****
IT SERVICE MANAGEMENT NEWS - GENNAIO 2013
****

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

****
1- Standardizzazione: ISO 22313:2012 - Business continuity management systems - Guidance

Franco Ferrari del DNV Italia mi ha segnalato la pubblicazione, al 15 dicembre 2012, della ISO 22313 "Societal security — Business continuity management systems — Guidance". Si tratta della linea guida che accompagna la ISO 22301 (non capisco perché non l'abbiano numerata come ISO 22302, ma forse non è importante).

Si tratta di un documento di 58 pagine e costa 154 CHF (circa 125 Euro). L'ho sfogliato molto rapidamente e mi sembra ci siano diversi spunti interessanti, in particolare nel capitolo in cui si tratta dei requisiti per le risorse (persone, informazioni e dati, sedi e infrastrutture associate, apparecchiature e strumentazione, sistemi ICT, trasporti, liquidità economica, fornitori) e per le procedure (gestione operativa e strategica degli incidenti, comunicazione, sicurezza delle persone, continuità, ripristino dei sistemi ICT, ripristino delle attività).

Continuo però a pensare che sia preferibile lo studio della NIST SP800-34: 149 pagine gratuite, pubblicate da un prestigioso ente statunitense e con l'efficace stile che contraddistingue i manuali pubblicati negli USA.

****

2- Standardizzazione: Commenti sulla revisione della ISO/IEC 27001 e non solo

Fabrizio Monteleone del DNV Italia, oltre ad essere mio amico, ha una grande esperienza di audit ISO/IEC 27001. A fronte delle mie segnalazioni sulla futura ISO/IEC 27001 ha fatto qualche commento che riporto di seguito.

1- Riguardo la 27001 suggerirei, anche se ciò non è possibile, di promuovere la revisione dell'Annex A con i controlli a livello annuale o biennale al massimo: stiamo parlando di IT cioè di un mondo che evolve talmente in fretta, che i controlli da mettere in campo dovrebbero essere riesaminati per capire se in grado di accogliere quanto succede. Inoltre, anche la lista minacce e vulnerabilità dovrebbe essere sempre aggiornata dalle imprese; ma quanti la aggiornano? Se non spinti da uno standard, non lo farebbero mai.

2- Sull'analisi dei rischi, nel tempo ho visto si sono fatti strada alcuni metodi più o meno accettabilmente applicati (per lo meno, per il primo audit...). Dopo 7 anni siamo arrivati ad un livello di competenze accettabile. Ora, con il cambiamento delle carte, abbiamo dei rischi di confusione e di nuovi "esperti" che esperti non sono.

3- Per quanto riguarda l'impegno della direzione, purtroppo è vero che la Direzione è spesso latitante e non partecipa all'analisi e valutazione dei rischi.

4- Sul fatto che le linee guida siano linee e basta mi trovi in accordo. Dovrebbero essere in numero inferiore (quindi meno soldi) e solo tecniche (gli esempi sulle misure sono indecenti).

5- Per il resto, giustamente, se l'auditor fa l'auditor, i problemi sono dell'azienda o vogliamo che tra il valore aggiunto chiesto all'auditor ci sia quello di fare il consulente? La realtà è che le aziende se lo aspettano, visto che pagano...

****

3- Standardizzazione: Requisiti per le compagnie di sicurezza private

Max Cottafavi di Spike Reply mi ha segnalato la pubblicazione dello standard ANSI/ASIS PSC.1 per i "private security contractors".

Stiamo parlando di sicurezza fisica e più specificatamente delle forze armate private: tema estraneo a questa newsletter, ma non troppo.

Si tratta di uno standard di requisiti per un sistema di gestione, impostato secondo i nuovi e futuri standard ISO per i sistemi di gestione (vedere i commenti sulla futura ISO/IEC 27001). E' quindi richiesta una pianificazione basata sulla valutazione dei rischi, l'erogazione dei servizi in conformità con i risultati di questa valutazione, un monitoraggio e un approccio basato sul miglioramento continuo.

Cosa interessante: il ministero competente inglese (Foreign & Commonwealth Office) ha formalmente approvato ed avallato questo standard ASIS PSC.1.

Lo standard può essere reperito (costo di 165 USD) presso il sito dell'ANSI:
- http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI%2fASIS+PSC.1-2012#.UNhWEaywWSo

****

4- CERT Italia?

Dal blog di Over Security trovo un riferimento all'articolo "Cybersecurity, Italia pecora nera in Europa" del Corriere delle Comunicazioni.

L'articolo dice che "l'Italia farebbe figura di unico Paese Ue a non essersi dotato di un CERT nazionale", anche se "l'Agenda digitale europea esorta tutti i paesi membri a istituire i propri CERT".

Un CERT nazionale ha il ruolo di gruppo di risposta agli incidenti informatici a livello nazionale e dovrebbe anche identificare minacce e vulnerabilità e informarne gli addetti. Un CERT nazionale potrebbe anche diffondere statistiche su minacce e vulnerabilità (mi chiedo ancora chi possa pensare ad analisi quantitative dei rischi se non ha queste informazioni) e buone pratiche di configurazione e sviluppo dei sistemi e dei software.

La notizia si commenta da sola.

