****
IT SERVICE MANAGEMENT NEWS - DICEMBRE 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

****
00- Editoriale

Come ogni anno, approfitto di questa newsletter per fare gli auguri di buone feste a tutti i miei lettori.

Questo mese, mi accorgo ora, siamo già in festa e le notizie sono molto poche. Cercando di non promuovere la quantità senza qualità, colgo comunque l'occasione per ricordarvi di segnarmi articoli o notizie interessanti.

Ci sentiamo a gennaio, sempre che dopodomani il mondo non finisca.
Cesare

****
01- Commenti sulla futura ISO/IEC 27001

Dopo i miei commenti del mese scorso sui cambiamenti previsti per la futura ISO/IEC 27001 ho ricevuto solo un commento scritto da parte di Andrea Veneziani di Data Management. Ho ricevuto anche alcuni commenti orali da altri, ma il risultato è sempre lo stesso.

Molti temono che la riduzione dei requisiti sull'analisi dei rischi possa comportare dei problemi e, in definitiva, lo schema attuale sarebbe preferibile. Tutti riconoscono comunque un aspetto: alcuni auditor e consulenti insistono a proporre schemi formali specifici che poi un'azienda non fa altro che lasciarli su carta.

Io penso che si dovrebbe fare una riflessione sulle linee guida della famiglia ISO/IEC 27000: ad oggi alcune sono troppo teoriche (vedere commento successivo), mentre altre sono troppo direttive, non lasciando spazio ad alternative. Se le linee guida della famiglia ISO/IEC 27001 fossero più pratiche, i dubbi sui requisiti della ISO/IEC 27001 forse scomparirebbero.

Non sono originale: è la stessa proposta che ha fatto UNI per la futura ISO 9001.

****

02- Standardizzazione: ISO/IEC 27032 sulla cybersecurity

Il 15 luglio è stata pubblicata la ISO/IEC 27032 dal titolo "Guidelines for cybersecurity".

Innanzitutto, ho trovato interessante la distinzione tra "Internet" e "Cyberspace", dove Internet è usato per indicare la parte fisica della rete, mentre il Cyberspace comprende anche i servizi disponibili. Insomma, normalmente il termine Internet è usato per le due accezioni, ma effettivamente bisognerebbe distinguere.

Lo standard è indirizzato agli utenti di servizi Internet (ops... servizi del ciberspazio) e ai loro fornitori.

Per i fornitori, sappiamo bene quante misure di sicurezza sono già presenti sulla 27001. Oltre a quelle, ne sono specificate alcune di relazione con i clienti, dedicate soprattutto alla loro sensibilizzazione sulla sicurezza. Un breve elenco di cose che mi sono segnato: fornire un canale di comunicazione per segnalare eventi e incidenti, fornire il software validato da certificati digitali, fornire manuali agli utenti, inviare agli utenti periodici messaggi di educazione sulla sicurezza, fornire ai clienti una guida per la configurazione del proprio pc, specificare i requisiti legali applicabili, mantenere un protocollo per garantire una mutua autenticazione del cliente e del fornitore, stabilire i contatti autorizzati per le comunicazioni. Infine, viene suggerito di ricordare ai clienti che non verranno mai chieste informazioni personali e credenziali di ogni tipo, né verranno inviati link via mail e che per collegarsi al servizio bisognerà farlo solo dal browser.

Utile, nell'Allegato B, un elenco di siti web dedicati alla sensibilizzazione degli utenti dei servizi del ciberspazio.

Lo standard è di 50 pagine, troppe sono dedicate a riflessioni teoriche, di modo che le indicazioni pratiche occupano in realtà poche pagine. Se consideriamo che il prezzo dello standard è proporzionale al numero di pagine, qualche riflessione critica viene spontanea.

****

03- Così vuoi fare l'auditor?

Simone Tomirotti mi ha segnalato questo articolo dal titolo "So You Want to Be an IT Auditor?":
- http://www.theiia.org/intAuditor/itaudit/2012-articles/so-you-want-to-be-an-it-auditor

E segnala la conclusione: la buona notizia per chi fa lo sforzo di studiare da auditor IT è che la richiesta di tali professionisti sta crescendo rapidamente. Secondo CNN Money, la contabilità e l'audit IT sono tra le professioni che stanno crescendo più rapidamente, con una crescita dal 2008 al 2012 stimata tra il 22% e il 30%. Le organizzazioni stanno cercando auditor IT professionisti per valutare e raccomandare metodi per mitigare gli impatti dei rischi tecnologici. Dimostrare il proprio desiderio di imparare e allargare le proprie capacità è la strada migliore per coloro che intendono intraprendere una carriere da IT auditor.

Da parte mia, condivido il fatto che "il desiderio di imparare e allargare le proprie capacità è la strada migliore". Questo vale per tutte le professioni.

Ma ho una domanda: perché devono essere gli auditor IT a trovare i rischi e indicare le strade per ridurli? perché devono essere gli auditor IT a individuare le vulnerabilità o cattive pratiche? non dovrebbero essere i project manager e gli analisti o, in alternativa, un dipartimento di sicurezza che offre i propri servizi di consulenza?

Vorrei dire che è uno strano mondo quello in cui si chiede ai verificatori di dare indicazioni (come chiedere ai giudici di fare le leggi... ma non vorrei che la mia newsletter e il mio blog si occupino di politica).

****

04- Foto del principe William con password

Questa mi è piaciuta molto: il principe William è stato fotografato in una base della RAF e, per un po' di marketing, le foto sono state pubblicate sul web.

Problema: sullo sfondo si trova un foglio con scritte user-id e password di un qualche sistema chiamato MilFlip.

A essere pedanti, si trovano un'infinità di problemi di sicurezza. L'articolo di questo post (segnalato dalla newsletter di DFA) assicura che la password è anche banale:
- http://nakedsecurity.sophos.com/2012/11/21/prince-william-photos-password/

****
05- Attacco Eurograbber

Questo lo ritengo interessante (da SANS Newsbyte): alcune banche usano il sistema di autenticazione forte basato su normale user-id e password e su un codice casuale inviato via SMS quando l'utente si connette o effettua qualche disposizione.

Si sono inventati un attacco facile facile da capire, ma difficile da realizzare: la vittima riceve una mail di phising e installa il malware Zitmo Trojan sul suo pc; questo rimane silenzioso e si attiva quando la vittima si connette al sito della sua banca (sono colpite anche banche italiane) e gli segnala di aggiornare anche il software sul cellulare, ovviamente con altro software dannoso.

Il primo software, quindi, intercetta le credenziali per accedere al sito di web banking, il secondo software sul cellulare intercetta il codice temporaneo. Con questi elementi, il malintenzionato può fare bonifici dal conto della vittima ad un suo proprio conto.

Sembra troppo complesso, ma Check Point dice che le vittime, finora, sono state 30.000 e hanno perso 47 milioni di dollari.

Un articolo: https://www.informationweek.com/security/attacks/zeus-botnet-eurograbber-steals-47-millio/240143837
Il report di Check Point:
http://www.checkpoint.com/products/downloads/whitepapers/Eurograbber_White_Paper.pdf