Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – GIUGNO 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

****
PRIMA PARTE: TUTTO IL RESTO

01- 5 luglio 2018: DFA open day su GDPR, digital forensics e altro

Il Programma del DFA Open Day del 5 luglio 2018 è online!
- http://www.perfezionisti.it/open-day/dfa-open-day-2018/.

Si parlerà di social engineering, digital forensics e deep web, social media e riconoscimenti, privacy e intelligenza artificiale e infine GDPR.

Poco GDPR? Beh... era ora si ricominciasse ad alzare lo sguardo anche ad altri argomenti.

DFA è l'associazione di cui sono (per puro caso) Presidente e mi farebbe tanto piacere che partecipiate numerosi.

Organizziamo questo evento da anni ed è sempre stata un'occasione bellissima di incontri e discussioni tra esperti e "tecnici", senza alcuno spazio per i venditori di alcun genere (io sono presidente solo da pochi mesi e quindi il merito di tutta questa bellezza non è certo mio, ma dell'associazione nel suo complesso).

Per dire quanto il mio ruolo è immeritato, segnalo che quest'anno non ci sarò. I miei amici (professionisti che sono diventati miei amici negli anni) sanno sicuramente il perché :-)

****

02- Direttiva NIS in vigore (veramente)

Sabrina Prola mi ha segnalato la pubblicazione del D. Lgs. 65 del 18 maggio 2018, di recepimento della Direttiva NIS. Si trova sulla G.U. Serie Generale n. 132:
- www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg.

Questo fa seguito al mio post dal titolo "Direttiva NIS in vigore (ma non troppo)":
http://blog.cesaregallotti.it/2018/05/direttiva-nis-in-vigore-ma-non-troppo.html.

Qui elenco le mie prime riflessioni. Come già successo con il GDPR immagino che avrò l'opportunità di approfondire molti punti (e su alcuni di cambiare idea), grazie ad articoli, interventi e scambi di opinione con chi vuole contattarmi.

La NIS ha l'obiettivo di migliorare la sicurezza informatica nella UE.

Per quanto riguarda i privati, è indirizzata agli "operatori di servizi essenziali e dei fornitori di servizi digitali", con l'eccezione degli operatori di telecomunicazione (in quanto già normati dal Codice delle comunicazioni) e dei fornitori di servizi fiduciari (già normati da eIDAS e CAD). Gli operatori saranno identificati entro il 9 novembre 2018 dalle "autorità competenti NIS" (ossia i Ministeri dello sviluppo economico, delle infrastrutture e trasporti, dell'economica e finanze, della salute e dell'ambiente). L'elenco sarà mantenuto dal Ministero dello sviluppo economico, che quindi sarà da tenere monitorato.

Per quanto riguarda i fornitori di servizi digitali, sono 3 quelli ritenuti critici: Mercato online, Motore di ricerca online e Servizi di cloud computing (ad esclusione delle micro e piccole imprese; ossia imprese che occupano meno di 50 persone e realizzano un fatturato annuo o un totale di bilancio annuo non superiori a 10 milioni di EUR). Trovo interessante siano inclusi anche i primi due, in quanto li ho mai visti come "critici". Dovranno (articolo 14) assicurare la continuità dei servizi, oltre alla sicurezza.

Gli operatori dovranno comunicare alle autorità NIS le proprie misure di sicurezza. Spero non vedremo il proliferare di modelli inventati di sana pianta come sta facendo AgID con i servizi fiduciari (spero che le esperienze di questi anni abbiano insegnato).

Sono stato colpito dalla seguente: "la prova dell'effettiva attuazione delle politiche di sicurezza, come i risultati di un audit sulla sicurezza svolto dall'autorità competente NIS o da un revisore abilitato e, in quest'ultimo caso, metterne a disposizione dell'autorità competente NIS i risultati, inclusi gli elementi di prova". Infatti qui si parla di "revisori abilitati" di cui sapremo in futuro come saranno abilitati e si usa il termine "elemento di prova", invece dello scorretto (frutto di traduzione pigra) "evidenze".

Sui "revisori abilitati" (ma anche sui rappresentanti degli operatori), segnalo solo che al momento in Italia c'è carenza di persone competenti e con esperienza, come abbiamo visto anche nella "corsa al DPO". Speriamo non siano fatti troppi errori nelle prime fasi di attuazione, ossia che non vengano pubblicate check list troppo dettagliate per essere utili, gli auditor non si impuntino sui formalismi o su processi inutili e i rappresentanti degli operatori sappiano far valere le proprie ragioni (purché non cerchino di farsi validare pratiche scorrette).

