Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – LUGLIO 2017

****

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

****

00- Editoriale

Come sempre a luglio invio la newsletter un po' più tardi del solito "metà mese" ed è quindi molto più corposa (con anche 2 articoli "personali", oltre a questo editoriale).

Quindi vi faccio gli auguri di "buon agosto" e vi lascio alla lettura.

****

01- Migrazione della newsletter

Come già annunciai qualche tempo fa, è mia intenzione migrare la newsletter su un sistema di mailing professionale. Nulla cambierà per i lettori (spero), ma inizierò i lavori ad agosto-settembre, in modo che chi voglia chiedermi di cancellarlo lo possa fare.

Migrerò su MailUP (www.mailup.it), che risponde alle esigenze di mantenere il servizio in Europa e di poterlo controllare completamente. Potreste quindi ricevere qualche email "strana" quando configuro. Spero di no, ma sto sperimendando anche io e mi scuso per ogni noia potrò darvi. Cercherò di mantenere la grafica "quasi minima" attuale.

Il servizio è sponsorizzato dal Gruppo IMTEAM (non avrà accesso agli indirizzi). Ringrazio in particolare Piero Fuselli per avermi contattato per primo per dare il suo contributo.

Poco dopo di lui è arrivato Fabio Guasconi di Bl4ckSwan con una proposta identica. Lo ringrazio molto. Ho deciso solo in base all'ordine di arrivo.

Desidero anche ringraziare, per i loro contributi: Andrea Azeglio, Antonio Caccamo, Enos D'Andrea, Igor Falcomatà, Carlo Roatta, Pierluigi Stefli.

****

02- Miei prossimi interventi (con pubblicità)

Ho sempre detto che non avrei fatto pubblicità, però in molti recentemente mi hanno chiesto quando avrei tenuto un corso Lead auditor ISO/IEC 27001. Quindi, in breve, dovrei tenerlo il 9, 10, 11 ottobre a Bologna. Per non appestare oltre la newsletter, invito chi è interessato di contattarmi.

Il 12 ottobre, poi, dovrei partecipare ad un convegno a Rovigo. Per quello però non ho ancora ricevuto ulteriori dettagli (vorrebbero che parli di valutazione del rischio e GDPR).

****

03- Lavori sul Codice privacy (e integrazione con il GDPR)

Monica Perego mi segnala questo emendamento ad un DDL in discussione al Parlamento: http://www.senato.it/japp/bgt/showdoc/frame.jsp?tipodoc=Emendc&leg=17&id=1029112&idoggetto=1035671.

Questo il commento di Monica: "questa è la legge delega che non abroga il codice ma dice che va integrato con il Regolamento". Monica non lo dice, ma lo sottintende: avevano torto quelli che davano per abrogato il D. Lgs. 196 dopo l'entrata in vigore del GDPR (e purtroppo alcuni lo dicevano con troppa indisponenza).

****

04- Certificazioni privacy (ISO/IEC 27018 e "lo schema italiano")

Accredia ha pubblicato un regolamento per le "certificazioni" ISO/IEC 27018 (grazie a Franco Ferrari di DNV GL per la notizia):
http://www.accredia.it/extsearch_documentazione.jsp?area=55&ID_LINK=331&page=118&IDCTX=5549&id_context=5549.

Purtroppo ci sono stati casi in passato (e nel presente) di certificazioni rispetto a questa linea guida, con anche marchi di accreditamento. Sappiamo bene che le linee guida non sono certificabili.

Accredia ha messo un punto fermo e questo è un bene. Però non concordo con l'impostazione. Infatti la ISO/IEC 27018 fa parte di quelle norme di "estensione" dei controlli ISO/IEC 27002 e non dovrebbe essere trattata a parte. Ci dovremo quindi aspettare regole per la 27017, 27011, 27019, 27799 e le future ISO/IEC 29151 e 27552 (sulla privacy)?

Il fatto che continua a sfuggire è che la ISO/IEC 27006 permette di scrivere su un certificato ISO/IEC 27001 che il SOA include i controlli della ISO/IEC 27018 o di altre norme di "estensione" della ISO/IEC 27002. Anzi, si potrebbero citare anche controlli diversi, come quelli del NIST Cybersecurity framework. E quindi questa circolare riguarda solo un caso particolare e non aiuta ad impostare il lavoro in modo coerente e utile per il futuro. Un'altra occasione persa, ahinoi.

