Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – GIUGNO 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.

IT Service Management News di Cesare Gallotti è rilasciata sotto licenza Creative Commons Attribution 4.0 International License (creativecommons.org/licenses/by/4.0/deed.en_GB). Bisogna attribuire il lavoro a Cesare Gallotti con link a http://www.cesaregallotti.it/Newsletter.html.

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- Materiale di sensibilizzazione

In molti mi chiedono se ho in mente video o altro per la sensibilizzazione del personale. La risposta è sempre quella, dal sito di ENISA:
https://www.enisa.europa.eu/media/multimedia/material.

Trovo molto divertenti i video e i disegni.

Segnalo anche questo video molto interessante dal titolo "Amazing mind reader reveals his gift":
https://www.youtube.com/watch?v=F7pYHN9iC9I.

Utile (forse) per ricordare quanto bisogna stare attenti a quello che si pubblica sul web.

Grazie a Francesca Lazzaroni di Spike Reply.

Fabio Biancotto di Air Dolomiti mi ha segnalato questo video, indirizzato a chi fornisce assistenza (e non dovrebbe fornirne troppa):
https://www.youtube.com/watch?v=lc7scxvKQOo.

****

02- British Airways ferma per un giorno

Avevo letto inizialmente la notizia sul Corriere della Sera su un articolo dal titolo "Gb: guasto al sistema informatico, voli British tutti a terra, caos a Londra":
http://www.corriere.it/esteri/17_maggio_27/gb-guasto-sistema-informatico-voli-british-tutti-terra-caos-londra-24359854-42d4-11e7-bf8f-efa16b87b247.shtml.

Il problema sembra fosse dovuto ad un tecnico che per sbaglio ha staccato la corrente:
http://www.corriere.it/cronache/17_giugno_02/voli-cancellati-british-airways-causare-caos-errore-umano-un-tecnico-ha-spento-interruttore-06e0857c-476e-11e7-b4db-9e2de60af523.shtml.

Le stesse notizie in inglese, dai link forniti dal SANS Newsbyte:
Reuters: http://www.reuters.com/article/us-britain-airports-heathrow-idUSKBN18P01O;
BBC: http://www.bbc.com/news/uk-40069865.

I sindacati accusano BA di aver esternalizzato tutto l'IT presso un fornitore in India, perdendo così competenze. BA nega.

Di certo sappiamo che molti problemi delle aziende hanno come causa la gestione orientata alla Borsa (breve periodo) e non all'impresa (lungo periodo) e manager che stanno più attenti agli obiettivi personali (avidità economica) che a quelli dell'impresa (sostenibilità).

E io penso che veramente i manager di oggi non si rendano conto di cosa vuol dire "digitalizzazione". In termini di rischi, di costi e di necessità di manutenzione. Tutti a voler sistemi informatici più belli e più nuovi (cominciando dai pc, tablet, smartphone personali) e nessuno a chiedersi cosa bisogna fare tra qualche anno. E così ci sono aziende che hanno ancora Windows XP e altre che non vogliono investire in una prova di disaster recovery. Giusto pochi giorni fa, una persona mi diceva che ha dovuto combattere lungamente con gli altri manager per evitare che anche la sicurezza fosse esternalizzata e che venisse invece considerata come elemento strategico per il governo dell'impresa.

Oggi mi sembra che un manager non possa più ignorare la gestione dei sistemi IT.

****

03- Accesso abusivo ai sistemi IT anche con autorizzazione

L'articolo ha titolo " Le Sezioni unite confermano: è abusivo l'accesso a sistemi informatici per ragioni diverse da quelle per le quali l'agente dispone di autorizzazione":
http://www.penalecontemporaneo.it/d/5428-le-sezioni-unite-confermano-e-abusivo-laccesso-a-sistemi-informatici-per-ragioni-diverse-da-quelle.

Provo a riassumere: è stato chiesto alla Corte di cassazione se è da considerare reato l'accesso ad un sistema informatico da parte di qualcuno che ha sì le autorizzazioni a farlo, ma non ne avrebbe motivo. La risposta è sì.

Il quesito riguarda specificatamente pubblici ufficiali o incaricati di un pubblico servizio, ma credo sia importante anche per le aziende private e altre organizzazioni.

Infatti è vero che i sistemi IT dovrebbero essere configurati secondo i principi del privilegio minimo e del "need to know", ma è spesso necessario fare delle semplificazioni per evitare il sovraccarico di lavoro degli amministratori di sistema.

****

04- Legge contro il cyberbullismo

E' stata approvata la legge contro il cyberbullismo.

Su Altalex si trova una breve analisi del contenuto di legge:
http://www.altalex.com/documents/news/2016/09/21/bullismo-e-cyberbullismo.