Viene istituito il CSIRT italiano, unendo (se ho capito correttamente) il CERT nazionale (https://www.certnazionale.it/) e il CERT-PA. Sarà quindi importante seguirne le attività di informazione.

Le misure di sicurezza da adottare sono oggetto dell'articolo 12. "Nell'adozione delle misure, gli operatori di servizi

essenziali tengono conto delle linee guida predisposte dal gruppo di cooperazione, nonché delle linee guida delle "autorità competenti NIS"". Dovremo quindi tenere monitorati i lavori di ENISA, che ultimamente hanno messo a disposizione documenti molto interessanti (altri meno).

All'articolo 17: "promuovono l'adozione di norme e specifiche europee o accettate a livello internazionale relative alla sicurezza della rete e dei sistemi informativi". Speriamo quindi vengano promosse le norme della serie ISO/IEC 27000 e aumenti al partecipazione qualificata alla loro redazione.

Mi permetto di essere preoccupato per il requisito "Le autorità competenti NIS possono predisporre linee guida per la notifica degli incidenti", visto che AgID ha recentemente richiesto agli operatori di servizi fiduciari di comunicarle ogni incidente, secondo uno schema oggettivamente inapplicabile.

Ho qualche perplessità sullo spazio dedicato alla reazione agli incidenti, visto che poco è detto in merito alla prevenzione, rimandando tutto ad altre norme. Questo è un approccio, ovviamente sbagliato, che sta sempre più diffondendosi: molta attenzione alla reazione, minore alla prevenzione.

Infine: le sanzioni arrivano ad un massimo di 150.000 Euro.

****

03- NIS: regolamento di esecuzione 2018/151

A maggio era stato pubblicato il Regolamento di esecuzione (UE) 2018/151 della Commissione recante modalità di applicazione della direttiva (UE) 2016/1148 (ossia della NIS):
- http://data.europa.eu/eli/reg_impl/2018/151/oj.

Vengono forniti chiarimenti in merito alle misure di sicurezza che devono attuare gli operatori NIS. Mi pare che, in sostanza, chieda di applicare la ISO/IEC 27001.

All'articolo 4 sono descritte le caratteristiche per classificare un incidente come "rilevante". Penso che questi elementi dovranno essere considerati da tutti quelli che definiscono un modello di classificazione degli incidenti.

****

04- Modifica al Codice della proprietà industriale

Da Altalex ho la notizia che con il D. Lgs. 63 del 2018 è stato aggiornato il Codice della proprietà industriale (D. Lgs. 30 del 2005) per recepire la Direttiva europea 2016/943:
- http://www.altalex.com/documents/leggi/2018/05/28/know-how-approvato-il-decreto-attuativo-della-direttiva-europea.

Come riportato dall'articolo di Altalex, il provvedimento sostituisce alla nozione di "informazioni aziendali riservate", quella di "segreti commerciali" (vedere quindi l'articolo 1 per la definizione di "proprietà industriale" e l'articolo 98 per quella di "segreti commerciali"). Anche l'articolo 99 è importante per chi si occupa di sicurezza delle informazioni.

Il resto delle modifiche riguarda le sanzioni e i procedimenti giudiziari (interessante il fatto che sia stata considerata la tutela della riservatezza dei segreti commerciali nel corso dei procedimenti giudiziari).

Su Normattiva non è ancora disponibile la versione aggiornata dell'atto.

PS: un ulteriore articolo, più approfondito, è il seguente, segnalatomi da Luca De Grazia:
http://www.quotidianogiuridico.it/documents/2018/06/08/segreti-commerciali-in-g-u-il-d-lgs-63-2018-sulla-protezione-del-know-how.

****

05- Security Development Lifecycle di Microsoft

Stefano Ramacciotti mi ha segnalato le pagine aggiornate di Microsoft sul Security Development Lifecycle di Microsoft.

La prima è il The Security Development Lifecycle Developer Starter Kit:
- https://www.microsoft.com/en-us/SDL/adopt/customsdltraining.aspx.

La seconda è il SDL process: Training:
- https://www.microsoft.com/en-us/SDL/process/training.aspx.