Per quanto riguarda lo "schema italiano", proseguo quanto già scritto in un precedente post:
blog.cesaregallotti.it/2017/05/certificazioni-privacy-per-aziende-e-bs.html.

Infatti Pierfrancesco Maistrello, Franco Ferrari e Paolo Sferlazza mi hanno segnalato questo comunicato del Garante e Accredia:
http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/6621723.

Riassunto (mio): lasciate perdere le certificazioni di persone e organizzazioni fino a quando non ve lo diciamo noi (poi... Accredia ha già accreditato un organismo di certificazione senza l'avallo del Garante, ma evito di fare il pignolo).

****

05- Opinione del WP Art. 29 sulla privacy dei lavoratori

Ho notato la notizia in molti posti, ma non l'avevo ben considerata. Fino a quando ho letto questo articolo di Interlex:
- http://www.interlex.it/privacyesicurezza/ricchiuto43.html.

Ricordo che le opinioni del WP Art. 29 sono importanti, in quanto (mi scuso per l'imprecisione) espressione dei Garanti europei.

Inoltre avevo intravisto il punto "caldo" di questa opinione: è ritenuto non corretta la consultazione dei profili dei candidati sui social network da parte del potenziale datore di lavoro. Confesso che la cosa mi lascia perplesso: a mio parere, se una persona mette in pubblico i fatti suoi, legittima, di fatto, chiunque altro a giudicarlo. Comunque, sempre a mio parere, i potenziali datori di lavoro verificheranno sempre il profilo social di un candidato, ma non lo pubblicizzeranno.

Altri aspetti legati ai social network, che mi paiono invece molto pertinenti, sono: i capi non dovrebbero chiedere ai collaboratori la connessione (o la "amicizia"), i capi non dovrebbero obbligare i lavoratori a usare solo profili aziendali.

Inoltre, come già segnalato dall'articolo di Interlex, questa opinione non riguarda solo i dipendenti. E mi sembra corretto siano protetti tutti i lavoratori, a prescindere dal tipo di collaborazione subordinata che hanno.

Infine ho chiesto lumi a Pierfrancesco Maistrello, perché ricordavo un'altra recente "opinione" in merito alla privacy e ai lavoratori. E infatti mi ha confermato che nel 2015 era stata pubblicata dal "Comitato dei ministri" una raccomandazione:
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4224268.

Inoltre Pierfrancesco mi fa notare che questa del WP Art. 29 è una "opinion" e non una "linea guida". Forse perché (opinione anche questa!) vuole aiutare i processi di adeguamento legislativo al GDPR dei singoli Stati.

****

06- Privacy: Lavoro e dati giudiziari dei dipendenti

Il Garante privacy, con la sua ultima newsletter, ribadisce che le organizzazioni non possono trattare i dati giudiziari dei dipendenti (e neanche dei candidati) se non richiesto dalla legge o autorizzato dal Garante stesso.

La newsletter:
http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/6558875.

Il Provvedimento specifico:
http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/6558837.

In effetti, c'è la cattiva abitudine, in troppe imprese, di chiedere il casellario giudiziario. Questo non solo perché contrario alla normativa in vigore, ma perché i comportamenti passati di una persona non possono dare indicazioni su quelli futuri. In caso contrario, dovremmo pensare che le persone non potranno mai migliorare e neanche noi stessi; e quindi a che servirebbe studiare?

Forse sono fuori tema. Ma ci torno subito. Infatti è sbagliato pensare che il personale selezionato in quanto senza reati passati sia migliore di quello che è già stato oggetto di indagine. Sappiamo che una persona delinque spesso "in crescendo" e quindi un incensurato potrebbe già essere avviato per quella strada. Una persona che ha già scontato una pena, forse, riesce a riconoscere ed evitare di percorrere una certa strada, rinforzata anche dalla stabilità del posto di lavoro.

Inoltre non dobbiamo progettare controlli di sicurezza pensando che le persone interne siano tutte oneste (sindrome di Fort Apache). Questo è un errore: le persone possono compiere errori e possono anche peggiorare (non solo migliorare) e quindi i controlli di sicurezza devono essere progettati adeguatamente.

****

07- ISO/IEC 29134 - Privacy impact assessment

E' stata pubblicata la ISO/IEC 29134:2017 dal titolo "Guidelines for privacy impact assessment":
- https://www.iso.org/standard/62289.html.