Sul Corriere della Sera si trova la storia di questa legge, la cui proposta ha subito molte critiche prima di essere modificata e approvata nella versione attuale:
http://www.corriere.it/tecnologia/cyber-cultura/cards/lotta-cyberbullismo-arriva-l-ok-camera-cosa-prevede-legge/contro-bullismo-cyberbullismo-l-ok-camera_principale.shtml.

Sul sito della Camera dei Deputati, si trova un'analisi più istituzionale del provvedimento:
http://www.camera.it/leg17/522?tema=prevenzione__e_repressione_del_bullismo_e_del_cyberbullismo.

****

05- Videosorveglianza lavoratori, consenso e Cassazione

Articolo di Altalex dal titolo "Controlli a distanza e consenso dei lavoratori: la Cassazione fa dietrofront":
http://www.altalex.com/documents/news/2017/05/10/controlli-a-distanza-e-consenso-dei-lavoratori-la-assazione-fa-dietrofront.

La Corte di Cassazione in passato aveva dichiarato ammissibile l'installazione di telecamere nei luoghi di lavoro (in questo caso, in un negozio), purché fosse stato raccolto il consenso, anche non sottoscritto, da parte dei lavoratori. Con questa sentenza (Cassazione penale, sez. III, sentenza 08/05/2017 n° 22148), invece la Cassazione si smentisce e ribadisce la necessità di avere l'autorizzazione da parte delle rappresentanze sindacali o della Direzione territoriale del lavoro.

****

06- Piano Triennale per l'IT nella PA

Da un tweet di @diritto2punto0 segnalo la pubblicazione del "Piano Triennale 2017-2019 per l'informatica nella Pubblica Amministrazione":
https://pianotriennale-ict.italia.it/.

Confesso che non l'ho letto. Il poco che ho visto dimostra un piano decisamente ambizioso, ma alcuni mi dicono irrealizzabile nei tempi prospettati e considerando che si sta parlando di PA.

Su Nova 24 (grazie a Roberto Gallotti) ho letto un articolo di presentazione del piano. Sul web ne è disponibile solo una scansione su Twitter, probabilmente non legale (ma finché c'è, si può leggere): https://twitter.com/gabferrieri/status/873839729661399040/photo/1.

****

07- Aggiornamento "Piano nazionale per la protezione cibernetica e la sicurezza informatica"

Segnalo da un tweet di @cgiustozzi il "Piano nazionale per la protezione cibernetica e la sicurezza informatica":
http://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/pubblicato-il-nuovo-piano-nazionale-cyber.html.

****

08- Nuovi trend e norme ISO/UNI

Segnalo questa presentazione dal titolo " Uninfo - nuovi trend e norme ISO/UNI - Blockchain, IoT, Big Data, Industry 4.0 e certificazioni Privacy":
https://www.slideshare.net/bl4ckswan/uninfo-nuovi-trend-e-norme-isouni-blockchain-iot-big-data-industry-40-e-certificazioni-privacy.

Per chi vuole avere un quadro degli standard che si stanno preparando su alcuni temi molto innovativi. Segnalo solo che la gran parte degli standard citati non prevedono la possibilità di certificazione della conformità.

****

09- App medicali e nuovo Regolamento UE sui dispositivi medici

Ho trovato interessante questo breve intervento su "App medicali e nuovo Regolamento UE sui dispositivi medici":
https://www.filodiritto.com/articoli/2017/05/app-medicali-e-nuovo-regolamento-ue-sui-dispositivi-medici.html.

Mi pare tratti uno degli argomenti di sicurezza informatica più importanti in questo periodo. Infatti i dispositivi medici sono dei casi particolari (e critici) di IoT, che sappiamo essere molto vulnerabile.

Segnalo che anche la "vecchia Direttiva UE sui dispositivi medici" tratta, seppur meno esplicitamente, di app medicali e pertanto andrebbe applicata già da tempo.

****

10- ICT e lavoro

Franco Ferrari di DNV GL mi ha segnalato questa pubblicazione dell'INAIL dal titolo "ICT e lavoro: nuove prospettive di analisi per la salute e la sicurezza sul lavoro":
https://www.inail.it/cs/internet/comunicazione/news-ed-eventi/news/news-monografia-ict-lavoro-dimeila.html.

Si tratta di un lavoro interessante. Ho trovato interessante soprattutto il capitolo relativo ai rischi per il lavoratore (come ci si poteva aspettare da un lavoro dell'INAIL).

Chiaramente si parla del rischio di eccesso di impegno lavorativo, ma anche di cyberloafing (parola che non conoscevo e che indica l'eccesso di frammentazione e interruzione delle attività). Ci sono ultreriori rischi che intuitivamente tutti conosciamo, ma che è bene rileggere (per esempio io sono rimasto colpito dal rischio di "non uno inconsapevole degli strumenti informatici", con impatti anche sull'e-learning).

Infine, per il telelavoro ho scoperto che il riferimento normativo per le pubbliche amministrazioni è il DPR 70 del 1999.