Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS –GIUGNO 2014

****

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- Libro "Sicurezza delle informazioni"

Finalmente ce l'ho fatta e ho pubblicato il mio libro "Sicurezza delle informazioni". Si trova in formato pdf in alcune librerie on-line. Per il formato epub bisogna aspettare qualche giorno perché deve essere validato. Personalmente preferisco il formato pdf.

Nelle librerie che seguono c'è sicuramente, ma, quando il formato epub sarà validato, si troverà anche sui celeberrimi Amazon e Ibs:
- http://www.ultimabooks.it;
- http://libreriarizzoli.corriere.it
- http://www.bookrepublic.it
- http://www.deastore.com
- http://www.cubolibri.it
- http://www.hoepli.it

- http://www.libreriaebook.it
- http://www.biblonstore.it
- http://ebook.unita.it

La versione "giusta" è quella del 10 giugno e vi invito a guardare l'anteprima per vedere gli argomenti trattati (analisi del rischio, ISO/IEC 27001 e non solo) e quindi decidere se vi interessa.

L'ho pubblicato come self-publisher tramite la piattaforma Narcissus.me. Un nome un programma. Ed è stato molto divertente, anche se terribilmente faticoso.

****

02- Privacy e cookie - Provvedimento del Garante

Il Garante privacy, con Provvedimento Generale dell'8 maggio 2014, ha regolamentato l'uso dei cookie dei siti web:
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3118884

Ne faccio un brevissimo riassunto:
- per i cookie tecnici è richiesta l'informativa con le modalità più idonee;
- per i cookie di profilazione è richiesta l'informativa e il consenso; si può presentare all'utente solo un'informativa breve (banner), purché sia comunque disponibile un'informativa lunga.

Non mi pare cambi molto rispetto a quanto già fatto da molti siti web.

****

03- Google e diritto all'oblio - Sentenza

La notizia si è molto diffusa ed è questa: la Corte di Giustizia UE ha stabilito che un motore di ricerca è un titolare di trattamenti di dati personali e pertanto devono far sparire dalle ricerche le tracce della persona che vuole essere "dimenticata":
-
http://www.repubblica.it/tecnologia/2014/05/13/news/causa_contro_google_corte_ue_motore_di_ricerca_responsabile_dati-85985943/

Mi sto chiedendo se questo sia un bene (penso a persone accusate ingiustamente di cui rimane traccia per sempre senza alcun collegamento a notizie aggiornate) o un male.

Ad ogni modo, questa è la sentenza:
- http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62012CJ0131&qid=1401432812901&from=EN

e questo è un commento critico alla sentenza:
- http://www.filodiritto.com/note-critiche-alla-presunta-salvaguardia-del-diritto-alloblio-in-capo-a-chi-non-dovrebbe-e-non-potrebbe-il-motore-di-ricerca/

****

04- Social privacy - Guida del Garante

Franco Ferrari di DNV GL mi ha segnalato l'aggiornamento della pubblicazione del Garante della privacy dal titolo " Social privacy. Come tutelarsi nell'era dei social network":
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3140082

La pubblicazione è indirizzata ai "ragazzi", ma ci sono molti consigli utili ed è sicuramente utile anche agli adulti (alcuni miei contatti "professionali" su Facebook dovrebbero forse ricordarsi che non hanno chiesto l'amicizia solo ai veri amici...).

****

05- Uso di pc e mail aziendali per scopi personali - Sentenza

Enzo Ascione di Intesa Sanpaolo Group Services mi segnala una sentenza della Corte di Cassazione (sez. lav. - sent. 18.3.2014 n. 6222) la cui sintesi è: "L'uso di pc e mail aziendali per scopi personali non giustifica il licenziamento".

In poche parole, il datore di lavoro ha esagerato, visto che "il contratto collettivo applicato prevede per tali inadempimenti/infrazioni delle sanzioni di tipo conservativo, quali la multa o la sospensione dal lavoro".

Copio ulteriormente da un commento alla sentenza: "In particolare, i giudici della Suprema Corte di Cassazione hanno precisato che in tema di licenziamento disciplinare, l'uso, anche quotidiano, della mail aziendale per ragioni private, come anche l'installazione sul computer di programmi che non sono inerenti all'attività lavorativa, non rappresentano violazioni (inadempimenti) che di per sé sono sufficienti alla irrogazione del licenziamento del dipendente".

Bisognerebbe poi capire bene se questi comportamenti erano censurati dalle regole aziendali.

Segnalo infine l'articolo su Filodiritto:
- http://www.filodiritto.com/cassazione-lavoro-luso-privato-del-computer-e-dellemail-aziendali-non-legittima-il-licenziamento

****

06- DFA Open Day 2014 - Materiale digital forensics

Vi segnalo il materiale del DFA Open Day 2014:
- http://www.perfezionisti.it/proposte-formative/dfa-open-day-2014/

E' stato un evento molto bello, con circa 100 persone e molti spunti interessanti.

