Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS - OTTOBRE 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 dis-iscriversi
- 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: Pubblicate le nuove ISO/IEC 27001 e 27002

Fabrizio Cirilli è stato il primo ad informarmi che sul sito ISO (www.iso.org) sono disponibili dal 25 settembre le nuove versioni delle norme ISO/IEC 27001 e 27002.

Evidentemente, l'ISO aveva molta fretta e non ha aspettato l'applauso finale del Meeting dell'SC 27 che si terrà a fine ottobre e che sancirà la fine dei lavori per la ISO/IEC 27001.

Il testo non riporta alcuna tabella di confronto tra la versione del 2005 e quella del 2013. Infatti, questa sarà oggetto di discussione al Meeting. Mi chiedo ora in quali modalità sarà pubblicata.

Molti hanno già pubblicato una bozza delle tabelle, di cui parlo sotto.

****

02- Standardizzazione: Materiale sulla ISO/IEC 27001:2013

Mi hanno segnalato del materiale informativo relativo alla ISO/IEC 27001:2013. Molto è tratto dalla documentazione discussa nel corso della redazione della ISO/IEC 27001 e può quindi valere la pena leggerlo, soprattutto per comprendere alcuni impatti introdotti dai cambiamenti.

I titoli delle pubblicazioni sono i seguenti:
- " Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013";
- "Mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013";
- "Checklist of Mandatory Documentation Required by ISO/IEC 27001 (2013 Revision)";
- "Diagram of ISO 27001 2013 Implementation Process".

Non condivido tutto quello che si trova in queste schede: alcune cose le avrei approfondite di più, altre di meno. Gli ultimi due sono proprio delle interpretazioni a volte molto libere della norma. Ma si tratta comunque di analisi valide, che vale la pena studiare.

Ci tengo però a dire che non trovo corretti i riferimenti incrociati tra nuova e vecchia ISO/IEC 27001 e 27002. Infatti, alcuni requisiti e controlli del 2005 sono dati per "cancellati", mentre molti (quasi tutti, per la verità) sono invece "incorporati" o "impliciti" in quelli del 2013.

E' infatti importante osservare che le norme sono più sintetiche in alcuni punti (soprattutto la ISO/IEC 27001) perché alcuni requisiti sono stati ritenuti "impliciti". In altre parle, è ora importante che gli utilizzatori della norma la studino con molta attenzione e dimostrino molta competenza.

Per concludere: non so se i documenti sono liberamente reperibili, ma se li trovate con un motore di ricerca vuol dire che, in qualche modo, lo sono...

****

03- Standardizzazione: PAS 99:2012 sui sistemi di gestione integrati

Franco Ferrari del DNV Italia mi ha segnalato la pubblicazione della PAS 99:2012, che sostituisce la versione del 2006.

Questa versione è in realtà una linea guida all'Annex SL, ossia alla struttura che dovranno rispettare tutte le nuove edizioni degli standard ISO di requisiti per i sistemi di gestione. Sull'Annex SL ho già parlato in precedenza per i suoi impatti sulla futura versione della ISO/IEC 27001.

Avevo anche segnalato una breve guida IRCA in merito:
- http://www.irca.org/en-gb/resources/Guidance-notes/Annex-SL-previously-ISO-Guide-83/

A mio parere, la PAS 99 non aggiunge molto a quella guida, tranne una riflessione sulla gestione generale dei rischi, ora richiesta quando si pianifica un sistema di gestione.

La guida è del 2012 e quindi non recepisce, per la ISO/IEC 27001, alcune scelte fatte nell'ultimo anno.

****

04- Legale: Dei delitti, delle contravvenzioni e della privacy nella 231 (errata corrige)

Paolo Cupola, che ringrazio molto, mi ha fatto notare il grossolano mio errore nel post "Privacy e 231":
- http://blog.cesaregallotti.it/2013/09/privacy-e-231.html

L'articolo 9 del DL 93 del 2013 inserisce nel Dlgs 231 del 2001 i delitti previsti dal Dlgs 196 del 2003 dall'articolo 167 all'articolo 172.

Nel Dlgs 231 del 2001 sono quindi riportati solo i reati di: trattamento illecito dei dati, falsità nelle dichiarazioni e notificazioni al Garante, inosservanza dei provvedimenti del Garante.

