Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – APRILE 2018
****

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.

La newsletter è inviata via MailUp, offerta da Team Quality S.r.l.

Per iscriversi, cancellarsi e leggere l'informativa privacy: http://www.cesaregallotti.it/Newsletter.html.

Sulla stessa pagina è possibile consultare l'informativa sul trattamento dei dati personali.

****
Indice

****
01- DFA Open Day - 5 luglio 2018

DFA è l'associazione degli alunni e docenti del Corso di Perfezionamento in "Computer forensics e investigazioni digitali" e di tutti gli altri corsi di Perfezionamento delle Cattedre di Informatica Giuridica e Informatica Giuridica Avanzata dell'Università degli Studi di Milano (io ne sono Presidente da poco):
- http://www.perfezionisti.it/

Il pomeriggio del 5 luglio, presso la Statale di Milano, abbiamo organizzato l'Open Day, con vari interventi relativi a digital forensics, privacy e altre cose. Il programma è in costruzione e poi attiveremo le modalità di iscrizione (gratuita!). Intanto invito tutti a prendere nota della data.

****

02- VERA per privacy - versione beta

Ho pubblicato la versione beta del mio file Excel per la privacy:
- http://www.cesaregallotti.it/Pdf/Pubblicazioni/2018-VERA-4.4-ITA-privacy-BETA-20170416.xlsx.

Se non dovesse funzionare il link diretto, ecco la pagina web di riferimento:
- http://www.cesaregallotti.it/Pubblicazioni.html.

Io lo uso per la valutazione del rischio privacy, per la PIA e per i controlli privacy di ENISA. Spero che le istruzioni chiariscano i diversi modi con cui può essere usato. In caso contrario... vi prego di darmi suggerimenti.

Per questa versione Beta, grazie a: Alessandro Gaspari (che mi ha mandato il suo Excel, con anche traduzione, delle misure del "Handbook on Security of Personal Data Processing" di ENISA del dicembre 2017), Stefano Posti, Pierlugi Stefli.

****

03- Schema di decreto privacy

Il 21 marzo, il Consiglio dei Ministri ha approvato una bozza di decreto legislativo che dovrebbe armonizzare la nostra legislazione con il GDPR e abrogare il Codice privacy:
- http://www.governo.it/articolo/comunicato-stampa-del-consiglio-dei-ministri-n-75/9132.

La notizia me l'hanno data Pierfrancesco Maistrello e gli Idraulici della privacy; l'ho anche trovata su LinkedIn e su Twitter. Vorrei non parlarne, visto che si tratta di una bozza che dovrà essere sottoposta anche al Garante.

Ho sentito qualche commento:
- sembra che abroghino la "notifica preventiva" richiesta dalla Legge di Bilancio (va anche detto che finora il Garante non ha pubblicato alcuna istruzione e quindi nessuno poteva attuarla);
- c'è un articolo che dice che titolare e responsabile (intesi come "aziende") possono distribuire deleghe al proprio interno; lo trovo comico, visto che le aziende dovrebbero già sapere che possono farlo;
- lo stesso articolo dice che le autorizzazioni (le vecchie "nomine ad incaricato") possono essere date nel modo più opportuno; trovo divertente che la Legge si assuma l'onere di educare i consulenti (ho collaborato con aziende che, senza mai aver visto un consulente privacy, avevano già al loro interno processi che bastava adattare un poco per recepire i requisiti del GDPR; quindi evidentemente sono alcuni "consulenti privacy" che vanno educati perché la smettano di appesantire inutilmente i processi delle organizzazioni con nomine e designazioni, per giunta su carta e firme e contro-firme);
- viene abrogato e non modificato il Codice privacy (D. Lgs. 196), contrariamente a quanto io immaginavo (io pensavo avrebbero fatto la stessa operazione fatta con il D. Lgs. 82 del 2005 o CAD, dopo la pubblicazione del Regolamento eIDAS; l'esperienza con il CAD è stata negativa perché non era "aggiustabile" facilmente per renderlo allineato a eIADS; giustamente, con la privacy hanno preferito ripartire da zero per non ripetere gli stessi errori).

Massimo Cottafavi del Gruppo Snam mi ha segnalato questo articolo di Agenda Digitale:
- https://www.agendadigitale.eu/sicurezza/privacy/gdpr-approvato-lo-schema-di-decreto-questi-i-punti-sul-tavolo/.

