Cesare Gallotti

**********

**IT SERVICE MANAGEMENT NEWS – GENNAIO 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**

01- Privacy: Divieto di GPS per i lavoratori
02- Privacy e Registro delle opposizioni
03- Privacy: La notificazione al Garante dei trattamenti
04- Proposta di nuovo Regolamento privacy sulle comunicazioni elettroniche
05- Privacy: Linee guida DPO
06- Privacy: PIA e le proposte di ISO/IEC 29134 e ICO
07- Europa: contro la conservazione dei dati di traffico
08- Certificazione conservatori e SPID
09- Atti sottoscritti con Firma Elettronica Avanzata
10- Fattura b2b dal 9 gennaio
11- Nuova ISO/IEC 27004:2016 sulle misurazioni della sicurezza
12- Chiarimenti sulla "certificazione" di Lead auditor
13- Misurazioni e pulizie
14- Documenti ENISA su privacy on line, pagamenti elettronici, aeroporti, automobili
15- Eye Piramid
16- Procure e fornitori IT privati
17- Industria 4.0
18- Alternative a TrueCrypt

**********

## 01- Privacy: Divieto di GPS per i lavoratori

Dalla newsletter di Filodiritto segnalo la seguente notizia: "GPS - Ispettorato Nazionale del Lavoro: è vietato l'utilizzo del sistema GPS sull'auto aziendale senza un accordo sindacale". L'Ispettorato, il 7 novembre 2016, ha infatti pubblicato la circolare 2/2016 in merito all'uso di GPS:
- http://www.filodiritto.com/news/2017/gps-ispettorato-nazionale-del-lavoro-e-vietato-lutilizzo-del-sistema-gps-sullauto-aziendale-senza-un-accordo-sindacale.html.

Ricordo alcune notizie correlate all'uso di GPS:
- moduli per la richiesta di autorizzazione all'uso di GPS (http://blog.cesaregallotti.it/2016/05/modulo-unificato-per-videosorveglianza.html);
- possibilità di usare il GPS per rilevare abusi o usi illeciti di strumenti aziendali (http://blog.cesaregallotti.it/2015/11/nuovo-statuto-dei-lavoratori-riflessioni.html), forse in contrasto con la recente circolare.

**********

**02- Privacy e Registro delle opposizioni**

Oggi la normativa italiana vigente prevede che le chiamate telefoniche per finalità di marketing diretto possano essere fatte ai numeri disponibili su elenchi pubblici (l'elenco del telefono, per intenderci), a meno che l'utente non eserciti il "diritto di opt-out", iscrivendosi al Registro delle opposizioni (io l'ho fatto, ma ancora troppe volte ricevo telefonate indesiderate).

Il nuovo Regolamento europeo sulla privacy (GDPR) non prevede questa possibilità. Quindi, un'azienda che vuol fare marketing diretto telefonico deve lavorare con il consenso degli interessati.

Rimarrà però il solito alibi: "il numero di telefono, forse, non è un dato personale". A questo problema dovrà rispondere, se mai vedrà la luce, il futuro Regolamento ePrivacy, recentemente proposto dalla Commissione europea.

Ringrazio Pierfrancesco Maistrello, che mi ha confermato la mia conclusione, approfondendola.

Articolo anche su: http://europrivacy.info/it/2017/01/17/direct-marketing/.

**********

**03- Privacy: La notificazione al Garante dei trattamenti**

Rileggendo il GDPR (Regolamento europeo sulla privacy), mi sono accorto che non ho trovato traccia della "notificazione al Garante" di alcuni trattamenti, prevista dalla precedente Direttiva 95/46/CE.

In effetti, la notificazione risulta un concetto superato ed è sostituito con la Valutazione d'impatto sulla protezione dei dati o Data protection impact assessment (spesso anche indicata con i termini privacy impact assessment o PIA).

Infatti, nei considerando del Regolamento (dall'89) si legge che la notificazione "non ha sempre contribuito a migliorare la protezione dei dati personali".

I titolari saranno tenuti ad effettuare delle PIA per i trattamenti più critici e, nel caso dovessero rilevare rischi molto elevati, chiedere di propria iniziativa un parare al Garante (supervisory authority).

Ciascun Stato potrà chiedere che alcuni trattamenti non siano attivati senza il parere del Garante.

Ringrazio Pierfrancesco Maistrello di Vecomp, perché è lui che mi ha fornito la risposta al mio dubbio.