Nel Dlgs 231 del 2001 NON sono riportati i reati di: omissione di adozione delle misure minime di sicurezza, svolgimento di indagini sulle opinioni dei lavoratori, controllo a distanza dei lavoratori con impianti audiovisivi (questi ultimi sui lavoratori sono riportati dalla Legge 300 del 1970 a cui fa riferimento l'articolo 171).

Questo perché sono riportati nel 231 i "delitti" previsti dal Codice Privacy e non le "contravvenzioni". I "delitti" sono quelli che prevedono le sanzioni di morte, ergastolo, reclusione e multa, mentre le "contravvenzioni" sono quelle che prevedono le sanzioni di arresto e ammenda. Solo gli articoli 167 (trattamento illecito), 168 (falsità di dichiarazioni) e 170 (inosservanza dei Provvedimenti) parlano di "reclusione" (non prevedono "multe") e quindi sono "delitti". Gli articoli 169 (misure minime) e 171 (sui lavoratori, rimandando alla Legge 300 del 1970) parlano di "arresto" e "ammenda" e quindi sono "contravvenzioni" e pertanto non rientrano nel Dlgs 231.

Il riferimento è l'articolo 17 del Codice Penale.

Mi scuso con tutti per l'errore. Meno male che il DL non è ancora stato convertito in Legge e quindi forse non ho fatto troppi danni...

****

05- Legale: Articolo su privacy e 231

Riprendendo l'articolo precedente, segnalo questo articolo di approfondimento segnalato da CINDI dal titolo "Il trattamento illecito dei dati e la responsabilità dell'azienda", il cui merito, oltre ad un riassunto dei reati che potrebbero essere introdotti nella 231 (se il DL verrà convertito), è di presentare un esempio delle sanzioni:
- http://www.cindi.it/il-trattamento-illecito-dei-dati-la-responsabilita-dellazienda/

Mi permetto di fare una considerazione a cui ho pensato recentemente e collegandomi al testo dell'articolo stesso "fortunatamente, nell'ottica delle imprese, l'omessa adozione delle misure minime di sicurezza non rientra tra i reati presupposto del d.lgs. 231/01". Va detto che i Provvedimenti del Garante rientrano tra i reati presupposto del d.lgs. 231/2001 e molto spesso riepilogano le misure minime... di conseguenza non vedo molta fortuna per le imprese che ancora non applicano le misure minime.

****

06- Legale: Sanzioni per mancata iscrizione della PEC

Segnalo questo interessante articolo di CINDI relativo alle sanzioni economiche per le imprese che non hanno comunicato al registro delle imprese il proprio indirizzo di posta elettronica certificata:
- www.cindi.it/iscrizione-indirizzo-pec-registro-imprese-sanzioni/

****

07- Articolo sul caso NSA

Il The Economist del 14 settembre 2013 ha pubblicato un ottimo articolo di analisi sul caso NSA-PRIMS-Snowden e sulle sue conseguenze.

Ho trovato interessante soprattutto il paragrafo "Who cares?", dove sono spiegati gli impatti della vicenda (in sintesi, si dice che l'impatto più negativo l'hanno avuto i produttori USA di tecnologia, a causa dell'immagine negativa).

Ringrazio mio padre, Roberto Gallotti, per la segnalazione:
- http://www.economist.com/news/international/21586296-be-safe-internet-needs-reliable-encryption-standards-software-and

****

08- Minacce e attacchi: Report 2013 di Verizon

Dal gruppo infotechlegale.it di LinkedIn ricevo la notizia della pubblicazione del "2013 Data breach investigations report" di Verizon:
- www.verizonenterprise.com/DBIR/2013/

Il report è molto interessante. In particolare, analizza, per il 2012, le compromissioni di dati rilevate (dove gli attacchi da parte di esterni sono il 92%) e gli incidenti senza compromissioni (dove invece la maggioranza del 69% è stata causata da personale interno). Il report analizza i settori merceologici delle imprese coinvolte, i tipi di attaccanti, gli asset e i dati oggetto degli attacchi.

Ho trovato interessante anche le analisi sui tipi di attacchi adottati per le compromissioni e quelli per gli incidenti senza compromissioni (qui, gli agenti di attacco sono soprattutto gli interni e quindi errori e malware sono i più diffusi).

