Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – DICEMBRE 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.

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

****

00- Editoriale di auguri

Come ogni anni, approfitto della newsletter per fare gli auguri di Buon Natale e Buon anno nuovo a tutti (ci sarebbe anche l'epifania, ma poi qualcuno potrebbe interpretare male). So che ci sono altre feste in questo periodo, ma la mia ignoranza è troppa per elencarle. Ad ogni modo, a tutti, di qualunque fede siano, vanno i miei auguri.

Mi scuso per il ritardo di questa newsletter, ma nelle ultime due settimane ho subito un picco di lavoro che mi ha impedito di tener fede a questo impegno. Ora ce l'ho fatta e potrò godermi appieno le festività.

Grazie a quanti mi seguono e continuano a seguirmi.

****

01- VERA 4.4 per ISO/IEC 27001 e privacy

Ho pubblicato VERA 4.4 per ISO/IEC 27001 e privacy. Si trovano sul mio sito:
- http://www.cesaregallotti.it/Pubblicazioni.html.

Ringrazio per i suggerimenti: Nicola Nuti, Roberto Obialero, Antonio Salis.

Ora mi dedicherò al VERA "solo privacy", che sarà una "riduzione" di questo VERA.

Come sempre: vi prego di farmi sapere se trovate errori (temo ce ne siano tanti) o avete suggerimenti. Inoltre: chi vorrà vedere la bozza di VERA "solo privacy", me lo faccia sapere che lo invio appena pronto.

Segnalo che ho cambiato un poco il VERA "solo 27001": Roberto Obialero mi ha suggerito di cambiare alcune descrizioni di minaccia che ho accolto (ma non ho cambiato versione al file, consapevole che non ho seguito la pratica corretta).

****

02- Modifiche al Codice privacy

E' stata pubblicata in Gazzetta Ufficiale la Legge 167 del 20 novembre 2017:
- www.gazzettaufficiale.it/eli/id/2017/11/27/17G00180/sg.

Qui ci sono alcuni punti interessanti (e criticabili):

- l'articolo 24 stabilisce che ora i dati di traffico telematico vanno conservati per 72 mesi (6 anni), mentre in precedenza la durata era di massimo 2 anni; in tanti dicono che è follia; io non ho ancora capito se in questi anni questi dati sono serviti;

- l'articolo 28 allinea la nomina di responsabile del trattamento a quanto previsto dal GDPR, sicuramente inutilmente (e senza una ragione apparente), visto che tra pochi mesi entrerà in vigore proprio il GDPR e quindi questa modifica non era proprio necessaria;

- sempre l'articolo 28 prevede che il Garante pubblichi "schemi tipo" per stipulare accordi con i responsabili; ad ora mi risulta siano disponibili solo quelli per il trasferimento dei dati extra-UE; mi pare un po' strano questo obbligo di usare "schemi tipo" (la formulazione del requisito non mi pare lasci margini di manovra); Pierfrancesco Maistrello mi segnala che forse questo è per evitare che i contratti stipulati oggi con la PA siano messi in discussione a maggio;

- sempre l'articolo 28 impone restrizioni nel riutilizzo dei dati per finalità di ricerca scientifica o per scopi statistici; ci sono un paio di questioni bizzarre: la richiesta di autorizzazione preventiva al Garante, nonostante il GDPR, volontariamente, non la preveda più, e l'introduzione del silenzio-rigetto (ulteriore aberrazione);

- l'articolo 29 stanzia maggiori fondi al Garante e permette l'aumento di organico (mi viene da pensare che prevedono maggiori introiti grazie alle nuove sanzioni amministrative).

Sembra che questo non sia il provvedimento per allineare la 196 al GDPR. Per quello dovremo aspettare un altro atto.

****

03- DPO: le raccomandazioni del Garante e qualche articolo

Il (solito) Pierfrancesco Maistrello mi ha segnalato che il Garante ha aggiornato le faq sul DPO ed emanato uno schema tipo di nomina e un modello per comunicare al garante gli estremi del DPO:
- http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/7322110.