Ne ho già parlato in precedenza. Da notare che è il recepimento ISO delle linee guida del CNIL (gratuite!):
- www.cnil.fr/english/news-and-events/news/article/privacy-impact-assessments-the-cnil-publishes-its-pia-manual/.

Su questa norma ho qualche perplessità teorica (confusione su "fonti di rischio" e "minacce") e pratica (gli esempi non sono illuminanti). Però non ci ho minimamente lavorato, malgrado ne avessi la possibilità, e quindi non ho approfondito i perché di queste scelte.

****

08- Libro "Privacy & audit"

Mi piace consigliare il libro "Privacy & audit" di Fulvia Emegian, Monica Perego:
http://shop.wki.it/Ipsoa/Libri/Privacy_Audit_s559485.aspx (link della casa editrice).

Ovviamente ho trovato qua e là qualche piccola imprecisione (!), ma l'ho trovato ben fatto: ben raccontato e con molti esempi (veramente tanti, con anche tracce di audit svolti). E poi mi trovo d'accordo con l'approccio proposto sia per gli adempimenti privacy sia per l'esecuzione degli audit.

Ho conosciuto Fulvia e Monica e ci siamo scambiati i libri. Meno male che non è stata quella situazione imbarazzante per cui qualcuno ti regala il suo libro e a te non piace!

Monica è formatrice presso corsi per DPO, che ho sempre sconsigliato (e ci sono altre cose che chi mi conosce potrebbe trovare interessanti). Però sia Fulvia sia Monica sono molto preparate, brave e entusiaste e il libro è fatto bene.

Conclusione: sono ben contento di fare questa pubblicità estiva (d'altra parte non ci guadagno niente).

****

09- Privacy: il Garante si diverte

Segnalo, grazie a Giulia Zanchettin, che il Garante ha pubblicato "Estate in privacy", ossia consigli per tutti da seguire durante l'estate (e non solo):
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3240343.

Mi sembrano regole banali, ma ben presentate.

Confesso che stavo ignorando completamente la notizia (semplicemente perché i miei lettori sono principalmente professionisti della sicurezza), ma è vero che un ripasso delle regole di base non guasta mai (sono purtroppo tanti i professionisti della sicurezza che scrivono tweet quando atterrano a Hong Kong, Parigi, Londra, New York eccetera, non preoccupandosi di potenziali ladri interessati a sapere quando non sono a casa).

Inoltre il titolo di Giulia ("Il Garante si diverte") era troppo bello per essere ignorato.

****

10- ISO/IEC 27004:2016 sulle misurazioni

E' stata pubblicata a dicembre 2016 la nuova versione della ISO/IEC 27004 dal titolo "Information security management -- Monitoring, measurement, analysis and evaluation": https://www.iso.org/standard/64120.html.

Sono stupito di non aver rilevato la notizia all'epoca. Infatti tengo molto a questa versione della ISO/IEC 27004, a cui ha contribuito molto Fabio Guasconi e anche io ho partecipato.

Questa versione è molto meno teorica della precedente e presenta ben 35 esempi di misurazioni per la sicurezza (c'è il mio zampino...). Non tutti questi indicatori mi convincono (per esempio quello che richiede di misurare il numero di riesami di Direzione), mentre altri sono più indicatori di avanzamento (per esempio percentuale degli audit interni rispetto a quelli programmati). Infine rimangono gli indicatori "veri" (per esempio disponibilità dei sistemi, tempi di intervento sugli incidenti), che sono pochi, come ho sempre sostenuto.

Ricordo infatti che il problema della sicurezza delle informazioni è che ha come obiettivo il "non verificarsi di eventi" e quindi non è possibile raccogliere molti dati utili per misurare.

****

11- Nuova versione della UNI 10459 (sul security manager)

Mi segnala Franco Ferrari di DNV GL che è stata pubblicata la UNI 10459:2017, aggiornamento della versione del 2015, dal titolo "Attività professionali non regolamentate - Professionista della security - Requisiti di conoscenza, abilità e competenza": http://store.uni.com/magento-1.4.0.1/index.php/uni-10459-2017.html.

Franco mi segnala un articolo su Punto Sicuro, però non accessibile senza credenziali. Riporto però questa frase: "Questa nuova edizione della norma presenta dei miglioramenti, soprattutto di tipo formale, che mirano a rendere la norma sempre più leggibile ed aderente a una realtà in costante evoluzione, come la realtà degli scenari di rischio e delle strategie di attacco e difesa".

