Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – APRILE 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.

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- Approvato il Regolamento europeo sulla privacy

Finalmente, dopo diversi anni di elaborazione è stato approvato il Regolamento europeo sulla privacy:
- http://www.europarl.europa.eu/news/en/news-room/20160407IPR21776/Data-protection-reform-Parliament-approves-new-rules-fit-for-the-digital-era.

Qualche approfondimento dal Parlamento europeo sulla riforma:
- http://www.europarl.europa.eu/news/en/news-room/20160413BKG22980/QA-new-EU-rules-on-data-protection-put-the-citizen-back-in-the-driving-seat.

La pagina informativa del Garante (grazie a Pierfrancesco Maistrello per la segnalazione):
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4443361.

Ricordiamolo: questo Regolamento sostituirà il nostro Dlgs 196 del 2003 e sarà applicabile in tutta Europa.

I tempi: intorno a giugno sarà pubblicato nella Gazzetta ufficiale europea (EU Official Journal) e dopo 2 anni e 20 giorni dovrà essere applicato. Quindi c'è ancora un po' di tempo.

Il testo definitivo approvato ancora non ce l'ho. Non so se prendere per buono quello che circola da gennaio e quindi aspetto. Sul sito del Garante ci sono comunque i testi in italiano e alcuni hanno gioito per il ritorno dei termini "Titolare" e "Responsabile" (http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/4884272).

Confesso che mi mancheranno i consulenti che vendevano (dal 2012!) questo regolamento come imminente. Era una buona cartina di tornasole per capire la loro preparazione e prudenza.

A questo aggiungo altre due notizie. La prima, grazie anche per questo a Pierfrancesco Maistrello, riguarda l'inizio della revisione della "ePrivacy Directive" (quella dei cookies, per intenderci):
- https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive.

La seconda riguarda l'avanzamento del Privacy Shield, ossia l'accordo tra USA e Europa in merito alla privacy. Il WP Art. 29 ha dato il suo parere (grazie a un tweet di @EU_EDPS) con la "Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision"
- http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

****

02- Fornitori e ruoli privacy (ulteriore puntata)

In merito alla mia riflessione su fornitori e ruoli privacy (http://blog.cesaregallotti.it/2016/03/fornitori-e-ruoli-privacy.html), mi hanno fatto notare quanto segue.

Il Garante non si è mai espresso poiché il ricorso a sub-fornitori non è una pratica vista di buon occhio (anzi, ci sono delle posizioni negative). In altre parole, il titolare può nominare il responsabile, che però non può demandare a terzi.

Ma…..poiché la realtà è quella che è, la linea da seguire è analoga a quanto previsto nei diversi provvedimenti per i trasferimenti all'estero: ci deve essere un mandato generale o specifico affinché il

responsabile possa contrarre accordi con sub-fornitori, purché ne informi il titolare e ne abbia l'approvazione.

Ecco quindi che la situazione non migliora! E il Garante, ahinoi, continua a pensare che:
a) una filiera di fornitura corta sia meglio di una lunga; non avrebbe torto, ma dovrebbe considerare che in Italia il 99% delle aziende sono PMI ultra specializzate, ed è meglio avere una filiera lunga di gente capace che una filiera corta di gente incapace; e anche all'estero è così;
b) le aziende si possano adeguare ad avere una filiera di fornitura corta; dovrebbe invece dare istruzioni chiare e praticabili su come gestire una filiera lunga;
c) tutti dovremmo nominare certi grandi operatori (o i suoi concorrenti) come responsabili esterni e chiedere di autorizzare i suoi sub-fornitori...

Le mie riflessioni in merito a fornitori e sub-fornitori e privacy sono state pubblicate su Europrivacy:
- in italiano: http://europrivacy.info/it/2016/03/25/processors-and-sub-processors/;
- in inglese: http://europrivacy.info/2016/03/25/processors-and-sub-processors/.

****

03- Standardizzazione: ISO 22318 - Continuità della filiera di fornitura

Franco Ferrari di DNV GL mi ha segnalato la pubblicazione (a settembre!) della ISO/TS 22318 dal titolo "Societal security — Business continuity management systems — Guidelines for supply chain continuity":
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=65336.

Questa norma fornisce alcuni spunti interessanti sulla gestione dei fornitori relativamente alla continuità operativa. Soprattutto non riduce erroneamente il tutto a "chiedere ai fornitori di avere un piano di continuità operativa".

Una riflessione su questi standard: sono utili? Per studiare la continuità operativa non sarebbe meglio leggere un libro piuttosto che uno standard?

