Cesare Gallotti

**********
**IT SERVICE MANAGEMENT NEWS – MAGGIO 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- 28 giugno: DFA Open day

Si terrà presso l'Università degli Studi di Milano il giorno martedì 28 giugno 2016 il DFA Open day.

Sono consigliere di DFA (www.perfezionisti.it) e gli anni scorsi sono stato molto orgoglioso di questo appuntamento. Credo anche quest'anno lo sarò.

I temi che vorremmo affrontare sono tanti. Tra questi:
- Internet of Things (con particolare riguardo per le implicazioni giuridiche e sulla privacy nell'accesso ai dati dei sistemi di videosorveglianza);
- applicazioni di tecniche forensi ai centralini VoIP;
- implicazione giuridiche nel trattamento dei soggetti vittime dei ramsonware (con riferimento alle vittime ma anche ai loro consulenti);
- Regolamento UE privacy ;
- valorizzazione della professione di informatico forense.

Vi invitiamo quindi a segnalarci se volete partecipare come relatori o se avete dei suggerimenti su chi coinvolgere. Vorremmo promuovere interventi su esperienze pratiche o su progetti innovativi.

Ultimo punto su cui vi chiediamo collaborazione riguarda la ricerca di sponsor: se avete qualche contatto da segnalarci, ve ne saremo grati.

**********

**01- Pubblicato il nuovo Regolamento privacy**

Sulla Gazzetta ufficiale della UE è stato pubblicato il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

In realtà è stato pubblicato tutto il "nuovo pacchetto privacy", che include anche 2 Direttive (segnalo che il mese scorso avevo segnalato solo l'approvazione del Regolamento, dimenticandomi delle Direttive; Agostino Oliveri mi ha segnalato l'errore e io mi scuso per l'incompletezza dell'informazione):
- Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio
- Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.

Qui il link al testo ufficiale, da cui può essere letto in tutte le lingue dell'Unione:
- http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=OJ:L:2016:119:TOC.

Il Regolamento sostituirà quindi il nostro Dlgs 196/2003 (cosiddetto "Codice privacy"). Le Direttive, invece, dovranno essere recepite da nostri Decreti legislativi. Entro il 24 maggio 2018 tutte le aziende dovranno adeguarsi al nuovo Regolamento.

Dovremo quindi vedere, nel futuro, se il Dlgs 196 verrà abrogato totalmente o parzialmente (e quindi, per esempio, se rimarrà in vigore l'Allegato B e altre sue parti non previste dal Regolamento. Dovremo anche vedere come il nostro Garante modificherà o abrogherà i Provvedimenti generali o settoriali emessi negli anni (spero che sarà quanto prima creata una pagina dedicata a questo argomento).

Segnalo alcuni punti a mio parere fondamentali se confrontati a quanto già previsto dal nostro Dlgs 196 del 2003:
- necessità di minimizzare i dati raccolti e trattati considerando le diverse finalità;
- inserimento, nell'informativa, dei tempi di conservazione dei dati e diritto all'oblio;
- diritto di portabilità dei dati;
- possibilità di certificazioni che possono dimostrare gli obblighi del titolare del trattamento;
- principi di protezione fin dei dati fin dalla progettazione e di default;
- nessuna considerazione delle attuali filiere di fornitura "lunghe" (ma questa non è una novità, purtroppo);
- predisposizione di un "registro dei trattamenti" per molte aziende;
- comunicazione al Garante da parte di qualunque titolare che subisce delle violazioni dei dati trattati;
- valutazione degli impatti in caso di specifici trattamenti e condizioni (con indice del rapporto);
- previsione di un "referente (o responsabile) della protezione dei dati" in casi particolari (che però fa riferimento a "trattamenti di dati sensibili su larga scala", senza specificare cosa "su larga scala" significa).

Segnalo quindi questo articolo (da tweet di @europrivacy) dal titolo "Lack of EU Data Reg Guidance Has Companies Uncertain":
- http://www.bna.com/lack-eu-data-n57982070660/.

Ne approfitto per segnalare questo sito web del CNIL che spiega, per ogni Paese del mondo, le regole da seguire per trasferirvi i dati personali:
- https://www.cnil.fr/en/data-protection-around-the-world.

Qualche mia domanda ironica:
- fino a che anno leggeremo documenti con scritto "il nuovo Regolamento europeo sulla privacy";
- fino a che anno leggeremo informative e documenti con riferimento al Dlgs 196/2003 (io ho visto riferimenti alla L. 675/1996, abrogato nel 2003, anche nel 2014).