Intanto il CNIL (il Garante francese) ha annunciato che, per i primi mesi e a determinate condizioni, non sanzionerà le imprese per inadempienze rispetto al GDPR (grazie agli Idraulici della privacy per la segnalazione):
- http://www.etiprivacy.it/gdpr-francia-per-i-primi-mesi-no-a-sanzioni-alle-aziende-sui-nuovi-obblighi/.

****

04- Articolo "GDPR: il 25 maggio non accadrà nulla"

In questi giorni ho visto molti richiami all'articolo di Andrea Lisi dal titolo "GDPR e Protezione dei dati, ma il 25 maggio non accadrà nulla":
- https://www.key4biz.it/gdpr-e-protezione-dei-dati-il-25-maggio-non-accadra-nulla/218389/.

Conferma alcune cose che dico da tempo, meglio di come le dico io. Quindi lo consiglio.

****

05- Ius law web radio: Come effettuare una DPIA secondo la ISO/IEC 29134

Elia Barbujani di Ius law web radio mi ha intervistato su PIA e ISO/IEC 29134. La puntata (48 minuti!) è qui:
- https://webradioiuslaw.it/speciale-adeguamento-privacy-come-effettuare-una-dpia-secondo-la-iso29134/.

****

06- Linea guida per la PIA degli Osservatori.net

Enrico Luigi Toso mi ha segnalato questa "Linea guida per la Data protection impact assessment" a firma Politecnico e Osservatori.net:
- https://www.osservatori.net/it_it/pubblicazioni/linea-guida-per-la-data-protection-impact-assessment.

Non è facilissimo scaricarla perché bisogna registrarsi e poi bisogna fare parecchi clic. La lettura è piuttosto interessante. Nulla di particolarmente originale, ma una bella rassegna su questo requisito del GDPR.

Viene presentato un metodo semplice per calcolare il rischio per la PIA e penso che questo sia molto positivo.

Visto che il CNIL ha proposto un metodo (recepito anche nella ISO/IEC 29134) troppo macchinoso e di difficile applicazione, mi fa piacere quando voci autorevoli promuovono approcci più pragmatici.

****

07- Il caso Cambridge Analytica

Si è parlato tantissimo del caso Cambridge Analytica e quindi faccio una breve rassegna stampa (con commenti).

Il primo link racconta la storia:
- https://www.theregister.co.uk/2018/03/19/boom_cambridge_analytica_explodes_following_extraordinary_tv_expose/.

Il secondo racconta la storia e aggiunge un commento: non si tratta di violazione di dati personali, visto che il modello di Facebook esplitamente consentiva la raccolta ed elaborazione dei dati personali degli utenti:
- https://motherboard.vice.com/en_us/article/3kjzvk/facebook-cambridge-analytica-not-a-data-breach.

La penso esattamente come l'articolo di Motherboard. Quando mettiamo dati su Facebook sappiamo bene che Facebook li può vendere a chi e come vuole. Non dobbiamo lamentarci.

Questo articolo spiega come configurare convenientemente Facebook:
- https://www.eff.org/deeplinks/2018/03/how-change-your-facebook-settings-opt-out-platform-api-sharing.

Perché il caso Cambridge Analytica dovrebbe preoccupare anche te
- https://www.wired.it/attualita/politica/2018/03/19/cambridge-analytica-facebook-privacy/.

La penso parzialmente come l'articolo di Wired. Io penso che culturalmente molti dicono che non abbiamo niente da nascondere. Non si tratta di nascondere; si tratta di intimità e la sua perdita è un fatto culturale che mi inquieta. Fin qui è un'opinione come un'altra. Il fatto inquietante è che noi non abbiamo niente da nascondere (forse), ma altri non solo nascondono, ma usano le informazioni che noi volontariamente diamo loro. La sproporzione tra un utente di Facebook e un OTT come Facebook dovrebbe metterci in guardia. Invece... niente.

L'articolo di Wired spiega anche che il caso di Cambridge Analytica non è emerso a causa del coinvolgimento di Trump (forse inconsapevolmente, tra l'altro), ma perché ci spiega come funziona oggi la manipolazione delle persone. E inquieta esattamente come tanti anni fa inquietavano alcune tecniche di pubblicità occulta: ci rendiamo conto di essere manipolabili. In troppi, però, continuano a pensare di essere immuni e continueranno a diffondere tutto ciò che li riguarda, senza voler nascondere niente. Alcuni, come me, si inquietano. Altri non se ne preoccupano minimamente. Me ne farò una ragione.