Credo di aver già, a suo tempo, segnalato il materiale MS sul SDL, sicuramente molto buono. Ora molto è cambiato in meglio e si trova molto materiale pratico, cosa sempre difficile da trovare (perché è facile dire "fate vulnerability test", meno capire con cosa).

Anche Stefano mi ha confermato di apprezzare l'approccio più pratico del sito rispetto al precedente.

Grazie a Stefano: finalmente qualcosa che non sia "GDPR"!!! Un po' di freschezza ci voleva...

****

06- Mio articolo sulla sicurezza dei dispositivi mobili

Un mio articolo su ICT Security Magazine dal titolo "Sicurezza dei dispositivi mobili e BYOD":
- www.ictsecuritymagazine.com/articoli/sicurezza-dei-dispositivi-mobili-e-byod.

****

SECONDA PARTE: GDPR (dal mese prossimo spero non avrà più bisogno di una parte dedicata)

07- Dlgs 51/2018 da Direttiva privacy 2016/680

Per chi si fosse dimenticato, il GDPR (numero 679 del 2016), regolamento "generale", era accompagnato da una Direttiva "specifica" per i dati trattati dalle "autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali".

È stato quindi pubblicato nella Gazzetta Ufficiale n. 119 del 24 maggio 2018 il decreto legislativo 18 maggio 2018, n. 51 che attua la direttiva UE 27 aprile 2016 n. 2016/680. Il D.Lgs. 51/2018 entrerà in vigore l'8 giugno 2018:
- http://www.gazzettaufficiale.it/eli/id/2018/05/24/18G00080/SG.

Ringrazio lo pseudoanonimizzato Idraulico della privacy NN per aver segnalato questa novità.

****

08- Privacy: bozza di "prassi" UNI per la certificazione GDPR

Fabio Guasconi mi segnala l'avvio della consultazione pubblica per una "Prassi di riferimento" (PdR) UNI relativa alla gestione della privacy:
- http://www.uni.com/index.php?option=com_content&view=article&id=7144:gestione-della-privacy-in-ambito-digitale-progetto-di-prassi-di-riferimento-ora-in-consultazione-pubblica&catid=171&Itemid=2612.

La PdR si compone di due parti. La prima è una "linea guida", ma è in sostanza un documento organizzato male, con molti errori anche tecnici (si parla di responsabili interni, tanto per intenderci). Nel caso migliore lo dichiarerei inutile.

La seconda parte (o "sezione") è invece importante perché si propone come riferimento per le certificazioni GDPR. Ho trovato qualche punto discutibile (mi fa ridere l'idea di "inventario ripetuto" e mi fa paura la descrizione dell'ambito con la descrizione dei dispositivi rimovibili), ma mi pare un buon prodotto.

Importante segnalare che questa PdR riguarda il solo ambito ICT e quindi solo alcuni trattamenti o parti di essi.

Osservo che questa operazione è evidentemente la conseguenza della non felice storia italiana sulla "certificazione privacy", di cui scrissi a suo tempo: http://blog.cesaregallotti.it/2017/05/certificazioni-privacy-per-aziende-e-bs.html.

Ho il timore che venga fuori un'altra storia non felice. Infatti non mi risulta che il Garante abbia partecipato alla scrittura di questo documento e, se dovesse seguire il comportamento fin qui tenuto, non dovrebbe avallare uno schema nazionale, mentre Accredia vorrebbe avviare uno schema meno controverso di quello attuale. Vedremo, visto che le cose cambiano.

Per completezza segnalo che avevo chiesto di partecipare ai lavori (anche in quanto socio UNINFO), ma il promotore del gruppo di lavoro non ha voluto. Spero di non venire accusato di aver scritto dei giudizi spinto dalla delusione, ma di aver seguito lo stesso atteggiamento tenuto in altre occasioni.

Ultimissima nota: si tratta di bozze e come al solito ne sconsiglio la lettura a coloro che non hanno intenzione o che non hanno l'opportunità di partecipare attivamente alla consultazione.

****

09- GDPR: l'EDPB sostituisce il WP art. 29

Il WP Art. 29 dal 25 marzo ha passato le proprie funzioni all'European Data Protection Board o EDPB. Il sito è questo: https://edpb.europa.eu/edpb_it.

Al momento non vedo migrate tutte le linee guida e le Opinion (per esempio non trovo quella sul consenso). Se ho capito correttamente, dovremmo trovare tutto in questa pagina:
- https://edpb.europa.eu/guidelines-relevant-controllers-and-processors_en.

