Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – LUGLIO 2016

****

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

****

00- Piccolo editoriale

Anche quest'anno invio la newsletter di luglio in ritardo, visto che ad agosto non ci sarà e riprenderà a metà settembre, con la solita puntualità altalenante (sempre però il 15 del mese o qualche giorno dopo).

Mi rendo conto che questa newsletter, dedicata com'è a sicurezza, qualità e informatica varia, sembra scritta da una persona al di fuori di questo mondo: non si parla di terrorismo o di profughi, non si parla di politici (ascoltati!) che propongono soluzioni semplicistiche e promuovono l'approccio "si può fare subito" e "per dirigere il Paese non è necessario essere competenti", di politici (sempre votati!) che non decidono niente e non prendono mai posizione, di politici, calciatori e manager che rubano tanti o pochi soldi.

Eppure sono tutte cose che in parte mi fanno paura, in parte mi dicono che il mondo in cui viviamo sta cambiando e ne devo prendere atto.

Non voglio lamentarmi, ma la paura del terrorismo ha degli impatti sulle nostre vite e su come ci comportiamo, l'idea che esistano soluzioni semplici e rapide a problemi complessi e che non richiedano particolari competenze ha dei riflessi nel modo in cui lavoriamo e in cui ci è chiesto di lavorare, politici inutili che non decidono mai nulla ma che sabotano iniziative altrui senza mai entrare nel merito fungono da esempio a troppe persone (che dire poi di quelli che votano "no" al referendum perché "non è abbastanza"? Ascolto quelli che discutono del merito, ma non ho rispetto per quelli che, consapevolmente e non consapevolmente, promuovono l'idea che si possa fare un unico passo bello lungo e in tempi brevi) e infine i ladri promuovono l'idea che l'importante è arraffare quanto più possibile e in malora tutto il resto.

Di tutto questo dobbiamo tenerne conto nella nostra vita quotidiana e nel nostro lavoro. Perché, se vogliamo farlo bene, dobbiamo riconoscerlo e affrontarlo per come si manifesta negli ambiti meno pubblici ma importanti per noi.

Quindi meno male che arrivano le vacanze che spero mi tolgano i brutti pensieri e mi impediranno per altri anni di scrivere cose inutili su questa newsletter. E a voi auguro un buon agosto, qualsiasi cosa facciate.

Cesare

****

01- Privacy shield approvato

Il 12 luglio, più o meno, è entrato in vigore il Privacy shield, ossia il nuovo accordo USA-EU che sostituisce Safe Harbour, invalidato qualche tempo fa.

Questo accordo permette il trasferimento di dati personali da EU a USA, evitando una serie di adempimenti da parte delle aziende europee. Le aziende USA che vogliono importare dati personali (pensate per esempio ai tanti fornitori di servizi IT, in particolare quelli di hosting e cloud), dal 1 agosto potranno aderire ad un protocollo del U.S. Department of Commerce, in modo simile a quanto avveniva con Safe Harbour.

Al momento non sono riuscito a capire cosa dice il protocollo né in quale sito poter vedere quali aziende aderiscono.

Quindi segnalo qualche link esplicativo (grazie a tweet di @Leilyllia, @roberta_zappala). Segnalo che le traduzioni automatiche in italiano sono piuttosto divertenti:
- http://europa.eu/rapid/press-release_IP-16-2461_en.htm;
- http://europa.eu/rapid/press-release_STATEMENT-16-2443_en.htm;
- http://www.dimt.it/2016/07/12/via-libera-al-privacy-shield-per-la-protezione-dei-dati-trasferiti-tra-ue-e-usa/.

Non mancano le critiche. Joe McNamee, Executive Director of European Digital Rights , ha detto chee questo accordo sarà presto giudicato illegale. Ma non è il solo (grazie a tweet di @edri, @alexsib17, @madmaus:
- https://edri.org/privacy-shield-privacy-sham/;
- http://arstechnica.co.uk/tech-policy/2016/07/privacy-shield-to-be-dragged-across-finish-line-sources/;
- http://www.infosecurity-magazine.com/news/privacy-shield-approved-expected.

Nota: alcuni di questi articoli sono precedenti al 12 luglio, quando l'accordo è diventato operativo.

Anche questa volta mi congedo con un tweet di @DailyPratchett. Terry Pratchett era un genio della letteratura (a mio immodesto avviso) e forse pensava a questo Privacy shield: "The innocent would have nothing to fear, d'you think? I wouldn't bet tuppence".

