Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – SETTEMBRE 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- Migrata la newsletter

Questa è la prima spedizione della newsletter con il servizio MailUp (offerto da Team Quality S.r.l.).

Ho inviato un'altra email usando il vecchio sistema. Spero nessuno abbia dei problemi.

Invito i miei lettori a segnalarmi ogni problema e ogni errore. L'informativa è perfetta! Ma di tutto il resto non sono così sicuro (e neanche dell'informativa, per dire tutta la verità).

Grazie mille.
Cesare Gallotti

****

01- 27 settembre: DFA Open Day - GDPR e investigazioni aziendali

Io sono Consigliere di DFA e sono molto orgoglioso di presentarvi l'Open day 2017 dedicato a GDPR e investigazioni aziendali:
- http://www.perfezionisti.it/open-day/dfa-open-day-2017/.

Ci si può iscrivere gratuitamente, ma al momento in cui io sto scrivendo questo annuncio l'evento risulta "tutto esaurito". Magari si libereranno dei posti nei prossimi giorni:
- https://www.eventbrite.it/e/biglietti-dfa-open-day-2017-36684332827.

****

02- Il Garante privacy e i requisiti del DPO

La newsletter del Garante (e Franco Ferrari del DNV GL, che ringrazio) mi segnalano questo articolo dal titolo "Regolamento privacy, come scegliere il responsabile della protezione dei dati":
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6826945#1.

Mi pare divertente leggere che "Non sono richieste attestazioni formali sul possesso delle conoscenze o l'iscrizione ad appositi albi professionali". Lo dicevo da tempo.

Trovo che la corsa alle certificazioni non sempre sia giustificata. Vorrei si promuovessero dei corsi seri e dei momenti di approfondimento, anche senza certificazioni e senza spargimenti di terrore per l'entrata in vigore del GDPR.

Nota: un momento di approfondimento è quello che abbiamo organizzato come DFA (vedere articolo precedente).

****

03- Privacy e controllo lavoratori: accesso del datore di lavoro a email e IM - Sentenza Barbulescu

Interessante caso della Corte di giustizia europea che verrà ricordato, penso, come "Sentenza Barbulescu".

Vediamo se ho capito bene (in caso contrario, scrivetemi):
- Barbulescu lavora per un'azienda, che gli chiede di aprire un account all'instant messaging di Yahoo per comunicare con i clienti;
- Barbulescu usa lo stesso account per scambiare messaggi con la fidanzata e il fratello;
- l'azienda se ne accorge, si legge e stampa 45 pagine (!) di messaggi di Barbulescu e lo licenzia;
- Barbulescu fa ricorso fino alla Corte di giustizia europea;
- la Corte di giustizia europea, a dicembre 2016, dà ragione all'azienda;
- la Grand chamber of human rights, a settembre 2017, dà invece ragione a Barbulescu (comminando però una multa molto bassa).

A me interessa capire cosa ha fatto l'azienda per dimostrare la propria ragione. Ossia le misure ritenute "corrette" dai giudici. Quindi, dalla sentenza della Corte di giustizia europea, ricavo quanto segue:
- l'azienda, nel regolamento interno, aveva ben specificato che era vietato l'uso dei pc aziendali per scopi personali;
- Barbulescu aveva asserito di aver usato il proprio account Yahoo solo per scopi di lavoro (non solo mentendo, ma dichiarando quindi che Yahoo non riguardava dati personali e poi, illogicamente, da qualche punto di vista, lamentandosi dell'invasione della propria privacy);
- comunque l'azienda, licenziandolo, non ha menzionato nelle motivazioni il contenuto dei messaggi, ma solo al fatto che fossero "non di lavoro";
- l'azienda aveva "limitato" l'indagine al solo account di Yahoo (non al pc o altro) e in un tempo limitato (pochi giorni e solo in orario di lavoro) e quindi in modo "limitato e proporzionato".

La Grand chamber, per contro, mi pare abbia notato che il regolamento interno non specificava le modalità di controllo delle comunicazioni Internet (ossia di come l'azienda intendesse verificare email, IM, eccetera).