Non dimentico di ringraziare chi mi ha avvisato della pubblicazione del Regolamento: Fabrizio Bottacin del Politecnico di Milano (che mi ha anche allegato il file in italiano); Biagio Lammoglia (che mi ha inviato i link al "pacchetto privacy" sia in inglese che in italiano); Pierfrancesco Maistrello di Vecomp (che però mi ha fornito il link alla sola versione in italiano) e Pasquale Tarallo (anche lui con la sola versione in italiano). Anche se ho ricevuto la medesima notizia molte volte, mi ha fatto piacere in tutti i casi.

**********

**02- Garante privacy: Facebook e il furto di identità**

È stata sufficientemente pubblicizzata la notizia relativa alla pronuncia del Garante privacy in merito alle false utenze su Facebook:
- http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/4833448.

Ho trovato molto interessante questo articolo che ne spiega l'importanza:
- http://www.webnews.it/2016/04/27/garante-facebook-fake/.

Riassumendo molto, una persona ha subito un furto di identità su Facebook e ha chiesto aiuto al social network, ma "la richiesta di cancellazione o del blocco del falso account, nonché la comunicazione dei suoi dati in forma chiara, anche di quelli presenti nel fake, non sembravano un percorso fattibile".

Il Garante privacy ha quindi dato ragione alla vittima.

**********

**03- Privacy: Modulo unificato per videosorveglianza e GPS**

Il Ministero del lavoro ha pubblicato un modulo, valevole a livello nazionale, per richiedere l'autorizzazione all'installazione di impianti di videosorveglianza e all'installazione e utilizzo di impianti e apparecchiature di localizzazione satellitare GPS a bordo di mezzi aziendali:
http://www.assodpo.it/News/tabid/98/articleId/112/articlesListTabId/98/articlesListModId/541/articleDetailsModId/541/listType/templateBased/Default.aspx.

Qual è la novità? Che in precedenza ogni Direzione territoriale aveva il proprio modulo, mentre oggi ce n'è uno solo.

Questa notizia mi è stata data da Massimo Cottafavi di Snam, che ringrazio.

**********

**04- L'FBI può attaccare qualunque computer nel mondo**

La notizia è decisamente inquietante (da tweet di @F_Traficante): la Corte suprema USA ha sancito nuove regole per le investigazioni digitali dell'FBI che a breve potrà compromettere più facilmente i computer di chiunque, ovunque si trovi, sia indiziato di un qualsiasi reato:
- http://www.repubblica.it/tecnologia/sicurezza/2016/04/29/news/corte_suprema_usa_intercettazioni-138732392/.

Questo articolo ("U.S. Supreme Court allows the FBI to Hack any Computer in the World") è in inglese (da tweet di @mayhemspp):
- http://thehackernews.com/2016/04/fbi-hacking-power.html.

**********

**05- eIDAS: norme di sicurezza per dispositivi di creazione di firme e sigilli elettronici**

Da un tweet di @fposati, segnalo che è stata pubblicata in Gazzetta ufficiale UE la decisione di esecuzione 2016/650 del 25 aprile 2016 della Commissione europea. Essa stabilisce le norme per la valutazione di sicurezza dei dispositivi per la creazione di una firma e di un sigillo qualificati a norma del Regolamento eIDAS.

Riporto il link a Diritto&Internet con la notizia e il link alla decisione:
- http://www.blogstudiolegalefinocchiaro.it/documento-informatico-e-firma-digitale/sicurezza-e-firma-elettroniche-pubblicate-le-norme-ue/.

Questa decisione si affianca alle alte già pubblicate per l'esecuzione delle disposizioni del Regolamento eIDAS di cui ho già parlato in altri articoli (dovrei cercare di realizzare un elenco di quante decisioni sono previste e quante pubblicate).

Ricordo la pagina della Commissione europea dedicata a questo tema, anche se non aggiornata con questa ultima decisione:
- https://ec.europa.eu/digital-single-market/en/trust-services-and-eid.

**********

**06- Stato delle norme ISO/IEC 270xx**

Venerdì 15 aprile si è concluso a Tampa (Florida, USA) il 52mo meeting dell'SC 27 dell'ISO/IEC JTC 1, ossia il gruppo che si occupa della redazione e aggiornamento delle norme collegate alla ISO/IEC 27001 e a cui ho partecipato come delegato italiano.