Articolo anche su: http://europrivacy.info/it/2017/01/17/notification-to-the-supervisory-authority/.

**********

**04- Proposta di nuovo Regolamento privacy sulle comunicazioni elettroniche**

Fornisco la notizia (e ringrazio Pierfrancesco Maistrello di Vecomp) che la Commissione Europea vuole proporre un nuovo Regolamento, da affiancare al GDPR (Regolamento europeo sulla privacy) e sostitutivo della Direttiva 2002/58 (Direttiva ePrivacy, nota soprattutto per il Provvedimento sui cookies), in merito alle comunicazioni elettroniche:
- https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

Come al solito, i tempi sono incerti e il testo finale potrà essere molto diverso da quello ora proposto. Come per il GDPR, fioccheranno corsi (a pagamento) e consulenti agitati. Io, come già feci per il GDPR (ma senza molto successo), consiglio di aspettare la pubblicazione del testo definitivo.

Per chi vuole approfondire un po' di più sul contenuto della proposta, segnalo questo articolo di Europrivacy:
- http://europrivacy.info/it/2017/01/12/italiano-pronta-la-proposta-di-regolamento-su-privacy-e-comunicazioni-elettroniche/.

Infine, un mio lettore anonimo mi ha segnalato 6 comunicati stampa, tutti del 10 gennaio, della Commissione Europea e pertinenti proposte su privacy, data economy e servizi elettronici ai cittadini. Sia io che il mio lettore preferiamo non dedicare troppo tempo a proposte che poi non si sa bene in che tempi e in che modi finiranno. Però magari altri sono curiosi:
- http://europa.eu/rapid/press-release_IP-17-5_en.htm;
- http://europa.eu/rapid/press-release_IP-17-16_en.htm;
- http://europa.eu/rapid/press-release_IP-17-23_en.htm;
- http://europa.eu/rapid/press-release_MEMO-17-6_en.htm;
- http://europa.eu/rapid/press-release_MEMO-17-15_en.htm;
- http://europa.eu/rapid/press-release_MEMO-17-17_en.htm.

**********

**05- Privacy: Linee guida DPO**

Elisa Fontanelli mi ha segnalato la pubblicazione delle "prime linee guida dei Garanti europei", così come proposte dal nostro Garante:
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5792160.

La più interessante è quella sui DPO, proposta dal WG Art. 29. In particolare, mi sembrano importanti alcuni chiarimenti in merito a chi deve obbligatoriamente nominare un DPO.

Alcuni chiarimenti su:
- http://europrivacy.info/it/2017/01/09/dpo-fulfilling-other-tasks-and-conflict-of-interests-in-wp29-guideline-wp243-isaca-frameworks-are-helpful-tools-to-better-define-internal-segregation-of-duties/.

**********

**06- Privacy: PIA e le proposte di ISO/IEC 29134 e ICO**

Un mio articolo su Europrivacy su PIA e le proposte di ISO/IEC 29134 e ICO:
- http://europrivacy.info/it/2017/01/17/pia-and-proposals-from-isoiec-29134-and-ico/

**********

**07- Europa: contro la conservazione dei dati di traffico**

Da Filodiritto segnalo la seguente notizia: "Privacy - Corte di Giustizia dell'Unione Europea: gli Stati membri non possono imporre un obbligo generale di conservazione di dati ai fornitori di servizi di comunicazione elettronica":
- http://www.filodiritto.com/news/2017/privacy-corte-di-giustizia-dellunione-europea-gli-stati-membri-non-possono-imporre-un-obbligo-generale-di-conservazione.html.

Non credo che questa sentenza abbia impatti sul nostro Dlgs 109 del 2008, ma forse sarà aggiornato.

**********

**08- Certificazione conservatori e SPID**

Accredia ha pubblicato le regole per la certificazione dei conservatori e dei gestori SPID, sulla base di quanto concordato con AgID:
- http://www.accredia.it/news_detail.jsp?ID_NEWS=2356&areaNews=95&GTemplate=default.jsp.

Per chi vuole essere qualificato da AgID come conservatore o gestore SPID, rimane il percorso in due fasi: prima una certificazione da parte di un Organismo di certificazione accreditato (da Accredia) e poi la domanda ad AgID.

In questo modo si allineano le procedure per i servizi fiduciari previsti dal Regolamento europeo eIDAS e quelli più specificatamente italiani (SPID e conservazione).