La notizia è poi finita sulla newsletter del Garante, ma Pierfrancesco me l'ha fornita con largo anticipo insieme a qualche commento che io riprendo:

- lo schema di nomina del DPO è standard, quindi non lascia spazio a nulla di eccitante, ma è comunque comodo;
- la nomina del DPO per società in-house o partecipate di PA non è obbligatoria, ma fortemente consigliata;
- la posizione del DPO interno (dirigente, o "funzionario di alta professionalità", che sia in contatto con il vertice) non sembra di immediata individuazione in tutte le tipologie di PA;
- certificazioni DPO: utili solo come indicazione di competenze;
- come si nomina: schema tipo, più comunicazioni al garante dei suoi estremi;
- interessante notare che: il DPO nelle FAQ del Garante è sempre una persona fisica;
- può esserci più di un DPO? domanda interessante per le grandi PA, ma la risposa è NO, il DPO è uno, gli altri sono figure di supporto per lui (sia interno che esterno);
- cosa può fare il DPO oltre a quello che prevede la normativa? Difficile dirlo, visto che questo punto è in garantese stretto, che non dice nulla di nuovo, ma conferma che è il titolare a decidere se assegnare altri compiti a figure già ingolfate di attività (ad esempio il responsabile per la prevenzione della corruzione o altri ruoli) o come assegnare compiti in assenza di conflitto di interessi.

In definitiva, le FAQ diradano qualche nebbia, ma non completamente.

Pierfrancesco mi ha anche segnalato tre begli articoli (in inglese) su come scegliere il DPO.

Il primo ha titolo "What skills should your DPO absolutely have?":
- https://iapp.org/news/a/what-skills-should-your-dpo-absolutely-have/.

Il secondo ha titolo "Outsourcing your DPO: Questions to ask":
- https://iapp.org/news/a/what-to-ask-your-potential-dpo/.

Il terzo ha titolo "How to contract with your outsourced DPO":
- https://iapp.org/news/a/how-to-contract-with-your-outsourced-dpo/.

Aggiungo che sappiamo bene che il DPO non è sempre necessario in tutte le organizzazioni. Però le stesse cose sono applicabili (con pochi cambiamenti) anche ai consulenti privacy e (con maggiori cambiamenti) a tutti gli altri consulenti.

****

04- Strumento PIA del CNIL

L'autorità francese per la privacy (il CNIL), ha pubblicato uno strumento per realizzare le PIA:
- https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment.

La segnalazione mi arriva da Pierfrancesco Maistrello, che l'ha analizzato molto rapidamente e l'ha trovato facile da usare.

Personalmente rilevo che le misure di sicurezza da considerare non sono incluse nel prodotto (ho analizzato la versione beta, quella disponibile ad oggi). Queste sono comunque presenti nelle linee guida sempre del CNIL (già segnalate a suo tempo):
- https://www.cnil.fr/en/guidelines-dpia.

In definitiva mi sembra uno strumento che aiuta la scrittura del rapporto; una sorta di "indice sofisticato". Non voglio ridurre l'importanza di questo strumento, che rappresenta un punto di vista autorevole e di buona qualità. Anzi, sono contento che questo prodotto sia stato progettato considerando le reali necessità degli utilizzatori, e non le elucubrazioni di qualche "saggio nella torre d'avorio" (come siamo troppo spesso a vedere in troppi documenti o prodotti italiani quando si parla di conformità a normative).

****

05- Certificazioni privacy

Il 30 novembre 2017, ad un convegno organizzato dal Dipartimento di scienze giuridiche dell'Università degli studi di Milano, ho fatto una presentazione sullo stato delle certificazioni privacy. Si trova a questo indirizzo:
- http://www.cesaregallotti.it/Pubblicazioni.html.