Franco Vincenzo Ferrari di DNV GL mi ha segnalato questo altro articolo dal titolo "Il nuovo Comitato europeo per la protezione dei dati (Edpb), dopo il Gdpr: compiti e poteri":
- https://www.agendadigitale.eu/sicurezza/il-nuovo-comitato-europeo-per-la-protezione-dei-dati-edpr-dopo-il-gdpr-compiti-e-poteri/.

L'articolo si concentra soprattutto sulla struttura e l'organizzazione dell'EDPB. Io sono più interessato ai lavori di redazione e pubblicazione delle linee guida e mi sono iscritto all'RSS Feed.

Intanto l'EDPB ha pubblicato una linea guida definitiva (sulle deroghe ai trasferimenti internazionali) e una bozza (sulle certificazioni; peraltro lo stato di bozza è segnalato solo dal sito, non dal documento stesso).

****

10- Informativa per i cookies dei social network

Chiara Ponti degli Idraulici della privacy ha segnalato una interessante sentenza della Corte di giustizia dell'Unione europea. Prima il link al Comunicato stampa:
- https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-06/cp180081it.pdf.

In poche parole: l'autorità Garante di un Land tedesco (in Germania c'è un Garante per Land!) ha chiesto di bloccare la fanpage di Facebook di un'organizzazione perché né l'organizzazione né Facebook informavano compiutamente gli iscritti di Facebook sull'uso dei cookies. La sentenza specifica che, in questo caso, Facebook e l'organizzazione devono essere considerati contitolari del trattamento.

Questo credo ponga un problema: come deve fare l'organizzazione a pubblicare l'informativa su Facebook? Non ho controllato, ma credo e spero che Facebook si sia già adeguata. Da qualche parte anche le organizzazioni che usano i social devono specificare la contitolarità e questo non sempre saprei farlo (devo pensare anche al mio blog).

****

11- GDPR: Perché avere un DPO certificato (risposte)

Nel mio post dal titolo "GDPR: Perché avere un DPO certificato" (http://blog.cesaregallotti.it/2018/04/perche-avere-un-dpo-certificato.html), avevo ripetuto la domanda di Monica Perego: qual è il documento legislativo che stabilisce come la fornitura di un bene o la prestazione di un servizio, eseguita in conformità a norme UNI, CEI od equivalenti norme europee od internazionali, costituisce fornitura o prestazione a "regola d'arte"?

Alcuni mi hanno risposto (con toni anche accesi) che non esiste, per lo meno applicabile al DPO.

La risposta più interessante me l'ha inviata Mauro Caio di Emaze e la copio qui di seguito.

<< Il primo riferimento normativo che io ricordi e che ha spianato la strada alla legislazione in merito a Stato dell'arte e Norme (in quel caso CEI – Comitato Elettrotecnico Italiano) risale al 1968 (L. Legge 1 marzo 1968, n. 186). Il ricordo risale a quando ho avuto modo di partecipare ai lavori del CEI 64 (impianti elettrici) e 62-5 (apparecchiature elettromedicali).

Un buon link è https://www.certifico.com/news/22-news/news-generali/1956-regola-dell-arte-i-riferimenti-normativi>>.

Raccomando l'articolo perché è molto interessante, anche se applicabile ad altro contesto. Forse Biasiotti intendeva proprio quei "documenti legislativi", anche se non so (per ignoranza) quanto l'analogia possa reggere.

****

12- Check list su privacy dell'autorità norvegese

Sabrina Prola mi ha segnalato "una guida semplice ma utile su privacy by design e default" pubblicata dalla DPA norvegese:
- https://www.datatilsynet.no/en/regulations-and-tools/guidelines/data-protection-by-design-and-by-default/.

È una guida molto interessante e molto ampia, anche se affronta i vari elementi in modo estremamente sintetico.

****

13- Rettifiche al GDPR

Sono state pubblicate le ultime rettifiche al GDPR. Per visualizzarle, si può ricercare nella pagina di Eur Lex: https://eur-lex.europa.eu/homepage.html?locale=it.

Si tratta di correzioni, quindi nulla di sostanziale.

Il testo consolidato purtroppo non è ancora disponibile.