Ringrazio Andrea Caccia per la segnalazione di questa importante notizia.

**********

**09- Atti sottoscritti con Firma Elettronica Avanzata**

Andrea Caccia mi ha segnalato il suo articolo "Atti sottoscritti con Firma Elettronica Avanzata: il rischio nullità":
- https://www.linkedin.com/pulse/atti-sottoscritti-con-firma-elettronica-avanzata-il-rischio-caccia.

Tratta della validità legale della firma elettronica avanzata e del rischio nullità nel caso in cui un soggetto non fosse in grado, in caso di contenzioso, di dimostrare che la propria soluzione risponda ai requisiti previsti dalle regole tecniche.

È un articolo piuttosto tecnico sulla validità delle FEA dopo la pubblicazione di eIDAS e del nuovo Codice dell'amministrazione digitale. Per chi non è addetto ai lavori, però, questo articolo ricorda che purtroppo l'uso di "nuove tecnologie" ha dei rischi, visto che la legislazione non è (ancora) stabile.

**********

**10- Fattura b2b dal 9 gennaio**

Dal 9 gennaio è partita la fattura elettronica tra privati. Ecco un articolo di Andrea Caccia e Daniele Tumietto che presenta l'iniziativa e i suoi problemi da un punto di vista teorico e poi pratico:
- http://www.agendadigitale.eu/fatturazione-elettronica/parte-la-fattura-elettronica-tra-privati-ma-e-un-caos-ecco-che-fare_2811.htm.

**********

**11- Nuova ISO/IEC 27004:2016 sulle misurazioni della sicurezza**

È stata pubblicata la ISO/IEC 27004:2016, dal titolo "Information security management -- Monitoring, measurement, analysis and evaluation":
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=64120.

Questa norma sostituisce la precedente versione del 2009 e mi trova maggiormente soddisfatto.

In particolare, è stata ridotta moltissimo la parte teorica. In questo modo è più facile interpretare il requisito della ISO/IEC 27001 e cogliere indicazioni su come applicarlo.

Ancora più importanti sono i 35 esempi finali, che forniscono un valido punto di partenza per chi vuole attuare un sistema di gestione per la sicurezza delle informazioni. Ne approfitto per dire che ho apprezzato moltissimo l'idea di dedicare più di metà della norma agli esempi, piuttosto che alla teoria (io poi ho contribuito con qualche esempio, poi migliorato e inserito nel documento finale dal gruppo di lavoro).

In particolare molti di questi esempi suggeriscono un approccio meno fantasioso (e più utile) di alcuni che ho visto negli anni, che prevedevano troppi numeri da presentare alla Direzione, senza interrogarsi sulla loro reale validità. Qui si dimostra che non è necessario seppellire un'azienda sotto troppi numeri, soprattutto quando è di dimensioni ridotte.

Ricordo infine due cose:
1- questa è una linea guida e quindi può essere presa come punto di partenza per riflettere sul tema delle misurazioni della sicurezza; non può essere usata come insieme di requisiti da attuare per la certificazione ISO/IEC 27001 (anche perché gli unici requisiti da attuare sono quelli della ISO/IEC 27001 stessa, non altri);
2- le misurazioni non possono né devono sostituire la conoscenza reale di un'organizzazione; né i manager, né i consulenti, né gli auditor devono dare troppa enfasi a questo aspetto.

**********

**12- Chiarimenti sulla "certificazione" di Lead auditor**

Segnalo questo articolo di Fabrizio Cirilli dal titolo "Certificazione degli auditor/lead auditor per la ISO/IEC 27001: c'è ancora troppa confusione!":
- http://www.ictsecuritymagazine.com/articoli/certificazione-degli-auditorlead-auditor-la-isoiec-27001-ce-ancora-troppa-confusione/.

Trovo sia importante che quanti richiedono titoli di competenza sappiano di cosa si sta parlando. A mio avviso, Fabrizio ha ben colto il punto.

Nota personale: questo articolo lo lessi a fine novembre su LinkedIn; preso da pigrizia non l'avevo segnalato. Provvedo adesso, seppure un po' in ritardo, grazie ad un tweet di @sramakk, che ringrazio.

**********

**13- Misurazioni e pulizie**

In questi giorni, mi hanno raccontato un esempio di misurazioni fallaci che mi sembra interessante.