****

02- Privacy: elenco BCR

La normativa sulla privacy permette il trasferimento dei dati extra-UE in vari casi. Uno di questi riguarda le multinazionali, che possono fornire adeguate garanzie di sicurezza attraverso regole aziendali (Binding corporate rules, BCR) approvate da un'autorità garante europea.

Ivo Trotti di TNS Italia mi ha segnalato il link ufficiale dove sono elencate le imprese con BCR approvate:
- http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm.

****

03- Privacy: Sulle misure minime (che non sono abrogate!)

In questi giorni leggo e sento che saranno abrogate le misure minime per la privacy, a causa dell'entrata in vigore del Regolamento europeo sulla protezione dei dati personali.

In realtà, quanto riportato dal Codice privacy italiano (D. Lgs. 196 del 2003) rimane in vigore, purché non in conflitto con il Regolamento. È vero che le misure minime non sono richieste dal Regolamento europeo, ma la loro obbligatorietà, prevista dall'ordinamento italiano, non è in conflitto con esso.

Ovviamente il Parlamento dovrebbe emendare il Codice privacy per evitare confusione e armonizzare completamente la normativa italiana con quella europea (problema che oggi abbiamo con il Codice dell'amministrazione digitale, che non è ancora stato modificato considerando quanto previsto dal Regolamento eIDAS). Probabilmente le misure minime saranno cancellate, ma fino ad allora sono ancora in vigore.

Ho chiesto aiuto a Pierluigi Perri, della Facoltà di Giurisprudenza Università degli Studi di Milano, che ringrazio. Mi ha confermato quanto da me capito. E, anzi, aggiunge: "Il Regolamento espressamente demanda agli Stati membri la definizione delle sanzioni penali (cfr. Considerando n. 149) per cui, visto

che allo stato attuale delle cose la violazione delle misure minime è punita penalmente, nulla vieta che vengano riproposte dal nostro Legislatore, in quanto non contrastano con le previsioni di cui all'art. 32 del Regolamento".

Pierfrancesco Maistrello di Vecomp mi ha scritto un'ulteriore riflessione sulle misure minime.

Intanto mi ricorda che le misure minime sono considerate obsolete da tempo, come dimostrano anche le due segnalazioni del garante:
- http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/3531329;
- http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/4575782.

E questo mi sembra pacifico. Aggiungo che in alcuni casi erano obsolete anche nel 2003.

Pierfrancesco aggiunge che l'articolo 36 del Codice Privacy riporta: "Il disciplinare tecnico di cui all'allegato B), relativo alle misure minime di cui al presente capo, è aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie e il Ministro per la semplificazione normativa, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore".

Pierfrancesco non ironizza, come tutti, sul fatto che l'aggiornamento dal 2003 al 2016 non c'è mai stato. Ma dice: "Sembra quasi una garanzia di immutabilità, dato che il ministro per le innovazioni e le tecnologie non si chiama neanche più così!".

Poi Pierfrancesco mi cita la relazione 2015 del Garante: "permangono numerose le violazioni delle misure minime di sicurezza; ciò, nonostante si tratti di adempimenti di non particolare complessità, in vigore da più di dieci anni, che dovrebbero essere stati oramai "metabolizzati" sia dalle imprese che dagli enti pubblici. Deve essere nuovamente segnalata la ormai indifferibile esigenza di aggiornare il Disciplinare tecnico in materia di misure minime di sicurezza, All. B al Codice in vigore dal 2003, le cui prescrizioni appaiono in buona parte non più adeguate allo stato dell'evoluzione tecnica, anche alla luce della ormai consistente esperienza maturata dall'Autorità in sede di controllo. Tale revisione dovrebbe essere ispirata a criteri di semplificazione, rispetto ad adempimenti di natura prettamente burocratica oggi previsti dalle disposizioni, e di maggiore effettività delle misure, prevedendo adeguati accorgimenti tecnici che intervengano in modo progressivo in funzione della quantità e della qualità dei dati, nonché della complessità della struttura tecnologica utilizzata e del numero di incaricati che vi hanno accesso".

Conclude "credo che l'abrogazione delle misure minime vigenti sia quantomeno auspicabile".

A me non resta che sottoscrivere e ringraziarlo per questa analisi approfondita.