Rapidamente elenco lo stato delle norme discusse:
- ISO/IEC 27001: si è deciso di non procedere, per ora, al suo aggiornamento, ritenendo adeguata l'attuale versione del 2013;
- ISO/IEC 27002: si è deciso di avviarne l'aggiornamento (richiederà comunque qualche anno);
- ISO/IEC 27003 (guida alla ISO/IEC 27001): non è stata discussa e se ne è rimandata la discussione a giugno in modo da redigere la bozza finale (FDIS) e, spero pubblicarla per fine 2016;
- ISO/IEC 27004 (guida alle misurazioni della sicurezza): come la ISO/IEC 27003, la discussione è stata rimandata a giugno;
- ISO/IEC 27005 (guida alla valutazione del rischio): dopo anni di discussione su una bozza, si è deciso di ripartire da zero; questo, ahimè, rimanderà l'aggiornamento (necessario) di questa norma importantissima di almeno 3 anni;
- ISO/IEC 27007 (guida all'audit sulla ISO/IEC 27001): si è proceduto a migliorare la bozza della sua nuova versione (non ritengo si tratti comunque di una norma fondamentale);
- ISO/IEC 27008 (guida alla valutazione dei controlli di sicurezza): come per la ISO/IEC 27007, si è discusso delle bozze di una nuova versione di questa norma;
- ISO/IEC 27009 (uso della ISO/IEC 27001 in specifici settori): si è discusso della bozza finale in modo che venga pubblicata quanto prima;

- ISO/IEC 27011 (controlli per il settore delle telecomunicazioni): si è discusso in modo da predisporre la bozza finale di una nuova versione di questa norma;
- ISO/IEC 27014 (governance della sicurezza delle informazioni): si è deciso di aggiornare questa norma; i lavori quindi partiranno al prossimo incontro;
- ISO/IEC 27019 (controlli per il settore dell'energia): si è discusso delle bozze di una nuova versione di questa norma;
- ISO/IEC 27021 (competenze sui sistemi di gestione per la sicurezza delle informazioni): si è discusso delle bozze di questa nuova norma.

Si sono discusse anche molte altre cose. Mi piace segnalare solo che sono stati avviati i lavori per una norma sulle "cyber insurance".

**********

**07- ISO/IEC 29147 sulla gestione delle vulnerabilità è gratis**

Da un tweet di @mattia_reggiani, segnalo che la ISO/IEC 29147, dal titolo "Information technology -- Security techniques -- Vulnerability disclosure" è ora gratuita:
- http://www.itnews.com.au/news/iso-vulnerability-disclosure-standard-now-free-418253.

L'articolo segnalato fornisce qualche dettaglio in più su questo standard e quanto è collegato ad esso.

**********

**08- Rapporto semestrale MELANI**

È pubblicato il 22o rapporto semestrale della "Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI" della Confederazione Svizzera:
- https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/rapporto_semestrale-2-2015.html.

Si trova anche in inglese.

In questo numero il tema principale è la gestione delle vulnerabilità (ma purtroppo non dà raccomandazioni complete per aggiornarsi).

Io sono un fan dei rapporti MELANI e ne consiglio sempre la lettura.

**********

**09- Report di sicurezza delle informazioni 2016**

Verizon ha pubblicato il suo Data Breach Investigations Report (DBIR) 2016:
- http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.

Non mi pare dica niente di fondamentale e non riesco a capirne fino in fondo l'impostazione (sono analizzate alcune minacce in modo un po' disomogeneo; ci sono delle raccomandazioni, ma non mi sembrano sempre pertinenti alla minaccia in questione). Chi vuole leggere la versione breve, segnalo questo articolo di DarkReading:
- http://www.darkreading.com/endpoint/verizon-dbir-over-half-of-data-breaches-exploited-legitimate-passwords-in-2015/d/d-id/1325242.

Anche la Microsoft ha pubblicato il suo report "Security Intelligence Report (SIR)" relativo al secondo semestre 2015 (a tweet di @skhemissa):
http://www.neowin.net/news/microsoft-publishes-security-intelligence-report-including-cloud-data-for-the-first-time.

Non basta? Ecco un elenco di 9 report sulla sicurezza (da un tweet di @ieeecybsi). Ce n'è per tutti i gusti (segnalo però che il report di Juniper è segnalato malamente, subito dopo quello di Verizon, di cui ho già scritto qui sopra):
- http://www.forbes.com/sites/stevemorgan/2016/05/09/top-2016-cybersecurity-reports-out-from-att-cisco-dell-google-ibm-mcafee-symantec-and-verizon/#49a0a0333edb.

**********

**10- qSOA**

Luciano Quartarone ha reso pubblico un suo foglio Excel per realizzare una Dichiarazione di applicabilità (o Statement of applicability o SOA) utilizzabile per la conformità alla ISO/IEC 27001 o per una valutazione dei controlli di sicurezza:
- http://www.lucianoquartarone.it/wp/?p=752.

Gentilmente, Luciano fa notare che si può integrare con il mio foglio di calcolo VERA per calcolare dei livelli di rischio.