Sempre procedendo nella lettura del report, è curioso il paragone tra i dati relativi al malware analizzati da Verizon e da Microsoft: per Verizon, l'84% del malware è installato con l'aiuto degli utenti mentre per Microsoft solo il 45%. La differenza, per Microsoft, è dovuta ad errori di configurazione.

C'è però un neo: il report non si basa su alcun dato dall'Italia.

****

09- Minacce e attacchi: Amazon e l'errore del prezzo

La notizia è la seguente: Amazon ha messo in vendita un computer ad un prezzo sbagliato e molto basso. Ha quindi corretto il prezzo e ha comunicato agli acquirenti che il loro acquisto era annullato.

Notizia e commento di Andrea Monti:
- http://www.ictlex.net/?p=1473

Lo trovo molto pertinente e mi è piaciuta molto la conclusione: "E' regola generale nel diritto dei contratti che le parti – tutte e due – devono agire secondo buona fede". Purtroppo lo fanno in pochi...

****

10- Minacce e attacchi: Udine - compromesso il sito dell'azienda sanitaria

Sandro Sanna mi ha inviato questa notizia, a cui potremmo dare il titolo "A Udine violati i computer dell'Ass 4. On line i reclami dei malati" ed è in tre parti:
- http://messaggeroveneto.gelocal.it/cronaca/2013/10/07/news/a-udine-violati-i-computer-dell-ass-4-on-line-i-reclami-dei-malati-1.7881088
- http://messaggeroveneto.gelocal.it/cronaca/2013/10/10/news/assalto-informatico-insiel-noi-parte-lesa-1.7898761
- http://messaggeroveneto.gelocal.it/cronaca/2013/10/11/news/ma-quale-hacker-csi-ho-scoperto-i-reclami-all-ass-4-1.7903434

In poche parole: un utente dell'azienda sanitaria numero 4 vuole inviare un reclamo attraverso il loro sito web e si accorge di una piccola falla di sicurezza e la comunica ad un giornale on-line.

La "piccola falla" è piuttosto banale: l'applicazione non verifica se le pagine web sono richieste da un utente autenticato e quindi è sufficiente cambiare il numero di richiesta dall'URL e questa appare, a prescindere da chi l'ha fatta. Direi che rientriamo nella quarta vulnerabilità più diffusa secondo OWASP:
- https://www.owasp.org/index.php/Top_10_2013-A4-Insecure_Direct_Object_References

Mi chiedo se queste pagine sono almeno protette dagli spider di Google. E però ho trovato meraviglioso il fatto che Insiel, l'azienda che ha sviluppato il sistema, si è dichiarata parte lesa.

Ma sappiamo bene come vanno le cose: un prodotto sicuro costa di più di uno insicuro e quindi si opta spesso e volentieri per il secondo. Mi auguro che un qualche giudice multi l'Ass 4 per non aver fatto i controlli e Insiel per aver fatto male il proprio lavoro.

****

11- Minacce e attacchi: Uso di apparati KVM e furti in banca

Guido Uglietti mi ha segnalato il seguente articolo dal titolo "Barclays Bank computer heist: Eight arrested over £1.3m haul":
- http://www.independent.co.uk/news/uk/crime/barclays-bank-computer-heist-eight-arrested-over-13m-haul-8828844.html

In breve: 8 persone sono state arrestate per un furto di 1,3 milioni di sterline attraverso un attacco informatico.

La cosa interessante è come è stato condotto l'attacco: uno di essi si è presentato come tecnico informatico presso una filiale della banca in Svizzera; ha quindi collegato ad un PC un apparato "keyboard video mouse" (KVM) per intercettare le attività su schermo, tastiera e mouse; ha collegato il KVM ad un modem e poi ha raccolto (da casa?) tutti i dati necessari per il furto.

Insomma, è stata usata la buona vecchia tattica di presentarsi da qualcuno confidando che nessuno verifichi l'identità e la ragione della nostra presenza.

****

12- Cultura digitale: Deepweb and Cybercrime

Segnalo questa breve ricerca dal titolo "Deepweb and Cybercrime - It's Not All About TOR" della Trend Micro, segnalata sul gruppo Italian Security Professional di LinkedIn:
- http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-deepweb-and-cybercrime.pdf

Francamente, mi aspettavo un po' di più (ho sentito cose più approfondite durante il corso di Digital forensics della Statale di Milano). Ad ogni modo, è utile per aggiornarsi un po' sul sottobosco della criminalità
informatica.