Infine... pochi giorni prima del caso di Cambridge Analytica il Corriere della Sera aveva pubblicato un articolo dal titolo "Chi spia i nostri conti" di Ferruccio De Bortoli. Non mi è piaciuto come è scritto, ma credo ci dica qualcosa di importante. Questo link riporta fedelmente l'articolo, ma temo non lo faccia legalmente; potrebbe quindi essere cancellato:
- http://prontoagente.it/component/cobalt/item/674-chi-spia-i-nostri-conti.

PS: Pierfrancesco Maistrello mi ha segnalato questa "Opinion" dell'European data protection supervisor (EDPS), dal titolo "online manipulationand personal data", pubblicata proprio il giorno dopo il mio post qui sopra:
- https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

****

08- ISO 9004:2018

Franco Ferrari di DNV GL mi ha informato dell'uscita della nuova edizione della ISO 9004 dal titolo "Quality management - Quality of an organization -- Guidance to achieve sustained success":
- https://www.iso.org/standard/70397.html.

Si tratta, in poche parole, di una riscrittura della precedente ISO 9004 per allinearla alla ISO 9001:2015.

****

09- Rapporto Clusit 2018

Il Clusit, a metà marzo 2018, ha pubblicato il consueto rapporto annuale sulla sicurezza informatica:
- https://clusit.it/rapporto-clusit/.

A mio parere è meno interessante di altre volte. Però consiglio comunque di guardarlo.

Il Clusit ha organizzato a marzo il Security summit di Milano. Le presentazioni sono ora disponibili:
- https://www.securitysummit.it/event/Milano-2018/atti.

****

10- AgID e le regole per i fornitori cloud

AgID ha pubblicato le due circolari relative ai criteri per la qualificazione dei Cloud Service Provider per la PA e per la qualificazione di servizi SaaS per il Cloud della PA (grazie a Franco Ferrari di DNV GL per la notizia):
- http://www.agid.gov.it/notizie/2018/04/10/piano-triennale-circolari-software-service-cloud-cloud-service-provider-pa.

Consiglio vivamente di leggere le due circolari, in particolare gli Allegati, anche a chi non offre servizi per la PA. Infatti essi riportano le "misure minime di sicurezza" che penso saranno di riferimento per il futuro in Italia.

Io avevo mandato qualche commento nella fase di consultazione pubblica. Non ho controllato se e come sono stati recepiti. Ritengo comunque che sia un lavoro da considerare attentamente.

Servizi SaaS:
- https://cloud-pa.readthedocs.io/it/latest/circolari/SaaS/circolare_qualificazione_SaaS_v_4.12.27.html.

Cloud service provider (IaaS e PaaS):
- https://cloud-pa.readthedocs.io/it/latest/circolari/CSP/circolare_qualificazione_CSP_v1.2.html.

****

11- Valutazione del rischio e controlli per il CIS

Il CIS, Center for Internet Security, ha pubblicato due interessanti documenti, sotto il titolo di "Controlli":
- https://www.cisecurity.org/controls/.

Il primo (grazie a Giancarlo Caroti) è l'elenco vero e proprio dei controlli, arrivato alla versione 7. Si tratta di un elenco di 20 categorie di controlli, poi meglio espressi in circa 170 controlli di dettaglio per la sicurezza informatica. I controlli sono espressi in forma sintetica. Si tratta ovviamente di una lettura faticosa, ma utile.

Il secondo (grazie a Franco Ferrari) è la "CIS RAM Version 1.0" (titolo più esteso è "Risk Assessment Method"). L'ho sfogliato molto rapidamente, ma confesso che, quando ho cominciato a occuparmi di valuazione del rischio, avrei voluto avere una pubblicazione così. Ho notato una cosa importante: sono presentati più approcci, uno dei quali è quello solito ("asset based"), mentre gli altri sono meno tradizionali.

Sono anni che l'approccio asset-based non è più usato efficacemente, se non in rari casi. Spero che anche questa pubblicazione permetterà di riconsiderare la centralità di questo approccio.

****

12- Fog e mist computing

L'informatica nebbiosa sembrerebbe materia da milanesi. Invece si tratta di un modello di supporto all'IoT, alternativo al cloud computing.

Personalmente non ne so nulla, ma, se il NIST dedica una Special Publication a questo argomento, ritengo sia opportuno cominciare a sapere che esiste.

Quindi fornisco il link del NIST sulla NIST Special Publication 500-325 "Fog Computing Conceptual Model":
- https://csrc.nist.gov/News/2018/Fog-Computing-for-Internet-of-Things-Devices.

****