L'articolo del Corriere delle comunicazioni:
- http://www.corrierecomunicazioni.it/it-world/18802_cybersecurity-italia-pecora-nera-in-europa.htm

****
5- Accordi con i servizi esterni (cloud e social network)

Nella newsletter Crypto-Gram di Bruce Schneier del 15 gennaio 2013 c'è un interessante articolo sugli accordi (terms of service) stipulati con servizi cloud e social network:
- https://www.schneier.com/blog/archives/2012/12/terms_of_servic.html

Per capire meglio, vi segnalo questo articolo in italiano:
-
http://www.repubblica.it/tecnologia/2012/12/18/news/instagram_le_foto_diventano_pubblicit_la_mano_di_facebook_sulla_nuova_privacy-49014541/

Cosa è successo: Facebook ha acquistato a metà 2012 la società Instagram che fornisce dei servizi di archiviazione foto; a dicembre 2012 è stato emesso un nuovo accordo con gli utenti che lascia alla società molti più diritti su quanto archiviato dagli utenti rispetto all'accordo inizialmente sottoscritto. Questo ha scatenato molte proteste.

Bruce Schneier ha esteso la sua analisi anche al servizio cloud Prezi.

Le riflessioni conseguenti sono:
- qualcuno ha letto con attenzione l'accordo sottoscritto con il fornitore del servizio?
- questo accordo può essere tale per cui in futuro esso possa essere modificato unilateralmente e senza preavviso?

E poi mi si chiede perché non voglio sincronizzare il mio cellulare con i contatti e l'agenda Google...

****

6- Tecnologia: Protezione smartphones

L'U.S. Federal Communications Commission, come ho appreso dalla newsletter SANS Newsbyte, ha pubblicato delle linee guida per la protezione degli smartphones:
-
https://www.computerworld.com/s/article/9234928/FCC_offers_security_advice_to_smartphone_users?taxonomyId=17

Potete trovare le check list (con il solito stile basato su decaloghi) su:
- https://www.fcc.gov/smartphone-security

Queste linee guida mi sono piaciute perché in molti casi riportano link a tool per applicare alcune misure.

La sicurezza di questi oggetti è un problema per gli utenti e le imprese. In molti asseriscono che solo l'iPhone garantisce un buon livello di sicurezza, ma non ne sono convinto (sarà perché ho comprato il 3G, non più aggiornato dal 2010...).

****
7- Sentenza: Firma elettronica e digitale

Dalla newsletter di Filodiritto, segnalo la "Tribunale di Catanzaro - Sezione Prima Civile, Ordinanza 30 aprile 2012, n. 68/2011".

Tale sentenza stabilisce che non possono essere sottoscritte con "un semplice clic", corrispondente alla firma elettronica, le clausole vessatorie di un contratto. Queste dovrebbero essere sottoscritte con firma digitale o autografa.

Per gli interessati, segnalo l'articolo di Gianni Penzo Doria:
- http://filodiritto.com/index.php?azione=visualizza&iddoc=2980

Ho trovato più comprensibile questo articolo:
- http://www.laleggepertutti.it/12644_contratti-sul-web-inefficaci-tutte-le-clausole-vessatorie

Dagli articoli trovati, comunque, non ho capito quale fosse la materia del contendere. Sembra che il potere di eBay di escludere dei sottoscrittori a seguito di loro condotte inadempienti sia una clausola vessatoria. Mi sembra quindi che la sentenza abbia effetti ambivalenti sulla tutela dei consumatori (da una parte li garantisce, dall'altra riduce i poteri di controllo del fornitore del servizio).

Invito chiunque abbia maggiori dettagli a condividerli.

****
8- Attacchi: Ottobre rosso

Credo che il prossimo attacco di cui si parlerà tanto tanto sarà "Ottobre rosso".

Dall'articolo non ho capito come è stato possibile infettare le macchine; si capisce come l'attaccante sia riuscito a propagare l'attacco, ma non come sia riuscito a trovare la prima vittima. Eppure, sarebbe molto interessante.

L'analisi del Kaspersky Lab:
-
https://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies

****

9- Attacchi DDOS come "libera espressione"?

Sul gruppo "Clusit" su LinkedIn è stato pubblicato un post di Aldo Ceccarelli che segnala un articolo di Information Security News dal titolo "Anonymous chiede al governo Usa di riconoscere gli attacchi come libera espressione":
- http://www.informationsecuritynews.it/news/anonymous-chiede-al-governo-usa-di-riconoscere-gli-attacchi-come-libera-espressione

In sostanza, Anonymous dice che un attacco DDOS che blocca l'accesso a dei sistemi IT è equiparabile ad una manifestazione di piazza che blocca l'accesso agli edifici. Ma non è un reato anche quello?

****

10- Risk assessment: VERA 3.1

Gianluca Stretti mi ha segnalato un errore nelle istruzioni del VERA 3.0 italiano. In particolare, nelle istruzioni si diceva di dare valore 3 ad un controllo debole e valore 1 ad un controllo robusto. Il calcolo, però, prevedeva l'inversione di tali valori.

Bizzarro: nessuno l'aveva mai segnalato, eppure so per certo che qualcuno lo usa. Evidentemente, lo strumento è più intuitivo di quanto pensassi.

Ringrazio comunque Gianluca (che non conosco) per la segnalazione.