Il personale delle pulizie degli hotel è spesso misurato unicamente in base al tempo (molto basso) impiegato a pulire le camere. Questo però ha creato problemi non tanto di pulizia (gli addetti sono comunque dei professionisti), ma di manutenzione, visto che il personale, considerate le misure, non aveva tempo per segnalare i problemi riscontrati. E i consulenti e gli auditor che sono spesso in albergo sono ben consapevoli di questo problema. In effetti mi è sempre sembrato stupido trovare camere bellissime e ben pulite, ma con lampadine rotte, gli scarichi lenti, le porte cigolanti, le docce piene di calcare.

Alcuni hotel hanno finalmente capito che la velocità e la "misura esatta" non sono tutto, anche se costituiscono un parametro da considerare insieme ad altri (per esempio, le lamentele degli ospiti relative a problemi non segnalati).

**********

**14- Documenti ENISA su privacy on line, pagamenti elettronici, aeroporti, automobili**

Fabio Teoldi, che ringrazio, mi ha segnalato che ENISA a dicembre 2016 e gennaio 2017 ha pubblicato 4 documenti interessanti.

1- "PETs controls matrix - A systematic approach for assessing online and mobile privacy tools": misure da applicare (o da verificare) per assicurare la privacy nei sistemi online (soprattutto siti web e applicazioni per dispositivi mobili):
- https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-controls-matrix-a-systematic-approach-for-assessing-online-and-mobile-privacy-tools.

2- Security of Mobile Payments and Digital Wallets: uno studio di 3 piattaforme (Apple Pay, Google Wally e Android Pay, Samsung Pay) seguito da alcune raccomandazioni (troppo poche, a mio avviso):
https://www.enisa.europa.eu/publications/mobile-payments-security.

3- Securing Smart Airports: un elenco di 44 controlli di sicurezza applicabili ai sistemi informatici per gli aeroporti (ma non solo, a mio parere):
https://www.enisa.europa.eu/publications/securing-smart-airports.

4- Cyber Security and Resilience of smart cars": un elenco di "good practices" soprattutto tecniche (precedute da troppe pagine di analisi), da considerare non solo per le automobili:
https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars/.

**********

**15- Eye Piramid**

Tutti avete sentito parlare della vicenda dei fratelli Occhionero e di Eye Piramid, i due spioni che hanno raccolto dati dai pc di persone note. Per chi vuole leggere una sintesi della storia, ecco un link:
- http://cybersecurity.startupitalia.eu/53903-20170111-eye-pyramid-the-italian-job-storia-malware-spionaggio-massoneria.

Un'analisi di Trend Micro:
- http://blog.trendmicro.com/trendlabs-security-intelligence/eye-storm-look-eyepyramid-malware-supposedly-used-high-profile-hacks-italy/.

Una sintesi tecnica (e non solo), in Italiano, di Stefano Zanero:
- https://www.facebook.com/raistolo/posts/10155658726324307.

Purtroppo non trovo articoli significativi su come difendersi da questi attacchi. Certo: c'è il pieno di articoli che dicono "state attenti ai file che aprite", ma questo non è niente di nuovo.

Ringrazio Sandro Sanna, che per primo mi ha segnalato la notizia.

**********

**16- Procure e fornitori IT privati**

La notizia è di fine novembre 2016. Se ho capito correttamente, nel 2015 la Procura di Trieste ha un guasto ai propri server usati per le intercettazioni e chiede aiuto per il recupero di un file al fornitore del servizio di assistenza informatica (Area S.p.A.). La referente di Area S.p.A. riesce a recuperare il file dal proprio pc aziendale. Dopo aver ringraziato, la Procura riflette sul fatto che copie dei file delle intercettazioni sono conservate su pc di persone esterne alla Procura stessa e avvia delle indagini:
- http://milano.corriere.it/notizie/cronaca/16_novembre_29/intercettazioni-pm-server-procure-all-azienda-informatica-5593741c-b5ac-11e6-a2c1-e1ab33bf33ae.shtml.

Due giorni dopo, il Ministero della giustizia invia una circolare alle Procure per chiedere di "alzare la soglia di allerta sulla sicurezza dei sistemi informativi delle intercettazioni":
- http://milano.corriere.it/notizie/cronaca/16_novembre_30/intercettazioni-ministero-pm-80bf5490-b678-11e6-9fa1-de32925f0429.shtml.