Scusatemi, per una volta che non parlo male di uno standard ISO, riesco a lamentarmi lo stesso...

****

04- Standardizzazione: ISO/IEC 30121 - Governance of digital forensic

A marzo 2015 è stata pubblicata la ISO/IEC 30121 dal titolo "Governance of digital forensic risk framework":
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53241.

Se togliamo copertina, indice, appendici e altre cose, rimangono 3 pagine. Queste 3 pagine non dicono nulla né di interessante né di utile. Mi chiedo perché l'abbiano voluta pubblicare.

In realtà lo so: qualcuno ha proposto al comitato (ISO/IEC JTC1 SC40) la norma e nessuno ha avuto la voglia di bocciare l'idea. In realtà, alcuni l'hanno appoggiata per potersi poi vantare con amici, parenti, clienti e potenziali clienti di aver scritto uno standard sulla digital forensics. Con la speranza che nessuno vada a vedere quale (nullo) contributo sia stato dato alla materia.

Se però sbaglio, vi prego di dirmelo e mi scuserò.

PS. Angus Marshall su LinkedIn mi ha fatto notare che questo standard ha almeno una funzione: usando il termine "governance", rende la digital forensics aziendale un tema della Direzione e non solo dei

tecnici. Io continuo a pensare che mi sembra un po' poco per un nuovo standard, ma almeno ne ho capito la finalità.

****

05- Standardizzazione: EN 16234-1:2016 sulle competenze digitali

Da AgID ricevo la notizia della pubblicazione della EN 16234-1:2016 "e-Competence Framework (e-CF) – A common European Framework for ICT Professionals in all industry sectors – Part 1: Framework":
- http://www.agid.gov.it/notizie/2016/04/07/nasce-il-framework-europeo-competenze-digitali.

Per ora si tratta solo dello schema di riferimento, mentre le caratteristiche dei profili professionali saranno pubblicate in un secondo tempo.

Giusto segnalare che questo schema di riferimento è uguale al e-CF 3.0, disponibile gratuitamente anche in italiano:
- http://www.ecompetences.eu/e-cf-3-0-download/.

****

06- Standardizzazione: ISO 8000-8:2015 sulla qualità dei dati

Franco Ferrari di DNV GL mi ha segnalato la pubblicazione della ISO 8000-8:2015 dal titolo "Information and data quality: Concepts and measuring":
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=60805.

Mi sembra interessante perché definisce cosa si intende per "qualità dei dati" nelle tre categorie di sintassi, semantica e pragmatica (questa è la più complessa, in quanto comprende sicurezza, accessibilità e completezza).

Vedo che si tratta di uno standard di "requisiti", ossia certificabile, in quanto usa la forma verbale "shall".

Da notare un'altra cosa: è pubblicata anche un'altra norma sulla qualità dei dati. È la ISO/IEC 25012:2008 dal titolo "Software engineering -- Software product Quality Requirements and Evaluation (SQuaRE) -- Data quality model". Giusto per creare un po' di confusione.

****

07- Standardizzazione: Presentazione UNINFO al Security summit

Ringrazio Domenico Squillace, presidente UNINFO, per aver messo a disposizione le slide della nostra presentazione del 16 marzo al Security summit di Milano.

L'incontro aveva come titolo "Norme tecniche nazionali e internazionali sulla sicurezza delle informazioni: ultime novità" e si trovano a questo link:
- http://www.slideshare.net/uninfoit/norme-tecniche-nazionali-e-internazionali-sulla-sicurezza-delle-informazioni-ultime-novit.

****

08- SPID: rapporto con eIDAS e difficoltà

Come noto, SPID è il sistema pubblico di identità digitale, lanciato ufficialmente il 15 marzo scorso.

Andrea Caccia mi ha segnalato questo suo articolo dal titolo "Regolamento eIDAS: differenza tra i servizi di identificazione come SPID e i servizi fiduciari":
- https://www.linkedin.com/pulse/regolamento-eidas-differenza-tra-i-servizi-di-come-spid-andrea-caccia.

In questo post, come mi segnala Andrea, anche collegato al tema assicurazioni, viene illustrato il grosso dibattito in corso con riferimento alle modifiche presenti nella proposta di modifica al CAD.

Avevo un dubbio sulla PEC e Andrea (grazie!) mi ha risposto così: la PEC nella terminologia eIDAS, è un "servizio di recapito elettronico certificato".