Già la sera stessa era vecchia perché era giunta la notizia della pubblicazione della UNI 11697 sulle certificazioni delle competenze in materia di privacy (vedere oltre).

Poco dopo Paolo Sferlazza di @ mediaservice mi ha segnalato il documento dell'ENISA dal titolo "Recommendations on European Data Protection Certification":
- https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification.

Qualche interpretazione del documento:
1- la certificazione richiamata dal GDPR non è per prodotti, ma per "elaborazioni di dati" (processing of data); la certificazione può includere prodotti, sistemi o servizi, ma nell'ambito di trattamenti effettuati; il mercato potrebbe comunque proporre schemi di certificazione per prodotti;
2- gli enti di Accreditamento potrebbero sviluppare schemi propri, senza l'appoggio dell'autorità garante e che non è necessario l'appoggio del board dei garanti europei (interpretazione che io e altri non condividiamo).

Ad ogni modo, il documento è molto criticabile perché, in definitiva, non presenta correttamente le certificazioni dei sistemi di gestione (lascia intendere che le certificazioni ISO/IEC 27001 riguardano solo la presenza di procedure, non la loro efficacia; ma questo è palesemente falso).

****

06- UNI 11697 per le certificazioni delle competenze privacy

E' stata pubblicata la UNI 11697:2017, che definisce le competenze dei professionisti che si occupano di privacy.

Credo che l'articolo su Linea EDP sia più che esplicativo (anche dove ricorda il far west:
- http://www.lineaedp.it/news/33253/attivita-professionali-non-regolamentate-la-norma-uni/.

Dove comprarla:
- http://store.uni.com/catalogo/index.php/uni-11697-2017.html.

Qualche nota amena:
- grazie a Pietro degli Idraulici della privacy e Franco Ferrari per avermi dato la notizia per primi;
- Monica Perego ha fatto notare che il numero della norma UNI (finisce per 697) è un anagramma del numero del GDPR (679);
- il giorno stesso della pubblicazione avevo tenuto una presentazione in cui avevo detto "chissà quando sarà pubblicato"; accipicchia!

****

07- GPG 2018 per la business continuity

È stata pubblicata la nuova versione delle Good practice guidelines del BCI:
- https://www.thebci.org/training-qualifications/good-practice-guidelines.html.

Sono il riferimento per quanto riguarda la business continuity e mi sembrano ben fatte.

****

08- IoT: Raccomandazioni ENISA e un caso

Alessandro Cosenza di BTicino mi ha segnalato questa pubblicazione di ENISA (l'ente europeo per la sicurezza IT) dal titolo "Baseline Security Recommendations for IoT" a cui ha collaborato:
- https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot.

Personalmente penso si sarebbe potuto fare ancora di più, specificando meglio le misure di sicurezza suggerite. Però mi rendo conto che non è questo l'obiettivo di questo documento.

Devo dire che il documento è molto interessante e c'è molto materiale da studiare.

I problemi sull'IoT comunque sono molti. Per esempio non sapevo neanche esistessero chiavi di casa di questo tipo (Amazon Keys): per facilitare le consegne (e non lasciare il pacco di Amazon fuori casa), Amazon si è inventato le serrature che può aprire autonomamente. Quindi, nel caso più "automatizzato", il trasportatore segnala ad Amazon e al cliente che è fuori dalla porta, arriva un SMS al cliente che può guardare cosa succede con una webcam fornita da Amazon stessa, Amazon apre la porta a distanza, il trasportatore lascia il pacco appena dentro casa e poi chiude la porta.

Tutto ciò mi dà i brividi, per motivi che dovrei ben capire. Però il timore che tutto questo meccanismo possa essere attaccato è uno dei motivi. Parte di esso, ossia la telecamera, lo è già stato:
- https://www.wired.com/story/amazon-key-flaw-let-deliverymen-disable-your-camera/.