A gennaio si tiene presso il ministero un incontro tra i capi delle Procure per discutere del problema e vengono fuori delle preoccupazioni da parte dei presenti in merito all'accesso da remoto dei fornitori privati, alla mancanza di personale interno qualificato presso le Procure, alla mancanza di un albo delle ditte qualificate. Un procuratore si è anche vantato di aver protetto la propria infrastruttura con un "apposito firewall":
- http://milano.corriere.it/notizie/cronaca/17_gennaio_11/intercettazioni-capi-procure-1ec86626-d76d-11e6-94ea-40cbfa45096b.shtml.

Premetto che in passato ho avuto modo di conoscere Area S.p.A. e posso solo dire che: a) ho apprezzato la dichiarazione di Andrea Formenti; b) so che hanno molto a cuore la sicurezza dei dati. Di più non posso dire.

La ragione per cui presento questo caso è che rende pubblico un classico rapporto cliente-fornitore.

Da quanto scritto sui giornali, escludo che Area S.p.A. facesse raccolta dati per finalità di profilazione o simili. Se così fosse, la referente di Area S.p.A. non avrebbe palesato la possibilità di recuperare i dati.

Quindi cosa rimane? Immagino questo: il fornitore dice al cliente che sarebbe opportuno investire anche in un sistema di backup; il cliente non ritiene invece opportuna questa misura (magari, addirittura, avrà chiesto di toglierla dall'offerta per ridurre i costi); il fornitore, però, sa bene che alla prima difficoltà il cliente gli creerà dei problemi e quindi si arrangia, facendo backup su un'infrastruttura sicura (di questo ne sono certo), anche se per questo deve ricorrere ad un barbatrucco.

E, alla prima difficoltà, il cliente ha creato comunque problemi. Dimostrando anche elevata incompetenza: pensa di risolvere il problema dei backup con "apposito firewall" o con un albo di fornitori; non si chiede perché il fornitore avesse accesso incondizionato da remoto (anche se immagino perché nessuno della Procura avesse voglia di aprire e chiudere porte del firewall per consentire le manutenzioni in emergenza anche di notte); pensa di risolvere il problema, pochi giorni dopo, inviando una circolare (7 pagine che risolvono i problemi) nonostante le medesime procure abbiano chiesto numerose proroghe per adeguarsi alle prescrizioni del 2013 (!) del Garante privacy in materia di sicurezza.

Non so se Area S.p.A. ha comunicato preventivamente alla Procura di Trieste le carenze di sicurezza riscontrate (inclusa la mancanza di un sistema di backup "a regola d'arte"), ma sono convinto che finora la carenza di soldi e di competenze ha dettato le scelte dei clienti. E la colpa, come sempre e nonostante tutto, è dei fornitori.

**********

**17- Industria 4.0**

Con la Legge di stabilità 2017 (Legge, 11/12/2016 n° 232, G.U. 21/12/2016 per chi volesse cercarla su www.normattiva.it), il Governo ha prorogato un "superammortamento" e stabilito un "iperammortamento" per i beni digitali.

Queste facilitazioni sono applicabili anche a "software, sistemi, piattaforme e applicazioni per la protezione di reti, dati, programmi, macchine e impianti da attacchi, danni e accessi non autorizzati". Questa mi pare una buona iniziativa.

Tutti gli altri investimenti di tipo informatico non sono collegati ad una garanzia di sicurezza informatica e forse questa poteva essere un'occasione per migliorare il livello di sicurezza informatica delle nostre imprese.

Segnalo due articoli di sintesi di Altalex:
- http://www.altalex.com/documents/news/2016/10/17/legge-di-stabilita-2017;
- http://www.altalex.com/documents/news/2016/12/27/legge-di-bilancio-2017-la-tabella-delle-novita.

Ringrazio Edmea De Paoli del TUV Nord per le riflessioni fatte su questa Legge.

**********

**18- Alternative a TrueCrypt**

Sophie Hunt mi ha scritto perché in alcuni post ho citato TrueCrypt senza poi fornire aggiornamenti.

Lei stessa si segnala un articolo in cui ne è spiegata la storia e ne sono fornite, con descrizione dei pro e contro, alternative (VeraCrypt, Bitlocker, DiskCryptor, Ciphershed, FileVault 2 e LUKS):
- https://www.comparitech.com/blog/information-security/truecrypt-is-discoutinued-try-these-free-alternatives/.

**********