Inoltre segnalo questo post di Daniele Tumietto:
- https://www.linkedin.com/pulse/il-consiglio-di-stato-annulla-definitivamente -i-criteri-tumietto.

Il Consiglio di Stato ha bocciato i criteri di qualifica dei fornitori di SPID, che prevedevano 5 milioni di capitale sociale. Il modello era infatti incentrato sulla presenza di pochissimi fornitori di grandi proporzioni economiche.

Vedremo cosa succederà.

****

09- Legale: Ricette mediche elettroniche - riferimenti normativi

Mi hanno segnalato un riferimento autorevole per approfondire il decreto del Ministero economia e finanze del 2 novembre 2011, che norma la dematerializzazione della ricetta medica per le prescrizioni a carico del Servizio sanitario nazionale:
http://sistemats1.sanita.finanze.it/wps/content/portale_tessera_sanitaria/sts_sanita/home/sistema+ts+informa/medici+in+rete/ricetta+dematerializzata+dm+2+novembre+2011.

Inoltre, questo DM, che riguarda la tessera sanitaria, un collettore di svariati dati personali (!), non è stato sottoposto al parere del Garante privacy, come denunciato dal Garante stesso nella sua relazione del 2011:
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2148180.

Un grazie al mio anonimo corrispondente.

****

10- Legale: Diffamare via mail è reato, ma non aggravato

Questa sentenza mi sembra interessante: inviare un'email "diffamatoria" via email ad un preciso insieme di destinatari, per quanto numeroso, è sì reato, ma non aggravato:
- http://www.penalecontemporaneo.it/area/2-/6-/15-/4506-diffamazione_tramite_e_mail__aggravante_del_fatto_commesso___col_mezzo_della_stampa_o_con_qualsiasi_mezzo_di_pubblicit_____ed_eventuale_competenza_del_giudice_di_pace__una_sentenza_del_tribunale_di_milano/

Notizia ricevuta da un tweet di @Silvia_Mar_, che fornisce il seguente link, che richiede registrazione:
- http://www.quotidianogiuridico.it/documents/2016/03/18/diffamare-via-mail-e-reato-ma-non-aggravato.

****

11- Rapporto Clusit 2016

Segnalo la pubblicazione del Rapporto Clusit 2016, forse la pubblicazione italiana più importante in materia di sicurezza informatica (tranne la mia newsletter, ovviamente!):
- http://clusit.it/rapportoclusit/.

A parte gli scherzi, una prima e veloce lettura mi è sembrata molto interessante. Per esempio ho imparato che il nostro CERT nazionale è attivo e ha un sito web interessante (https://www.certnazionale.it/), con diverse segnalazioni utili. C'è anche il CERT di Poste Italiane (www.picert.it), ma il loro sito mi è sembrato meno interessante e meno aggiornato.

C'è altro ancora, ma, per saperlo, vi consiglio di leggerlo.

****

12- Cisco 2016: Annual Security Report

Fabrizio Cirilli mi ha segnalato il "Cisco 2016: Annual Security Report".

In inglese:
- http://www.cisco.com/c/m/en_us/products/security/offers/cybersecurity-reports.html?Keycode=001124371.

In Italiano:
- http://www.cisco.com/c/dam/m/it_it/offers/assets/pdfs/cisco_2016_asr_011116_it.pdf.

****

13- Sicurezza nei social media

Pierfrancesco Maistrello mi ha segnalato questa pubblicazione del Clusit e di Oracle Community for Security dal titolo "La sicurezza nei social media":
- http://social.clusit.it.

Come spesso mi succede, faccio questa segnalazione con grande ritardo. Forse non avevo notato la notizia a suo tempo o forse l'avevo ignorata perché ci sono molte pubblicazioni su questo tema. Però questa è fatta bene ed è fatta in italiano. Non ci sono più scuse per ignorare questo argomento.

****

14- Tool per formare le persone sul phishing

Non so come funzioni esattamente questo strumento GoPhish, ma mi piace l'idea: formare il personale in modo pratico affinché riconosca il phishing e non faccia errori che possono compromettere la propria organizzazione o la propria vita privata:
- https://www.helpnetsecurity.com/2016/04/12/gophish-free-phishing-toolkit-training-employees/.

****

15- Google Vendor Security Assessment Questionnaire (VSAQ) Framework

Google ha reso disponibile il questionario che sottopone ai propri fornitori.

Il questionario è dinamico. Se la risposta non è "perfetta", l'utente è indirizzato verso una spiegazione del perché quanto dichiarato rappresenta un rischio e verso un campo in cui elencare eventuali controlli compensativi.

