Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS –NOVEMBRE 2015

****

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

****

01- Privacy: guida della Commissione europea per il post-Safe harbor

Segnalo questo articolo con le novità in materia di Safe harbour e dal titolo"Safe Harbor Update: The European Commission Issues Guidance on the Schrems Decision":
- http://www.jdsupra.com/legalnews/safe-harbor-update-the-european-61218/.

Questo articolo fa riferimento ad una guida della Commissione europea:
- http://europa.eu/rapid/press-release_MEMO-15-6014_en.htm.

In sintesi: questa guida dice che è necessario usare le clausole contrattuali o le binding corporate rules (BCR).

Nulla è semplice e bisogna cercare un po' per recuperare documentazione utile. Per scrupolo la riporto:

- Clausole contrattuali per trasferimenti tra titolari: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447323316386&uri=CELEX:32004D0915 (da decisione 915 del 2004 della CE);
- Clausole contrattuali tra titolare e responsabile esterno: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447323878179&uri=CELEX:32010D0087 (da decisione 87 de 2010 della CE);
- Schema di BCR del Art. 29 Working Party e riportato dai documenti WP 153, WP 154 e WP 155, reperibili al link http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

Questi riferimenti li ho trovati nel documento "Communication from the Commission to the European parliament and the Council on the transfer of personal data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)" del 6 novembre 2015:
- http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf.

****

02- Privacy: DPCM sul Fascicolo sanitario elettronico

È stato pubblicato sulla Gazzetta ufficiale il Decreto del Presidente del Consiglio dei ministri numero 178 del 29 settembre 2015 e dal titolo "Regolamento in materia di fascicolo sanitario elettronico":
- www.gazzettaufficiale.it/eli/id/2015/11/11/15G00192/sg.

Devo studiarlo. Immagino il Provvedimento sul Fascicolo sanitario elettronico (FSE) del Garante del 2009 (documenti web 1634116 e 1633793) sia abrogato. Ovviamente rimane in vita il Provvedimento sul Dossier sanitario elettronico (DSE) del 2015 (documento web 4084632).

Grazie ad Ernesto Belisario di cui ho letto un tweet con la notizia.

****

03- eIDAS: Regolamento eIDAS e CAD

Il Regolamento europeo cosiddetto eIDAS (n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2104) impone delle modifiche al nostro Codice per l'amministrazione digitale (CAD, D. Lgs. 82 del 2005).

Alcune considerazioni sono riportate da questo articolo dal titolo "Il senso del regolamento europeo eIDAS per il nuovo Cad: un coordinamento necessario":
- http://www.forumpa.it/pa-digitale/il-regolamento-europeo-910-slash-2014-eidas-e-il-suo-impatto-sulla-legislazione-nazionale-primaria-e-tecnica.

****
04- Legale: Nuovo Statuto dei lavoratori - Riflessioni

Valerio Vertua (Presidente di DFA) mi ha segnalato un interessante articolo di Andrea Stanchi sul controllo a distanza previsto dal nuovo articolo 4 dello Statuto dei lavoratori (ne ho parlato in http://blog.cesaregallotti.it/2015/10/privacy-statuto-dei-lavoratori.html):
- http://www.quotidianogiuridico.it/documents/2015/10/22/gps-il-controllo-per-la-cassazione-si-puo-fare-se-il-lavoratore-e-inadempiente.

Purtroppo l'articolo è ad accesso controllato. Io ho trovato queste slides, che sono ovviamente meno esaustive, ma comunque interessanti:
- http://www.pietroichino.it/?p=37560.

Stanchi parte da una sentenza in particolare (su una verifica dei movimenti di un lavoratore tramite GPS installato sulla macchina usata per gli spostamenti lavorativi) per alcune considerazioni.

In particolare: tramite gli strumenti posso eseguire i controlli sull'impiego corretto dello strumento rispetto alla sua specifica finalità (abuso ed uso illecito).

Inoltre suggerisce le finalità del trattamento dei dati personali raccolti dagli strumenti di lavoro: verifica della conformità del risultato della prestazione, verifica della qualità della prestazione, accertamento delle difformità, provvedimenti disciplinari e denunce penali.

****
05- Legale: Diffamazione via web: sentenza sugli accertamenti

Segnalo, da Altalex, questo articolo dal titolo "Reato di diffamazione mezzo web: l'accertamento è possibile grazie alla tecnica ed alla logica":
- http://www.altalex.com/documents/news/2015/08/25/diffamazione-rilievo-indirizzo-ip.