****

04- Privacy e Videosorveglianza: dove va posta l'informativa

Notizia da tweet di @a_oliveri dal titolo "Privacy - Cassazione Civile: l'informativa in materia di videosorveglianza va sempre posta prima del raggio d'azione della telecamera":
- http://www.filodiritto.com/news/2016/privacy-cassazione-civile-linformativa-in-materia-di-videosorveglianza-va-sempre-posta-prima-del-raggio-dazione-della.html.

Penso che il titolo dica già tutto.

****

05- Privacy: provvedimenti Garante su Videosorveglianza "lunga"

Franco Ferrari di DNV GL mi ha segnalato un articolo del Garante privacy, relativo a due recenti provvedimenti del Garante stesso che autorizzano la conservazione di videoregistrazioni per 30 e 45 giorni:
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4933227;
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4933452.

Si tratta di concessioni per aziende che si occupano di produzione o trattamento di materiali particolarmente critici (microprocessori per carte di pagamento e materiale classificato per il settore marino).

****

06- Privacy: Garante autorizza rilevazione GPS

Pierfrancesco Maistrello di Vecomp mi ha segnalato questo Provvedimento del Garante privacy:
- http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/5217175.

Il Garante ha autorizzato l'uso del cellulare (con GPS!) per calcolare la prestazione lavorativa.

Scrive Pierfrancesco: "precedentemente avevo visto le autorizzazioni per Wind ed Eriksson, che però erano incentrate sulle finalità di sicurezza, con problemi di lavoro isolato, ecc.).

Interessanti le misure: log obbligatori, utenze specifiche con profili determinati e una bella icona obbligatoria sullo schermo del telefonino.

E il titolare, secondo me, è stato fortunato ad avere sindacati collaborativi. Una soluzione del genere, prospettata a qualche ispettore del lavoro, avrebbe creato delle difficoltà.

Altro aspetto da segnalare è la velocità di risposta del Garante: l'istanza è di settembre 2015 e la risposta del 18 maggio. Tempi non brevissimi ma neanche lunghissimi".

****

07- Licenziato chi sta troppo tempo su Facebook

Notizia da tweet di @a_oliveri dal titolo "Licenziato chi sta troppo tempo su Facebook":
- http://www.ilsole24ore.com/art/norme-e-tributi/2016-07-08/licenziato-chi-sta-troppo-tempo-facebook-163506.shtml.

Penso che l'articolo dica già tutto in estrema sintesi e credo sia molto interessante per capire come sono interpretate alcune attività di indagine, per quanto artigianali e condotte senza strumenti sofisticati.

Penso che rimanga da vedere se verrà presentato ricorso in appello e poi, forse, in Cassazione e, quindi, i risultati di questi ricorsi.

****

08- Normativa europea: Direttiva NIS

È stata approvata la Directive on Security of Network and Information Systems (NIS Directive).

Segnalo dei link (grazie ad una segnalazione di Pierfrancesco Maistrello di Vecomp e ad un tweet di @francescotozzi9):
- http://europa.eu/rapid/press-release_MEMO-16-2422_en.htm;
- http://www.europarl.europa.eu/news/en/news-room/20160701STO34371/Cyber-security-new-rules-to-protect-Europe's-infrastructure.

Dal memo della Commissione europea sintetizzo ulteriormente:
- ogni Stato dovrà redigere una strategia sulla sicurezza informatica, dovrà istituire un'autorità relativa, designare uno o più Computer Security Incident Response Teams (CSIRTs);
- gli Stati dovranno collaborare e stabilire un programma di lavoro, condividere informazioni in merito alle minacce;
- la Direttiva riguarda aziende dei settori energia, trasporto, bancario, infrastrutture finanziarie, sanità, fornitura acqua, infrastrutture digitali.

Comunque la Direttiva (a differenza di un Regolamento), per essere completamente applicabile in Italia, deve essere tradotta in Decreto legislativo entro maggio 2018. E quindi è bene studiarla, ma consapevoli che il D. Lgs. potrà avere delle peculiarità a cui stare attenti.

PS: altro link, in italiano, lo segnalo da un tweet di @a_oliveri:
- http://www.europarl.europa.eu/news/it/news-room/20160701IPR34481/Sicurezza-online-il-PE-approva-nuove-norme-contro-gli-attacchi-informatici

****

09- eIDAS è entrato in vigore

Il 1 luglio 2016 è entrato in vigore il Regolamento europeo eIDAS, su firme elettroniche e altro. Segnalo quindi qualche articolo.