Ho seguito dei progetti in ambito IoT e so che parte delle persone che sviluppano queste cose sono professionali e preparate. Ma non tutte. E comunque penso che troppa automazione, oltre a ridurre le nostre capacità di elaborazione mentale, aumenti eccessivamente le possibilità di attacco. Forse è un problema solo mio.

****

09- Il caso Uber

Prendo spunto da questi due articoli di DarkReading:
- https://www.darkreading.com/attacks-breaches/ubers-security-slip-ups-what-went-wrong/d/d-id/1330496;
- https://www.darkreading.com/application-security/git-some-security-locking-down-github-hygiene/d/d-id/1330511.

Il primo riassume il caso Uber: a ottobre 2016 dei malintenzionati sono riusciti a raccogliere i dati di 57 milioni di autisti e clienti di Uber; Uber li ha pagati 100mila dollari per cancellare i dati rubati e non divulgare la notizia. La notizia si è però diffusa e Uber è ritenuta colpevole di non aver avvisato gli interessati della violazione (misura del GPDR, nuova per alcuni, ma già presente in altre normative).

Il secondo articolo discute le questioni tecniche, altrettanto interessanti. Gli sviluppatori usavano un ambiente GitHub, in cui archiviavano codice e dati, inclusi quelli poi compromessi. Qui i punti dolenti sono vari: gli sviluppatori non avrebbero dovuto avere accesso a quella mole di dati, né salvarli in un ambiente non completamente controllato.

GitHub ha sicuramente messo a disposizione degli sviluppatori una serie di strumenti per assicurare la sicurezza dei dati (controllo di assenza di dati critici, di configurazioni e di credenziali, il controllo accessi solo a utenti "aziendali" e non "pubblici", l'impostazione degli archivi come "privati", la possibilità di verificare le autorizzazioni, la possibilità di attivare la strong authentication), ma probabilmente non erano stati attivati (ci si chiede anche se l'uso di GitHub era stato in qualche modo analizzato dai responsabili della sicurezza di Uber, oppure se era un'iniziativa degli sviluppatori).

****

10- Mio articolo "ISO/IEC 27018: Cloud e Privacy"

Su ICT Security è stato pubblicato il mio articolo dal titolo "ISO/IEC 27018: Cloud e Privacy": https://www.ictsecuritymagazine.com/articoli/isoiec-27018-cloud-privacy/.

****

11- Sicurezza informatica (per i singoli)

Questo mese Bruce Schneier, nella sua newsletter, suggerisce alcune guide per la sicurezza dei dispositivi personali (pc Windows e Mac, Android, iPhone) e la navigazione Internet. Diffondo i suoi suggerimenti:
- https://motherboard.vice.com/en_us/article/d3devm/motherboard-guide-to-not-getting-hacked-online-safety-guide;
- https://ssd.eff.org/en;
- https://www.johnscottrailton.com/jsrs-digital-security-low-hanging-fruit/;
- https://www.frontlinedefenders.org/en/resource-publication/digital-security-privacy-human-rights-defenders.

Sono tutti piuttosto lunghi, anche se (ovviamente) non difficili.

Inoltre mi ha scritto John Mason (trovandomi su Google) per segnalarmi questo suo articolo, che è decisamente semplice e quindi un ottimo punto di partenza:
- https://thebestvpn.com/online-privacy-guide/.

****

12- Il tracciamento delle email

Per un Natale sempre più sereno, ecco qui un articolo (sempre segnalato dalla newsletter di Bruce Schneier) sul tracciamento delle email:
- https://www.wired.com/story/how-email-open-tracking-quietly-took-over-the-web/.

Mi chiedevo come MailUp faccia a dirmi quante persone hanno aperto la mia newsletter. Ora lo so. Ma so anche che non è solo MailUp che fa uso di questi meccanismi. Anzi: il 40% del traffico email è tracciato. E permette di sapere che le email indirizzate al CEO di Apple sono aperte con un pc Windows.

****