**********

**11- DevOps e SIAM**

Federico Corradi di Cogitek mi ha scritto qualche tempo fa per chiedermi se fossi a conoscenza di certificazioni personali in ambito DevOps e SIAM.

Confesso che, pur avendo letto in giro di DevOps, gli dissi che non ne sapevo quasi nulla. Federico Corradi continuò le sue ricerche e me ne ha reso partecipe. Ritengo che sia quindi utile condividerne una sintesi.

DevOps si occupa del rapporto tra sviluppatori di applicazioni IT (normalmente già strutturati con metodo Agile) e le operation (gestori dei sistemi, ma non solo). Materia fondamentale e molto antica, ma un po' dimenticata in questi anni in cui si è puntato soprattutto a migliorare il rapporto tra utilizzatori (o "business") e sviluppatori di servizi IT.

Per quanto riguarda esami e certificazioni personali DevOps, Federico Corradi ha visto che Exin ha annunciato una Devops Master Certification (mi era sembrato di averla vista in qualche email da parte di Exin, visto che con loro collaboro!) che dovrebbe essere disponibile entro l'estate 2016. Anche itskeptic ha annunciato che OGC (!) si dedicherà a Devops e questa certificazione entrerà nel catalogo dei "soliti noti", Exin inclusa.

Federico Corradi ha anche contattato il "Devops Iinsitute", che propone un corso dedicato (DevOps Foundation) e poi due corsi Agile con argomenti DevOps (Certified Agile Service Management o CASM; Certified Agile Process Owner o CAPO).

SIAM (Service Integration and Management) si occupa della gestione di contratti multi-sourcing, ossia contratti con vari fornitori che devono essere tra loro integrati. Anche questa è materia molto antica, soprattutto in ambito manifatturiero, anch'essa negletta in ambito IT soprattutto in questi anni in cui sembra che gli unici fornitori degni di nota siano quelli di servizi cloud.

Federico Corradi è riuscito a trovare due pubblicazioni promozionali sul SIAM:
- una di Axelos: https://www.axelos.com/case-studies-and-white-papers/who-is-the-king-of-siam;
- una del Information Services Group (ISG; www.isg-one.com): "Assembling the jigsaw: Service Integration and Management in a Multisourced Operating Model".

Sembra però che questa materia sia troppo recente e, quindi, non sono disponibili certificazioni in materia.

**********

**12- Nuovo PCI DSS 3.2**

Enos mi ha segnalato la nuova versione del PCI DSS, ora arrivata alla 3.2.

Segnala l'articolo del SANS (che insiste soprattutto sull'aggiornamento a TLS 1.2):
- https://isc.sans.edu/forums/diary/New+release+of+PCI+DSS+version+32+is+available/21003/

Un documento più tecnico, nonché ufficiale, è il "Summary of changes":
- https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2_Summary_of_Changes.pdf

Un articolo (da tweet di @mattia_reggiani):
- https://www.helpnetsecurity.com/2016/04/28/pci-dss-3-2-whats-new/

Anche se non ci si occupa di circuiti di carte di credito, è importante conoscere il PCI DSS perché, con tutte le cautele del caso, rappresenta uno stato dell'arte della sicurezza informatica.

**********

**13- Email temporanee**

Non sapevo esistessero i servizi di email temporanee (e gratuite). Grazie ad un tweet di @enigmadt ora lo so e condivido questa informazione:
- http://focustech.it/email-temporanea-mail-gratuita-come-107163.

**********

**14- Come si pronuncia "auditor"? (2a parte)**

Il mese scorso avevo scritto un piccolo articolo sulla pronuncia della parola "auditor":
- http://blog.cesaregallotti.it/2016/03/come-si-pronuncia-auditor.html.

Dicevo che l'Accademia della crusca segnalava che la pronuncia in italiano di "auditor" poteva basarsi su una raccomandazione della ISO 9000:2005. Però io questa raccomandazione non l'avevo trovata.

Stefano Brancolini di Engineering, che ringrazio, mi ha segnalato che questa questione è riportata nella UNI EN ISO 19011 (evidentemente c'è un refuso sul sito dell'Accademia della crusca), dove non si parla in modo esplicito della pronuncia, ma della derivazione latina.

Franco Ruggieri ha colto l'occasione per segnalarmi che nell'ordine dei cavalieri di S. Stefano, creato nel 1562 da Cosimo I de' Medici con sede a Pisa, c'era la carica dello "Auditore" che aveva il compito di controllare tutto l'Ordine. In effetti ne era il vero Capo. Quindi, ben prima che ereditassimo dagli anglo-sassoni il termine "auditor", c'era già in vigore una carica con tale nome. Ergo: il termine è di origine latina e non britannica!

Grazie Franco: un po' di cultura storica non fa mai male (anzi!).