Le domande e risposte della Commissione europea su eIDAS:
- https://ec.europa.eu/digital-single-market/en/news/questions-answers-trust-services-under-eidas.

Un articolo di Daniele Tumietto che spiega cosa è eIDAS, i suoi benefici e le sue relazioni con il CAD:
- https://www.linkedin.com/pulse/eidas-rappresenta-uno-nuovo-strumento-per-nuovi-modelli-tumietto.

Un articolo in inglese che spiega anch'esso cosa è eIDAS:
- https://ec.europa.eu/commission/2014-2019/ansip/blog/building-online-trust-and-confidence-role-eidas-and-digital-identity_en.

****

10- eIDAS: Standard ETSI

Segnalo questo articolo di Daniele Tumietto che elenca gli standard ETSI necessari all'attuazione di quanto previsto dal Regolamento eIDAS sull'identificazione elettronica e i servizi digitali fiduciari:
- https://www.linkedin.com/pulse/etsi-publishes-european-standards-support-eidas-eseals-tumietto.

Link Diretto alla lista di ETSI:
- https://portal.etsi.org//TBSiteMap/ESI/ESIActivities.aspx.

****

11- Standardizzazione: ISO/IEC 33072 sui processi della sicurezza delle informazioni

Tony Coletta, delegato italiano al ISO/IEC SC 7 WG 10, mi ha informato della recente pubblicazione del nuovo standard ISO/IEC 33072 ddal titolo "Process capability assessment model for information security management":
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=70803.

Si tratta, in poche parole, di una riscrittura della ISO/IEC 27001 descrivendone i processi e controlli come processi valutabili secondo la scala di capability, da 0 a 5, descritta nella ISO/IEC 33020. Per chi è abituato ad un'altra terminologia, ormai vecchia, traduco dicendo che si tratta di un modello per la valutazione della maturità del sistema di gestione per la sicurezza delle informazioni.

Si tratta di una lettura non veloce (194 pagine!) e impegnativa. Dubito che un esercizio di questo genere sia veramente utile per migliorare la sicurezza delle informazioni, soprattutto considerando che in troppe organizzazioni vedo processi talmente mal gestiti che raggiungere un livello di capacità pari ad 1 sarebbe già un bel risultato.

****

12- Standardizzazione: ISO 27799:2016: sicurezza nella sanità

Franco Ferrari di DNV GL mi ha segnalato la pubblicazione della nuova versione del 2016 dell ISO 27799 dal titolo "Health informatics -- Information security management in health using ISO/IEC 27002":
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62777.

La lettura (confesso che ho sfogliato rapidamente) ha degli alti e dei bassi. Gli alti sono rappresentati da considerazioni in merito alle specificità del settore della sanità (per esempio la gestione delle emergenze), un elenco di minacce da considerare e una guida per l'attuazione della sicurezza delle informazioni.

La mia critica principale riguarda proprio questa guida per l'attuazione, che trovo un po' rigida e "vecchia maniera" e quindi difficile da seguire da quelle strutture che oggi non hanno un approccio ben strutturato alla sicurezza delle informazioni.

****

13- Standardizzazione: ISO/IEC 27009 - Il metastandard

Ho ricevuto notizia che il 6 giugno è stata pubblicata la ISO/IEC 27009 dal titolo "Sector-specific application of ISO/IEC 27001 -- Requirements":
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42508.

Si tratta, come dice Fabio Guasconi, un meta-standard, ossia uno standard per scrivere standard relativi ai "controlli per specifici settori" come la ISO/IEC 27011 o la ISO/IEC 27017. In altre parole, uno standard non utile per chi non partecipa alla scrittura degli standard della famiglia ISO/IEC 27000.

****

14- Nuova versione del COSO ERM Framework

Per chi non lo conoscesse, il COSO ERM Framework è un documento del "Committee of sponsoring organizations of the treadway commission" (COSO) dedicato all'Entreprise risk management. Per vari motivi, esso è diventato un punto di riferimento per quanto riguarda la gestione delle aziende con un approccio basato sul rischio.

Protiviti, attraverso la sua newsletter, mi ha informato che il COSO ha reso pubblica una bozza della nuova versione dell'ERM framework.

La pagina dove trovare la bozza del nuovo COSO ERM Framework:
- http://erm.coso.org/Pages/default.aspx.