La Cassazione ha bocciato il ricorso della difesa, che riteneva inadeguate le prove di accusa di diffamazione perché:

- erano stampe delle pagine web in cui l'accusato aveva inserito dei post a nome della moglie con cui era in corso la separazione;
- nessun accertamento era stato fatto direttamente sul pc dell'accusato, ma solo facendo riferimento all'indirizzo IP dal quale erano stati inviati i post;
- l'indirizzo IP usato per inviare i post provenivano da un router (della casa della madre dell'accusato) che però poteva essere stato compromesso da altri.

Non ho letto completamente la sentenza, ma la Corte ha ritenuto completamente accettabile la condanna in quanto gli elementi raccolti sono incontestabili tecnicament, ma anche per un chiaro percorso di carattere logico-deduttivo.

La sentenza l'ho trovata qui:
- http://renatodisa.com/2015/08/12/corte-di-cassazione-sezione-v-sentenza-6-agosto-2015-n-34406-laccertamento-della-responsabilita-per-il-reato-di-diffamazione-commesso-a-mezzo-web-puo-desumersi-dallindividuazion/.

****

06- Standard: Stato delle norme ISO/IEC 270xx

Dal 26 al 30 ottobre si è svolto il 51o meeting del ISO/IEC JTC1 SC27, ossia l'incontro semestrale dei delegati delle diverse nazioni per scrivere le norme della serie ISO/IEC 270xx e non solo.

Questa volta la delegazione italiana era composta da tre persone (sempre poche): io, il presidente Fabio Guasconi e una persona dedicata alle norme correlate alla privacy.

Ecco lo stato delle norme della serie ISO/IEC 270xx, curate dal WG1 (ringrazio Fabio per aver fatto la sintesi):

- 27000 (vocabolario): dovrebbe uscire a breve una nuova edizione;
- 27001: noi italiani abbiamo individuato un errore da correggere (in sintesi e senza essere troppo accurato: è usato "criteri di rischio" per indicare la metodologia di valutazione del rischio, mentre la definizione e la ISO 31000 usano "criteri di rischio" solo per indicare i "criteri di ponderazione del rischio"; sembra una sciocchezza formale, ma credo sia nostro compito fare bene il lavoro ed evitare di introdurre elementi che potrebbero creare confusione);
- 27003 (guida alla 27001): il testo è stato migliorato e passa in DIS; se tutto va bene dovrebbe essere approvato ad aprile e pubblicato per fine 2016;
- 27004 (misurazioni e monitoraggio): testo riorganizzato ma non cambiato; passa in DIS;
- 27005 (gestione del rischio): rimane in bozza e rischia la cancellazione per superamento dei tempi massimi consentiti per il progetto; il comitato è molto litigioso;
- 27007 (linee guida per l'audit al sistema di gestione): rimane in bozza;
- 27008 (valutazione dei controlli di sicurezza): rimane in bozza;
- 27009 (certificazioni per settori particolari): va in bozza finale con alcuni voti negativi; personalmente credo sia una norma che potrebbe creare confusione perché promuove l'uso di linee guida insieme ad uno standard di requisiti (la ISO/IEC 27001);
- 27011 (controlli per le TLC): va in bozza finale;
- 27019 (controlli per il settore energia): rimane in bozza;
- 27021 (competenze): rimane in bozza ma cambia la struttura allineandosi a e-CF.

Altri lavori sono stati proposti (sulle assicurazioni, sulla resilienza, sulla sanità, sul settore avio). Ogni tanto penso si stia esagerando con questi standard, ma cerco di non contrastare chi ha voglia di lavorarci.

Per quanto riguarda gli standard correlati alla privacy:

- 29134 (per realizzare un privacy impact assessment, PIA): proseguono i lavori;
- 29151 (linee guida per la protezione dei dati personali): proseguono i lavori;
- 20889 (tecniche di de-identificazione): prima bozza.

Sono anche stati proposti lavori su informativa e consenso on-line, autenticazione, app per smartphone, smart city, correlazione tra privacy e ISO/IEC 27001.

Prossimo appuntamento ad aprile.

****

07- Controlli di sicurezza e standardizzazione: CIS Critical Security Controls

Stefano Ramacciotti mi ha segnalato questo documento dal titolo "The CIS Critical: Security Controls for Effective Cyber Defense":
- http://www.cisecurity.org/critical-controls.cfm.

Si tratta di una "solita" lista di controlli di sicurezza, con l'aggravante dell'uso "cyber". Però è ben fatta (sicuramente meglio della ISO/IEC 27002, con maggiori dettagli e più coerenza) e vale la pena leggerla. Il CIS mette anche a disposizione un Excel (xlsx) per condurre valutazioni su questi controlli.

Per scaricare il documento, purtroppo, è necessario fornire il proprio indirizzo email.