Ricordo che, fino ad un certo punto, non sono favorevole al controllo dei lavoratori. Ma è importante capire come si può agire in caso di abuso.

La sentenza della Grand chamber (grazie a Pierfrancesco Maistrello):
- http://www.dirittoegiustizia.it/allegati/PP_INTERN_CEDU_milizia_s_4.pdf.

Un articolo segnalato da Pierfrancesco Maistrello:
- https://strasbourgobservers.com/2016/12/20/resuscitating-workplace-privacy-a-brief-account-of-the-grand-chamber-hearing-in-barbulescu-v-romania/.

Un articolo di Altalex:
- http://www.altalex.com/documents/news/2017/09/06/datore-controllo-mail-lavoratore.

La notizia l'ho avuta inizialmente da ictBusiness.it, ma l'articolo non mi era chiaro (infatti il solito Pierfrancesco Maistrello mi ha dovuto correggere):
- http://www.ictbusiness.it/cont/news/email-dei-lavoratori-controllate-l-europa-dice-si-con-limiti/40030/1.html.

La sentenza di dicembre (il primo link segnalato da Qwant che permette di scaricarla):
- http://www.federalismi.it/nv14/articolo-documento.cfm?Artid=31234.

Infine una domanda: ora quale sentenza dovrà essere seguita? Quella della Corte di giustizia o quella della Grand chamber?

****

03- Privacy e controllo lavoratori: software per i call centre (e non solo)

Segnalo questo articolo di Filodiritto dal titolo "Controllo dei lavoratori - Ispettorato Nazionale del Lavoro: alcuni software di gestione dell'attività dei Call Center configurano un controllo a distanza dei lavoratori":
- https://www.filodiritto.com/news/2017/controllo-dei-lavoratori-ispettorato-nazionale-del-lavoro-alcuni-software-di-gestione-dellattivita-dei-call-center.html.

Ho trovato molto interessante la terza pagina, dove sono riassunte le due tipologie di software che possono comportare il controllo dei lavoratori e le quanto è necessario fare.

****

05- Pubblicata ISO/IEC 29151 - Controlli per la privacy

Fabio Guasconi di Bl4ckSwan mi ha informato che è stata pubblicata la ISO/IEC 29151 dal titolo "Code of practice for personally identifiable information protection":
https://www.iso.org/standard/62726.html.

E' applicabile ai soli titolari dei trattamenti (e non mi sembra una buona idea).

Si tratta di un'estensione dei controlli della ISO/IEC 27002. Per alcuni dei controlli già previsti dalla ISO/IEC 27002 sono indicate ulteriori indicazioni per l'attuazione. In Annex A sono poi riportati controlli aggiuntivi rispetto a quelli già presenti nella ISO/IEC 27002.

Questo documento potrebbe essere usato dalle organizzazioni già certificate ISO/IEC 27001 per estendere la propria Dichiarazione di applicabilità (o Statement of applicability). Questo poi potrebbe portare a certificazioni ISO/IEC 27001 basate "sui controlli riportati dalle ISO/IEC 27001 e ISO/IEC 29151" (non sono previste certificazioni ISO/IEC 29151).

Ora è anche in corso di discussione la ISO/IEC 27552, che dovrà estendere (non ridurre!) la ISO/IEC 27001 in modo che sia dedicata alla protezione dei dati personali. I lavori su questa norma sono in stato ancora di "Working draft" e pertanto uscirà tra almeno di due anni.

****

06- Privacy: Il flop della regolamentazione dei cookies

Fabrizio Monteleone di DNV GL mi ha segnalato uno studio dal titolo "Uncovering the Flop of the EU Cookie Law". L'ho trovato su questo sito:
https://scirate.com/arxiv/1705.08884.

Riassumo l'abstract. La Direttiva ePrivacy richiede che i siti web chiedano consenso esplicito agli utenti prima di usare i "tracking cookies". Gli autori hanno quindi analizzato più di 35.000 siti web e hanno scoperto che il 65% di questi siti installa i tracking cookies prima che l'utente possa accettarli esplicitamente. Gli autori sono convinti che le agenzie di controllo non facciano controlli, ma anche delle difficoltà di attuazione delle misure tecniche richieste.