****

07- NIST SP 800-160 "Systems Security Engineering"

Il NIST ha reso pubblico il final draft della SP 800-160, dal titolo "Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems":
- http://csrc.nist.gov/publications/PubsDrafts.html#800-160

Sono indeciso se leggerlo ora o aspettare la pubblicazione della versione finale. Ad ogni modo, credo sia una lettura da fare.

****

08- Draft ISO 9001:2015

La nuova ISO 9001 è allo stato DIS, ossia bozza. Secondo i miei calcoli, se il consenso sarà sufficiente, a novembre sarà disponibile il final draft e a inizio 2015 uscirà la nuova norma.

Devo dire che il lavoro mi sembra notevole, anche per i miglioramenti introdotti all'HLS e all'esplicitazione di aspetti che nella ISO/IEC 27001 sono stati invece ritenuti "impliciti".

In molti hanno scritto sulle novità della norma, soprattutto sull'analisi del rischio (a cui è anche dedicato un paragrafo nell'introduzione). Io vedo anche sottolineati: l'attenzione al cliente, il controllo dei cambiamenti, l'importanza della conoscenza. Io sottolineo il fatto che non si parla più di "risorse umane" ma di "persone" e lo trovo un bel segnale.

Invito quanti vogliono condividere approfondimenti sulla nuova ISO 9001 a segnalarmeli o inviarmeli.

Consiglio però di aspettare il final draft prima di trarre conclusioni sull'attuazione della ISO 9001. Potrebbe infatti essere ampiamente modificata, anche se in molti lo ritengono improbabile.

****

09- Presentazione sul rischio informatico

Enrico Luigi Toso di DB Consorzio mi ha inviato una interessante presentazione dal titolo "Circolare Banca d'Italia 263 Cap. 8 – Il Rischio informatico: Un inquadramento metodologico per favorire l'integrazione del rischio informatico nella gestione del rischio operativo".

Lettura quanto meno impegnativa ma molto interessante e che consiglio perché ci sono cose molto interessanti sulla valutazione del rischio, applicabili anche in ambiente non bancario.

Qualche esempio: riflessione sul rapporto tra rendimento e rischio e sul rapporto tra adeguamento normativo e rischio, suggerimento di analizzare il rischio per processi e non per asset (anche se poi questi si ripresentano). Non c'è solo questo, ovviamente.

Il materiale si troverà sul sito (sono richieste credenziali di accesso fornite dopo registrazione):
- http://www.abieventi.it/eventi/2044/banche-e-sicurezza-2014/

****

10- Password codificate e password di default

Dal SANS Newbyte trovo questa deliziosa notizia: il Department of Homeland Security (DHS) statunitense ha avvisato gli operatori dei pannelli stradali Daktronics Vanguard che questi possono essere attaccati a causa delle password codificate in essi.

Risposta della Daktronics Vanguard: "non si tratta di password codificate, ma di password di default non modificate".

Due cattive pratiche al prezzo di una:
- http://www.nextgov.com/cybersecurity/2014/06/flaw-lets-hackers-control-electronic-highway-billboards/85849/

****

11- OpenSSL - Ancora!

In tanti hanno scritto delle nuove vulnerabilità riscontrate su OpenSSL. Io scelgo un link presentato dal SANS Newsbyte:
- http://www.theregister.co.uk/2014/06/05/openssl_bug_batch/

Sembra che, una volta trovato un nuovo giocattolo, tutti vogliano divertirsi a trovarne i difetti.

Un editor del SANS (Northcutt) dice: "se stai usando OpenSSL, non agitarti perché i suoi sviluppatori ci stanno lavorando; se non stai usando OpenSSL, ci si può chiedere se il tuo prodotto è sicuro".

Aggiungo quanto scritto da Stefano Ramacciotti in una discussione sul gruppo Sikurezza.org di LinkedIn: "Il problema non è la crittografia, ma la sua implementazione; il protocollo SSL è a posto; se dovessimo scrivere un nuovo programma per SSL, non solo si rischierebbe di sbagliare ancora nello sviluppo, ma anche nell'implementazione del protocollo stesso".

****

12- TrueCrypt

La notizia ha fatto subito il giro del mondo: gli sviluppatori di TrueCrypt hanno dichiarato la fine dello sviluppo e della manutenzione dello strumento più noto e affidabile per cifrare hard disk o singoli file e cartelle:
- http://krebsonsecurity.com/2014/05/true-goodbye-using-truecrypt-is-not-secure/
- http://arstechnica.com/security/2014/05/truecrypt-is-not-secure-official-sourceforge-page-abruptly-warns/

Il sito ufficiale è questo:
- http://truecrypt.sourceforge.net

Alcuni suggeriscono strumenti come BitLocker di Windows e altre cose che mi sembrano molto meno intuitive e facili da utilizzare (con TrueCrypt è facilissimo creare una cartella cifrata da copiare-incollare quando se ne fa il backup).