****

14- 25 maggio 2018: Privacy Spam Day

Non me lo aspettavo, ma il 25 maggio non è il "GDPR day", ma il "Privacy Spam Day":
- tutti i clienti mi hanno inviato la loro email "noi abbiamo a cuore la tua privacy" (spesso di 6 o 7 pagine, quando convertita in un pdf formato A4);
- tutti i mittenti di spam mi hanno chiesto di confermare la sottoscrizione al loro spam;
- tanti editori di newsletter tecniche mi hanno chiesto di confermare la sottoscrizione alla loro newsletter;
- tutti i clienti mi hanno inviato la loro "nomina a responsabile", inclusa la richiesta di nominare un DPO (spesso di 5 o 6 pagine e con un peso di almeno 2MB);
- tutti i fornitori mi hanno inviato la loro "auto-nomina a responsabile", inclusa la richiesta di non chiedere troppi dettagli sulle loro misure di sicurezza, ma di fidarmi di loro e firmare il contratto.

Oggi ero da un cliente per risolvere i suoi ultimi dubbi e anche lui ha ricevuto tanto Privacy Spam.

E tutti i miei clienti hanno ricevuto Privacy Spam e me l'hanno inoltrato per chiedermi cosa fare di volta in volta.

Io ho anche avuto il tempo di scrivere un reclamo al Garante e qualcuno ha a sua volta inviato un reclamo al mio cliente (quello con cui stavo risolvendo gli ultimi dubbi).

E dimenticavo: tutti i miei contatti hanno scritto messaggi arguti sul GDPR (o inviato immagini) su Whatsapp, Facebook, LinkedIn e Twitter. Come sto facendo io adesso!

Quindi: spero che tutti i miei amici, colleghi, contatti e follower abbiamo passato un buon Privacy Spam Day!

****

15- GDPR e i ritardi dei "guru"

Scusate lo sfogo che segue.

Tutto nasce da questo post di Pizzetti su LinkedIn (segnalatomi dagli Idraulici della privacy e anche da Fabrizio Morandi), molto critico sulle certificazioni privacy:
https://www.linkedin.com/feed/update/urn:li:activity:6407501108947886080.

Non posso fare altro che essere d'accordo con Pizzetti.

Dico le stesse cose (anche se peggio e meno autorevolmente) da anni. E chiunque aveva le competenze adeguate avrebbe dovuto dirle da subito (da quando nel 2012 hanno cominciato a dire che il GDPR sarebbe stato approvato "domani", nel 2014 hanno promosso le "certificazioni DPO", nel 2016 le "certificazioni GDPR per le aziende").

E da ieri bisognava dire che non va chiesto il DPO (a norma di GDPR) in tutte le organizzazioni, non va fatta la PIA per ogni trattamento e non vanno inviate "nomine" a responsabile come se fossero spam.

Scusate lo sfogo, ma sono sicuro di non essere il solo che dice queste cose da anni (non sono particolarmente intelligente, competente o attento), ma la sensazione di esserlo c'è... E allora dove stanno tutti questi guru che non fanno chiarezza come dovrebbero? Forse troppo interessati a vendere corsi, consulenze o chissà che altro?

PS: avrei voluto tirare qualcosa a Modafferi (una gomma, una pallina di carta) quando in un intervento ha detto che per il Garante il Responsabile è sempre stato "esterno"... ma non ce lo hanno detto fino a pochi mesi fa. E chi in questi anni faceva notare che i requisiti del Codice erano incongruenti se applicabili a responsabili interni e esterni?

****

16- GDPR: qualche orrore (continuazione)

Dopo il mio post dal titolo "GDPR: qualche orrore" (http://blog.cesaregallotti.it/2018/05/gdpr-qualche-orrore.html), altri mi hanno segnalato delle chicche.

La prima è stata Miriam Carmassi (grazie!) direttamente sul mio blog: "tra gli orrori...dare data certa al registro dei trattamenti e al resto della documentazione predisposta mediante autoinvio per posta ordinaria... gli orrori del passato ritornano questa volta in nome del principio dell'accountability".

Aggiungo che io tutta questa accountability che permea il GDPR non la vedo. Il termine è usato solo una volta, ma la frase "l'accountability permea il GDPR" è ormai diventata un classico. Le responsabilità erano comunque stabilite prima (anche se il termine "accountability" non appariva) e sono stabilite adesso e sono comunque materia importante.

Ultimo aggiornamento: un mio cliente (per un lavoro non correlato al GDPR, per il quale aveva già trovato un consulente) mi ha inviato via email, in quanto fornitore, un'informativa con richiesta di ritornare firmata. Come rendere dannoso un adempimento già non utile.

****