****

07- Articolo su eIDAS

Fabrizio Cirilli (PDCA S.r.l.) mi ha segnalato un articolo dal titolo "Regolamento eIDAS (EU 910/2014) e direttive italiane in materia di digitalizzazione", che ha scritto con Riccardo Bianconi (ispettore Accredia). Si trova sulla rivista KnowIT (bisogna registrarsi per scaricarla):
- https://www.knowit.clioedu.it/rivista.

Personalmente, sarei stato più esplicito in alcune considerazioni (nell'articolo si accenna allo sforzo necessario per vedere tutti gli HSM e alle eccessive ridondanze delle check list AgID). In particolare avrei indicato anche alcune questioni relative al controllo dei fornitori, a mio parere non corrette, come già detto in altre occasioni (http://blog.cesaregallotti.it/2015/10/per-agid-linformatica-e-ferma-agli-anni.html).

Però penso che questo articolo sia un buon riferimento per ragionare in merito all'applicazione del Regolamento eIDAS in Italia.

****

08- Del NIST e della lunghezza e complessità delle password

Il NIST ha pubblicato la SP 800-63B, una nuova versione della "Digital Identity Guidelines: Authentication and Lifecycle Management":
http://csrc.nist.gov/publications/PubsSPs.html.

In realtà vedo che ha pubblicato anche, nella stessa data, la SP 800-63C e la SP 800-63-3. Confesso che mi sono perso in questi documenti e non li ho letti. Però segnalo quanto richiamato dal SANS Newsbites (https://www.sans.org/newsletters/newsbites/xix/62#200), in particolare facendo riferimento al punto 5.1.1 del SP 800-63B, "Memorized secrets", e all'Appendix A: "il nuovo documento suggerisce di usare password lunghe, facili da ricordare e da cambiare solo quando si pensa siano state compromesse". Un autore della precedente guida del NIST dice che "rimpiange" la vecchia impostazione che richiedeva di usare password complesse (con lettere maiuscole, minuscole, numeri e caratteri speciali) e da cambiare almeno ogni 3 mesi.

Si ritiene preferibile lasciare liberi gli utenti di scegliere le proprie password, purché di almeno 8 caratteri e non presenti in una blacklist di password troppo facili (per esempio password già diffuse a seguito di altri attacchi, parole del dizionario, caratteri sequenziali o ripetuti, come 1234 e aaaa, parole derivate dal nome del servizio, dal nome dell'utente, dalla sua user-id o altri elementi). Infatti le password sono più spesso individuate attraverso attacchi di social engineering e non di forza bruta.

Per quanto riguarda la lunghezza, il NIST fa notare che questa non ha impatto sugli attacchi offline, visto che questi sono rivolti ai valori hash, indipendenti dall'input. Per gli attacchi online, bisogna invece prevedere altre misure di sicurezza, come il blocco dopo alcuni tentativi errati, valutando però la possibilità che un malintenzionato possa provare deliberatamente password errate per bloccare l'utente. E' comunque raccomandata una lunghezza minima di 8 caratteri.

Per quanto riguarda la complessità, il NIST segnala che spesso gli utenti riescono ad aggirare la richiesta con scelte banali, per esempio usando al posto di "password" la stringa "Password1". In altri casi, la complessità porta gli utenti a scrivere le proprie password, annullando (o peggiorando) la misura.

Personalmente ho qualche perplessità e devo ancora pensare ai pro e ai contro di queste proposte. Per esempio, il cambio periodico della password è necessario negli ambienti in cui gli utenti si scambiano le password (anche se proibito o sconsigliato) o le usano su strumenti non personali o aziendali (e quindi ricavabili dalla cache dello strumento).

