, danni e minacce.

L'annuncio del Clusit termina con la seguente frase: "Inoltre, Riccardo ci sta mettendo a disposizione una vasta panoramica di sinistri realmente avvenuti e trattati dalle Assicurazioni. Non mancheremo di condividere queste informazioni (ovviamente anonimizzate) con la nostra community".

In attesa di questo materiale, ci si può leggere l'articolo liberamente disponibile su www.clusit.it/docs/rscalici_10-10-26.pdf.

****

04- Business Model for Information Security (BMIS)

Dalla newsletter dell'ISACA, segnalo la recente pubblicazione del "Business Model for Information Security (BMIS)". E' scaricabile gratuitamente da http://www.isaca.org/bmis.

Lo confesso: quando leggo un articolo sulla sicurezza e trovo la parola "olistico" (o un suo derivato, o "a 360 gradi"), parto prevenuto. Sarà perché sento gli stessi concetti da più di 10 anni, magari con altre parole, e non mi trovo a mio agio con modelli sempre più complicati, apparentemente "nuovi" che dicono sempre la stessa cosa: "la sicurezza non è solo tecnologia, non è solo reazione agli incidenti, non è solo materia tattica o operativa, richiede l'appoggio di tutta l'azienda e in particolare della Direzione, deve fondarsi sulla cultura aziendale, eccetera". L'esperienza conferma che questi concetti non sono però recepiti da tutti.

Questo BMIS non fa eccezione alla regola: usa diffusamente il termine "olistico", presenta un modello abbastanza complicato, ricorda molti principi noti da tempo come se fossero "nuovi". E' comunque scritto bene, con buoni esempi e quindi forse utile a chi ha ancora dei dubbi sulla materia.

Aggiungo un'ulteriore nota amena: spero che a breve questi documenti vengano anche diffusi in formato epub e non solo in pdf, visto che gli e-reader si stanno sempre più diffondendo e rendono la lettura agevole senza dover stampare (però il pdf è difficilmente convertibile in epub).

****

05- Quali manager per quale progetto?

Circola ancora la voce che "un buon manager può fare il buon manager in qualunque realtà". Ho visto diversi manager all'opera e ho imparato che non è vero, ma spesso incontro perplessità di fronte al mio convincimento.

Un manager, per quanto bravo, ha le proprie inclinazioni e le proprie competenze, non applicabili ad ogni realtà. Perché ogni realtà si basa su una cultura interna e agisce in un mercato con le sue precise particolarità, non sempre assimilabili a quello di provenienza del manager (mi ricordo sempre di alcuni dirigenti, provenienti dalla vendita di software, che chiedevano quante licenze aveva venduto la business unit "consulenza").

In questo articolo, Gianfilippo Cuneo racconta le stesse cose, ma con note tecniche preziose
http://www.fbritaly.it/articolo.php?aId=0000000043&n=Quali+manager+per+quale+progetto%3F

Ringrazio Gianni Signa di Itnet per la segnalazione.

****

06- Verifica sull'operato degli Amministratori di Sistema (Rev1)

Con Vito Losacco di Engineering, abbiamo elaborato una proposta di check list per la verifica dell'operato degli AdS secondo quanto richiesto dal Provvedimento del Garante.
http://www.cesaregallotti.it/art_pres/20100920-Checklist-AdS.pdf

Ogni proposta di miglioramento sarà la benvenuta.

****

07- Vulnerabilità delle applicazioni di ebanking per smart phones

Dal SANS NewsBites Vol. 12 Num. 89: "Alcuni ricercatori hanno trovato bachi di sicurezza in 6 applicazioni di ebanking (sulle 7 analizzate) per Android e iPhone; in particolare, hanno scoperto che i dati di accesso sono conservati in chiaro".
http://www.wired.com/threatlevel/2010/11/bank-apps-for-phones/
http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=228200291&cid=RSSfeed_IWK_News

Come sempre, si tratta di mancanza di una decorosa pianificazione dei requisiti di sicurezza a livello applicativo. Possiamo pubblicare tutti gli standard e le best practices che vogliamo, ma non serviranno a nulla, se il 90% dei project manager vedono la documentazione come "inutile sovraccarico di lavoro".

****

08- Stuxnet

In questi giorni si parla molto del work Stuxnet, che attacca le PLC, ossia gli strumenti di controllo elettronici degli impianti.

L'articolo più approfondito è quello di Bruce Schneier:
http://www.schneier.com/blog/archives/2010/10/stuxnet.html

Accanto alle sue riflessioni, ne aggiungo due mie:
- viste le sue modalità di propagazione, è opportuno ricordare la misura che prevede di isolare certi sistemi critici dal resto della rete
- sembra che sfrutti le password di admin di alcune PLC della Siemens e che queste non possano essere modificate, contrariamente a tutte le regole di buona sicurezza (i signori della Siemens sono in nutrita compagnia di altri prodotti, utilizzati in contesti assai critici, che possono girare solo con l'utenza di admin e non consentono agli Amministratori di Sistema di accedere con altre utenze)

****

09- Sicurezza delle applicazioni (REV. 1)

[Ripubblico l'articolo già uscito in novembre sulla sicurezza a livello applicativo, grazie anche ai suggerimenti di Fabrizio Monteleone del DNV Italia]

Quasi sempre è difficile trovare correttamente documentati i requisiti di sicurezza delle applicazioni. Anche senza voler imporre un modello waterfall, i troppi esempi di incidenti collegabili allo sviluppo non ben controllato suggeriscono di documentarli in maniera coerente. Ho riscontrato spesso la scarsità di idee su "quali requisiti considerare".