Ho chiesto lumi a Fabio Guasconi di Bl4ckSwan, che ha partecipato ai lavori. Mi ha detto che ha lavorato soprattutto "per evitare che ci fossero ambiguità tra il Security manager (che è in sostanza un CSO, con responsabilità di più alto livello in materia di sicurezza delle informazioni) e l'Information security manager".

Per questa figura ha anche uniformato la terminologia usata per riferirsi alla sicurezza delle informazioni con quella della ISO/IEC 27001 e richiamato i profili specifici della UNI 11621-4 con cui interfacciarsi, rimosso dove possibile le responsabilità e le competenze di dettaglio del Security manager sull'information security, lasciandogli quelle di più alto livello.

****

12- Legale: Email ammissibile come prova

Segnalo questo articolo di Altalex dal titolo "Email ammissibile come prova anche senza la firma elettronica qualificata":
- http://www.altalex.com/documents/news/2017/01/23/email-ammissibile-come-prova-anche-senza-la-firma-elettronica-qualificata.

Il titolo dice già tutto.

****

13- Raccomandazioni per i fornitori di cloud

Francesca Lazzaroni di Spike Reply mi ha segnalato una pubblicazione del German Federal Office for Information Security (anch'esso designato con BSI) sul cloud:
-
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/SecurityRecommendationsCloudComputingProviders.html.

Si tratta di una pubblicazione del 2011, ma mi sembra utile perché per ogni argomento è proposta una tabella di sintesi delle misure di sicurezza da prevedere per i servizi cloud (e non solo, per la verità). Queste tabelle potrebbero essere utili anche per chi si occupa di contratti con fornitori cloud.

In passato avevo già segnalato altre pubblicazioni:
- di AIEA, In italiano: http://www.aiea.it/attivita/gruppi-di-ricerca/it-audit-cloud;
- di ENISA: https://www.enisa.europa.eu/media/press-releases/enisa2019s-security-guide-and-online-tool-for-smes-when-going-cloud.

****

14- Fornitori di servizi per le aziende con i piedi per terra

Mio articolo dal titolo "Fornitori di servizi per le aziende con i piedi per terra":
- https://www.ictsecuritymagazine.com/articoli/fornitori-piedi-terra/.

****

15- Perché avere lo spezzatino dei documenti?

Dalla newsletter di ANSSAIF segnalo questo articolo dal titolo "Asset Protection. Perché alle aziende piace lo 'spezzatino' di norme ai testi unici?":
https://www.key4biz.it/assetprotection-perche-alle-aziende-piace-lo-spezzatino-norme-ai-testi-unici/191349/.

In sintesi, l'autore lamenta che troppe organizzazioni pubblicano documenti distinti per codice etico, regolamento per la privacy e guida alla sicurezza, nonostante siano elementi assolutamente integrabili.

****

16- Inventario degli asset: l'incompreso

Mio articolo dal titolo "Inventario degli asset: l'incompreso":
- https://www.ictsecuritymagazine.com/articoli/inventario-degli-asset-lincompreso/.

Mi hanno proposto di scrivere articoli per ICT Security Magazine. Di materia ne avrei e spero quindi di scriverne altri nel futuro.

****

17- Report sicurezza di Lloyds of London

Segnalo (grazie a Stefano Ramacciotti) il "Emerging Risk Report on Cyber Insurance" (sottotitolo "Counting the cost: Cyber exposure decoded") della Lloyds of London:
- https://www.lloyds.com/news-and-insight/risk-insight/library/technology/countingthecost.

Mi affido al commento del SANS: "il rapporto, in definitiva, suggerisce di trattare gli attacchi IT come disastri naturali, non come crimini "tradizionali".

Inoltre il report presenta due esempi: per il primo (fornitore di servizi cloud) con l'assicurazione si recuperano il 15% dei danni, mentre per il secondo (interruzione di un server critico) si recuperano il 7% dei danni. Tradotto: è sempre e comunque necessario attuare le "solite" misure di sicurezza preventiva.

****

18- Allagamento blocca i server del Tribunale di Napoli

Sandro Sanna mi segnala la seguente notizia, dal titolo "In tilt i sistemi informatici del Tribunale di Napoli, si torna alla carta":
http://www.ilmattino.it/napoli/cronaca/napoli_palazzo_giustizia_server_carta_tribunale-2550463.html.

Il suo commento: " c'è chi mette sempre nel risk assessment probabilità bassa è poi invece...".