Alcuni però sostengono che si tratti di un attacco al sito web di TrueCrypt e che la versione 7.2 pubblicata sia un falso. Quindi cosa fare? Io, non l'avessi già sul mio pc, scaricherei da qui la versione 7.1a (quella per Windows ha nome " TrueCrypt Setup 7.1a.exe"):
- https://github.com/DrWhax/truecrypt-archive

****

13- Accreditamento conservazione digitale (commenti)

In merito agli aggiornamenti relativi ai regolamenti sulla conservazione digitale (http://blog.cesaregallotti.it/2014/05/accreditamento-conservazione-digitale.html), Franco Ruggieri mi ha inviato alcune considerazioni molto interessanti che riporto.

E' vero che nel DPCM 3/12/2013 non c'è alcun riferimento allo ISO/IEC 27001, mentre c'è nella successiva Circolare AgID 65/2014. Insomma: la Circolare mette una pezza al buco del DPCM.

E' stato pubblicato da AgID un altro documento che ritengo di estremo interesse per i conservatori che, però ha un titolo chilometrico: "Accreditamento dei soggetti pubblici e privati che svolgono attività di

conservazione dei documenti informatici - Requisiti di qualità e sicurezza per l'accreditamento e la vigilanza"

Ebbene, questo documento esplode nei minimi particolari i requisiti da rispettare, riportando per ognuno la clause dello OAIS (ISO 14721) e dello ETSI TS 101 533-01. Insomma: la certificazione ISO/IEC 27001 potrà (o forse "dovrà") essere fatta avvalendosi del TS 101 533-01 come punto di riferimento per le misure di sicurezza da attuare. D'altronde ad oggi non c'è altro documento a cui rifarsi per un conservatore.

Peccato che questo TS sia stato redatto (e tradotto da UNI nella serie UNI/TS/TR 11465-1-2-3) nel 2012, quando cioè la versione ISO/IEC 27001 del 2013 ancora non era nata.

Anche se il documento di "Requisiti di qualità e sicurezza per l'accreditamento" è solo una linea guida, senza la forza né di una Circolare né di uno strumento giuridico, è sempre un documento emesso da chi fa la vigilanza. È quindi molto probabile che AgID si baserà su di esso e sui documenti da esso referenziati.

C'è un altro punto: si fa riferimento al TS 101 533-01 come "raccomandazione", mentre invece è una "specifica". Inoltre il DPCM si riferisce all'elenco dove è riportato come "elenco di specifiche". In definitiva: quanto indicato nella tabellona del documento "Requisiti di qualità e sicurezza per l'accreditamento e la vigilanza" diventa cogente, compresa la specifica ETSI TS 101 533-01.

Infine è buffo vedere che viene richiesta una certificazione ISO/IEC 27001, con scadenza triennale, e poi è richiesto di presentare un certificato di conformità ai requisiti tecnici (che comprendono il rispetto della ISO/IEC 27001 e della ISO 14721) ogni due anni.

****

14- Delle definizioni di rischio (approfondimento 2)

Delle definizioni di rischio (approfondimento 2)

Dopo gli articoli degli ultimi mesi, Andrea Rui mi ha inviato una considerazione personale che trovo molto interessante perché distingue tra una valutazione del rischio "economica", che quindi si basa sulla formula "rischio = minaccia x conseguenze", e una "umana" che deve basarsi su altre formule.

Copio e incollo la mail di Andrea e lo ringrazio.
<< Il D.Lgs. 81/2008 ha un approccio al rischio totalmente diverso da quello delle altre norme. La centralità del rischio non è sull'azienda, ma sul lavoratore.

Una gestione del rischio per i lavoratori dal punto di vista economico dovrebbe includere svariati aspetti, tra cui: costo derivante dall'assenza, eventuali sanzioni penali, eventuali sanzioni civili, perdita di know how, danno di immagine, aumento dei costi assicurativi, eventuale perdita di appalti o di partecipazione a gare, criticità derivanti dall'assenza del lavoratore, eccetera.

Al contrario, il rischio per il D.Lgs. 81/2008 è uno solo: che il lavoratore si faccia male.

In sintesi, mentre per la ISO/IEC 27001 il rischio che un lavoratore si possa fare male può essere accettabile (ed in particolari contesti potenzialmente anche conveniente) dal punto di vista del business, non lo è dal punto di vista della Legge.

Infatti le aziende tendono a delocalizzare dove la nostra legge non si applica, e dove il costo per i danni alle persone sono inferiori ai costi da sostenere per impedire che si verifichino gli incidenti e per minimizzarne l'impatto. >>