La pagina dove trovare il bollettino di Protiviti, che spiega in sintesi le ragioni del cambiamento e le novità:
- http://www.protiviti.com/cosoerm

Sicuramente l'approccio ha dei punti di interesse, ma mi preme sottolinearne una: il fatto che l'applicazione del framework è stata spesso sbagliata perché concentrata sui dettagli e non usata per impostare le strategie.

Come non riflettere, ancora una volta, sul fatto che troppe valutazioni del rischio si perdono nei dettagli e perdono di vista il loro vero obiettivo, seppellite da troppi dettagli?

Mi fermo qui, per non ripetere cose già dette e ripetute in precedenza (incluse le critiche ai software per valutare il rischio).

****

15- Attacchi: App per smartphone rischiose

Trovo interessante il caso di Pokemon GO, un gioco per smartphone Android molto popolare e scaricato più di WhatsApp e Snapchat. Il fatto è che l'applicazione chiede permessi quasi totali per accedere ai dati presenti sullo smartphone. E, ovviamente, gli utenti li danno!

I creatori di Pokemon GO hanno scaricato questi dati e pensano di farci qualcosa? Oppure si tratta veramente di un errore di programmazione?

Il problema è che troppi utenti danno piene autorizzazioni alle app per cellulare, senza preoccuparsi delle conseguenze. Anche quando usano cellulari aziendali!

Due articoli, uno in italiano e uno in inglese (grazie ai tweet di @NowSecureMobile e di @roberta_zappala):
- https://www.nowsecure.com/blog/2016/07/12/pokemon-go-security-risks-what-cisos-and-security-pros-need-to-know/;
- [ITA] http://www.ansa.it/sito/notizie/tecnologia/software_app/2016/07/12/pokemon-go-primi-grattacapi-sicurezza_f8fb97f7-13ca-459e-8899-f5e45d065076.html.

Ma anche altre app sono assai rischiose. Segnalo questo articolo di Paolo Perego su Flash Keyboard:
- https://codiceinsicuro.it//blog/quando-la-spia-e-la-tastiera-del-tuo-smartphone-il-caso-flash-keyboard/.

****

16- Attacchi: Come rubare un profilo Facebook senza essere esperti informatici

Questo articolo mi interessa perché dimostra ancora una volta come certe "misure di sicurezza" siano in realtà delle bufale:
- http://attivissimo.blogspot.it/2016/07/come-rubare-un-profilo-facebook-senza.html.

Un malintenzionato ha convinto facilmente Facebook di dargli le credenziali di un altro utente. È bastato inviare una scansione di un documento di identità (falso, in questo caso; ma è facile ottenere una scansione della carta di identità di qualcuno, visto che tutti la richiedono).

Certamente non è facile pensare a meccanismi più sicuri, ma dovremmo farlo.

****

17- Survey Deloitte su dispositivi medici

Pasquale Tarallo mi ha segnalato questo articolo di Sanità 24 dal titolo "Biomedicali a rischio hacker: Deloitte lancia l'allarme sulla cyber security":
- http://www.sanita24.ilsole24ore.com/art/imprese-e-mercato/2016-06-24/biomedicali-rischio-hacker-deloitte-lancia-l-allarme--cyber-security-162350.php?uuid=AD1elbi.

L'articolo fa riferimento ad una survey di Deloitte dal titolo "Cyber security of networkconnected medical devices in (EMEA) Hospitals 2016" (il link l'ho trovato io con Google):
- http://www2.deloitte.com/nl/nl/pages/over-deloitte/articles/medical-devices-cybersecurity-vulnerable.html.

Non mi interessano i risultati della survey (che trovo sempre poco utili, anche se ormai di moda), ma l'elenco delle misure specifiche, riassunto dall'articolo di Sanità24, mi sembra utile come base di partenza quando si tratta di sicurezza informatica dei dispositivi medici.

****

18- Perfezionisti e ottimalisti

Segnalo questo articolo di Anna Gallotti (sì... è mia sorella!):
- http://share-coach.com/ita/articoli.php?id=73&read=storia

Lo trovo interessante perché riguarda due aspetti fondamentali per chi si occupa di processi aziendali:
1- quando gli interlocutori sono perfezionisti rallentano l'attuazione di quanto necessario (ovviamente, qui non si sta parlando di "resistenza al cambiamento", che è altra materia); certamente è importante considerare le loro questioni, ma bisogna stare attenti a non bloccare tutto per essere perfetti;
2- i perfezionisti tendono a nascondere gli errori (e criticare quelli altrui), con l'ovvio risultato che poi non si migliora.