In Italia, comunque, sono ancora vigenti le misure minime del Codice della privacy che impone una lunghezza minima di 8 caratteri, un minimo di complessità e il cambio ogni 3 o 6 mesi. Vedremo dopo le modifiche che saranno apportate al Codice e ai Provvedimenti (e Linee guida) del Garante privacy.

Nota: un articolo simile l'ho proposto a https://www.ictsecuritymagazine.com/ (finora non risulta pubblicato).

****

09- Rasperry Pi e la insecurity by default

Bruce Schneier ha segnalato una guida per mettere in sicurezza i computer Rasperry Pi, ossia i dispositivi più diffusi per sviluppare gli oggetti dell'Internet of things.

Il post di Bruce Schneier:
https://www.schneier.com/blog/archives/2017/09/securing_a_rasp.html.

L'articolo "Take These Steps to Secure Your Raspberry Pi Against Attackers":
https://makezine.com/2017/09/07/secure-your-raspberry-pi-against-attackers/.

Il punto, come dice Bruce Schneier, non è tanto studiare come mettere in sicurezza un Rasperry Pi, quanto notare la difficoltà per farlo. Purtroppo la difficoltà a metterli in sicurezza è comune a

tutti i computer. Forse il Windows, pur con tutti i suoi problemi, è tra i più semplici e questo dà l'idea del problema. Continuiamo infatti a produrre, comprare e usare prodotti difficili da mettere in sicurezza.

La security-by-design (e quindi la privacy-by-design) è quindi un'utopia. L'insecurity-by-design è invece quello che c'è. Rendiamocene conto e cerchiamo di conviverci.

****

10- ISO 18295 sui Costumer contact centre

Franco Ferrari di DNV GL mi ha segnalato la pubblicazione, a luglio 2017, della norma ISO 18295 dal titolo "Customer contact centres". Essa è divisa in due parti: la prima ("Requirements for customer contact centres") presenta i requisiti proprio di customer contact centre (CCC), mentre la seconda ("Requirements for clients using the services of customer contact centres") presenta i requisiti che dovrebbero attuare i clienti, interni o esterni, dei CCC.

Si tratta di norme certificabili. Non si tratta di norme di "sistemi di gestione", ma "di servizio", e pertanto non sono impostate come la ISO 9001:2015 o la ISO/IEC 27001:2013.

Prima di questa norma era disponibile la norma europea EN 15838 (dal titolo "Customer Contact Centres: Requirements for service provision"), ora abrogata. In Italia la EN 15838 andava integrata con la UNI 11200 (dal titolo "Servizi di relazione con il cliente, con il consumatore e con il cittadino, effettuati attraverso centri di contatto: Requisiti operativi per l'applicazione della UNI EN 15838:2010") e ora vedremo se questa norma nazionale avrà ancora ragione di esistere.

La UNI 11200 è comunque interessante perché riporta delle metriche più precise rispetto a quelle generiche delle norme europee e internazionali. In molti casi riporta anche dei valori di riferimento (o SLA).

Tecnicamente, le norme precedenti riguardavano solo l'erogazione dei servizi. Ora la parte 2 della ISO 18295 introduce requisiti anche per i clienti dei contact centre.

Segnalo quindi la presentazione di queste norme fatta dall'ISO:
https://www.iso.org/news/ref2191.html.

****

11- Standard: Ritirata la ISO/IEC 27015 - Controlli di sicurezza per il settore finance

Franco Ferrari di DNV GL mi ha segnalato che è stata ritirata la ISO/IEC 27015 dal titolo "Information security management guidelines for financial services":
https://www.iso.org/standard/43755.html.

Infatti sembra che i fornitori di servizi finanziari (soprattutto le banche) preferiscono appoggiarsi ad altri standard interni o di altra provenienza. Per esempio, mi risulta che la BCE (Banca centrale europea) si appoggia sul NIST Cybersecurity framework, di origine USA.

Questo lo trovo molto bizzarro: piuttosto che appoggiare uno standard internazionale, con procedure di approvazione aperte, alcune istituzioni preferiscono appoggiarsi a standard elaborati da strutture che sfuggono completamente al loro controllo. Contenti loro...

****