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 (http://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.

Si propone qui di seguito un ulteriore ma breve elenco di requisiti da consierare, basati sui punti dell'allegato A della ISO/IEC 27001:

- i requisiti legali applicabili
- le necessità di capacity a livello tecnologico: potenza, spazio disco e banda di rete dedotte dal numero di utenti previsti e dalla mole di dati che saranno coinvolti dalla loro operatività)
- le necessità di disponibilità dell'applicazione, anche in modo da disporre delle risorse necessarie al momento del go live
- i meccanismi crittografici (inclusa la loro configurazione) da prevedere per la connessione degli utenti e degli amministratori di sistema
- le connessioni con altre applicazioni in modo da prevedere gli opportuni meccanismi di comunicazione sicura
- i 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?)
- i meccanismi di autorizzazione per gli accessi ai dati (controllo accessi, gestione dei ruoli e profili utente)
- i meccanismi di log (login, logout, azioni degli utenti)
- le modalità di validazione degli input (controllo dei campi di input), degli output (messa a disposizione delle opportune query) e della loro corretta elaborazione (con quadrature o report periodici)
- il processo di gestione del 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) in modo da aggiornarli opportunamente
- gli impatti sul service desk, in modo da aggiornare gli operatori e i loro strumenti
- gli impatti sulla configurazione dei firewall
- gli impatti sui sistemi di monitoraggio e discovery, anche per riconfigurarli opportunamente
- il ruolo dei fornitori, in modo da controllarli in modo adeguato

Accanto a questi requisiti più tecnici, è opportuno riflettere sulle modalità di controllo dello sviluppo. Tra queste:

- "normali" procedure di project management: modalità di comunicazione tra le parti interessate, pianificazione, attribuzione responsabilità per i diversi deliverable, tempistiche per lo sviluppo e per il testing, verifiche e riesami periodici, ...
- regole di codifica sicura (basate sulle best practices esistenti)

- regole per il debugging
- modalità di separazione delle funzioni tra i soggetti che analizzano, progettano, codificano, testano, portano in esercizio...

****

10- Cloud computing

Franco Ferrari (DNV Italia) segnala le pubblicazioni del Cloud Security Alliance, scaricabili da http://www.cloudsecurityalliance.org/Research.html.

Il punto di partenza è la versione 2.1 del "Security Guidance for Critical Areas of Focus in Cloud Computing".

Inoltre, ricorda la pubblicazione dell'ENISA "Cloud Computing - Benefits, risks and recommendations for information security" scaricabile da http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

****

11- I benefici dell'IT Auditing

Simone Tomirotti mi segnala questo articolo sui 5 benefici dell'IT Auditing.
http://www.freebie-articles.com/Art/67813/368/The-Top-Five-Benefits-of-IT-Auditing.html

Simone commenta: "Non sono riuscito a capire chi sia questo fantomatico "John Welsh" e non credo dica nulla di nuovo. Però, l'articolo è chiaro e ci permette di ricordare i nostri obiettivi.

In sintesi, i 5 maggiori benefici del lavoro degli IT Auditor sono:
1. Ridurre il rischio
2. Rafforzare i controlli (e migliorare la sicurezza)
3. Conformarsi alla normativa
4. Facilitare la comunicazione tra il business e l'IT
5. Migliorare l'IT Governance

Con un po' di spirito polemico ci si potrebbe chiedere: questi 5 benefici interessano veramente le aziende?"

Io ho risposto dicendo che, durante gli audit, il pensiero dominante dell'azienda è "speriamo che non ci rompano troppo le scatole". Quindi, difficilmente avrà spazio per pensare ad altri benefini.

Simone quindi: "Vero; altre volte si prende l'audit come un esame ed alla fine ci si aspetta - a prescindere da tutto - un bel voto. Si pensa: "con le nostre forze/risorse abbiamo fatto tutto il possibile, dovete darci un voto alto!". Dimenticando quali sono i veri obiettivi di un audit.

Spesso, sia nel tuo caso che nel mio, la colpa sta nel mezzo: chi è oggetto dell'ispezione non ne sa gli obiettivi e chi fa l'auditor non ha tempo (voglia?) di spiegarli."

Concludo dicendo che il mestiere dell'auditor può essere frustrante, ma va fatto bene e ogni tanto dà buone soddisfazioni.

****

12- Business Continuity - Norma AS-NZS-5050

Massimo Cottafavi (Spike Reply), dopo l'articolo del mese scorso sul BCM, segnala il fatto che la norma AS-NZS-5050 è composta da più parti e che al link http://www.calamityprevention.com/links/ sono liberamente scaricabili i draft.

Anche il sito http://www.calamityprevention.com/, nel suo complesso, è interessante.

****

13- Prossimi interventi di Cesare Gallotti

Il 18 novembre, intervengo al convegno "Stanco di fare l'equilibrista - Lasciatevi condurre sul cammino sicuro verso una corretta IT Governance" organizzato da ECS (http://www.ecs-group.com/it/default.aspx) all'Hotel Boscolo Exedra di Roma (ore 10.45 - 17.00)
Il mio intervento avrà il titolo "IT Governance: scelte e soluzioni".

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