Penso sia il caso di leggerlo con attenzione e trarne esempio.

La pagine di Google, da cui scaricare il sorgente del questionario o accedere alla demo:
- http://google-opensource.blogspot.it/2016/03/scalable-vendor-security-reviews.html.

La notizia mi arriva dal gruppo "Certified Information Systems Auditor" di LinkedIn, che ha inoltrato un post, sempre su LinkedIn, di Aurav Agarwal.

****

16- Analisi attacco a centrale elettrica ucraina

ll SANS ha pubblicato un'analisi dell'attacco del 23 dicembre 2015 ad una centra elettrica ucraina:
- http://www.darkreading.com/vulnerabilities---threats/lessons-from-the-ukraine-electric-grid-hack/d/d-id/1324743.

Ho segnalato l'articolo di Darkreading perché è una pagina web dove si trova il link al pdf del SANS. E poi riporta le stesse cose ma più sinteticamente.

Io l'ho capita così: gli attaccanti hanno inviato email mirate (spear phishing) a degli addetti della centrale. Hanno anche allegato dei file (Word, Excel) con delle macro nocive. Gli addetti hanno aperto i file ed è stato l'inizio della fine.

L'articolo prosegue indicando le misure di sicurezza da prevedere per evitare questi attacchi. A me sembrano decisamente complicate. Io tornerei alle basi: se si lavora in un impianto critico, la rete industriale deve essere completamente separata da quella usata per navigare su Internet e per ricevere l'email. Se gli operatori ne hanno bisogno, date loro 2 pc collegati alle due diverse reti.

Troppo semplice? Dove sbaglio?

PS: Su LinkedIn, Damiano Bolsoni mi ha risposto dicendo che non pensa sia possibile avere due reti completamente separate. Infatti altre aree aziendali hanno la necessità di avere dati sulla produzione in tempo reale. Si possono attuare strategie di controllo di questo traffico, ma non è semplice.

Damiano Bolsoni, inoltre, mi ha fatto notare che l'attacco iniziale in Ucraina ha permesso ai malintenzionati di individuare le credenziali per usare le connessioni VPN. Se le VPN avessero avuto un

meccanismo di autenticazione basato su due fattori e la rete ben segmentata, questo avrebbe migliorato le difese.

****

17- Attacco ad una centrale idrica

Pierfrancesco Maistrello di Vecomp mi ha segnalato questo attacco ad una centrale idrica, simile a quello condotto contro la centrale elettrica in Ucraina:
- http://www.securityweek.com/attackers-alter-water-treatment-systems-utility-hack-report.

La segnalazione viene da Verizon, che ha modificato il nome della centrale idrica e non ha rivelato dove si trova.

Qui la situazione credo sia incredibile: lo stesso sistema per controllare l'impianto era usato per i pagamenti on-line.

Pierfrancesco (ovviamente) concorda con me: "non credo affatto che qualsivoglia esigenza legata al business possa imporre un'esposizione di queste reti all'esterno".

****

18- Il caso dell'attacco informatico a Staminus Communications

Il caso dell'attacco informatico a Staminus Communications

Da un tweet di @TechEcon, una descrizione di un attacco (in italiano):
- http://www.techeconomy.it/2016/03/18/92899/.

Lascia perplessi l'elenco delle vulnerabilità sfruttate per condurre l'attacco. Alcune cose sono sì diffuse, ma presso una società di sicurezza fa effetto.

Nota sociale: la Staminus Communications è una società USA, quindi non è vero che gli italiani non applicano la sicurezza per "questioni culturali", ma è vero che molte aziende non applicano la sicurezza perché alla Direzione non interessa.

****

19- Come si pronuncia "auditor"?

A marzo avevo dato la notizia della pubblicazione delle nuove versioni di ISO 9000 e ISO/IEC 27000, dedicate alle definizioni in ambito qualità e sicurezza delle informazioni.

Fabrizio Cirilli, che ringrazio, ha approfittato di questo per segnalarmi questo articolo dell'Accademia della crusca in merito alla pronuncia di audit, auditor, eccetera:
- http://www.accademiadellacrusca.it/it/lingua-italiana/consulenza-linguistica/domande-risposte/storia-pronuncia-termine-audit.

Pare che, in Italia, sia preferibile pronunciare "audit" alla latina e non "odit" all'inglese.

L'articolo fa riferimento a una raccomandazione riportata nella ISO 9000:2005. Confesso che non ho trovato il passaggio, ma mi adeguerò.

****