Lo stesso documento è stato ripreso dall'ETSI (www.etsi.org) come norma ETSI TR 103 305. Questa si può scaricare senza fornire i propri riferimenti, ma (visti i tempi di recepimento) potrebbe non essere aggiornata. Inoltre, in questo secondo caso, l'Excel non è disponibile.

Lo stesso documento è anche proposto dal SANS, che rimanda al sito del CIS:
- https://www.sans.org/critical-security-controls/.

In questo caso ho notato che il SANS mette anche a disposizione una "Solution Directory" che mi sembra essere (ancora) vuota. Trovo l'idea ottima e spero venga attuata quanto prima.

****

08- Controlli di sicurezza: Security scanner

Un articolo di Pete Herzog sui vulnerability scanner
- http://darkmatters.norsecorp.com/2015/10/19/the-awesome-truth-about-vulnerability-scanners/.

Il sottotitolo è: "uno strumento altamente tecnologico utilizzato male e incompreso". In effetti, tratta di funzionalità che non sapevo oggi fossero incluse in questo strumento. Pete Herzog mi dà (non direttamente) del vecchio... Oggi questi strumenti non sono più quelli degli inizi.

Un solo difetto dell'articolo: avrei preferito altri esempi di strumenti (viene citato solo Nessus).

****

09- Cloud Forensics Capability Maturity Model

CSA ha pubblicato il "Cloud Forensics Capability Maturity Model":
- https://cloudsecurityalliance.org/download/cloud-forensics-capability-model.

Mi dicono che è "un buon lavoro", anche se migliorabile. Ne raccomando la lettura perché molte indicazioni sono applicabili ad ogni tipo di fornitore.

****

10- Sviluppo: Presentazione sulla sicurezza del software

Segnalo questa presentazione di Gary McGraw, un guru della sicurezza del software:
- https://www.cigital.com/blog/annotated-att-cybersecurity-conference-keynote.

Alcuni dei link proposti conducono ad articoli interessanti. Per i più attenti potrebbe valere la pena considerare i libri di Gary McGraw.

Promuove anche il BSIMM, uno studio sulle iniziative per la sicurezza del software:
- https://www.bsimm.com/about/.

****

11- Sviluppo: Non parlate di "ingegneria" del software

Segnalo questo articolo dal titolo "Programmers: stop calling yourselves engineers":
- http://www.theatlantic.com/technology/archive/2015/11/programmers-should-not-call-themselves-engineers/414271/.

In poche parole: i programmatori e gli sviluppatori non sono "ingegneri", visto che non adottano le tecniche di ingegneria e i risultati, con bug, difetti e vulnerabilità, si vedono.

Personalmente ritengo che programmatori e sviluppatori dovrebbero tendere ad essere "ingegneri". Purtroppo, però, quando si chiede loro piani di progetto, documenti di requisiti e verbali di test (con o senza elementi di sicurezza), dimostrano di essere degli "artigiani". Nella peggiore delle ipotesi non hanno neanche idea di cosa gli sia stato chiesto; nella maggior parte dei casi, per contro, questi requisiti sono ben chiari ma applicati poco e male.

Certamente la colpa è gran parte da addebitare alle aziende che li pagano poco, considerano il loro lavoro come "banale", impongono tempi di analisi, sviluppo e verifica brevissimi. Un vero "ingegnere" (per esempio chiamato a progettare e costruire un ponte) rifiuterebbe di adeguarsi a queste condizioni (e non rimarrebbe senza lavoro, al contrario di programmatori e sviluppatori software).

Quindi, forse, per non confondersi e non illudersi, sarebbe effettivamente meglio essere consapevoli dei limiti della "ingegneria" del software nel mondo reale.

L'articolo segnala la "Guide to the software engineering body of knowledge (SWEBOK Guide)" dell'IEEE, che sembra interessante (è necessario fornire la propria email all'IEEE, ma si tratta di un ente serio e non credo la usi per fare spamming):
- http://www.computer.org/web/swebok/index.

****

12- Sviluppo: Riportare bug

Questo articolo ha titolo "If You Find a Software Bug, Don't Try to Report It to These Companies":
- http://blogs.wsj.com/digits/2015/11/05/if-you-find-a-software-bug-dont-try-to-report-it-to-these-companies/.

In breve: ci sono delle grandi società che non mettono a disposizione del pubblico un indirizzo a cui segnalare difetti o vulnerabilità individuati, altre (Microsoft, Amazon) lo fanno.

Ovviamente un canale di comunicazione per ricevere segnalazioni è fondamentale per poter migliorare i prodotti e servizi. Alcuni pensano che questo rappresenterebbe una dichiarazione di disfatta (come se non si sappia che i software sono sempre pieni di bug e vulerabilità), altri semplicemente non ci pensano.

****

13- Gestione del rischio: VERA 4.1

Il mio foglio di calcolo per un Very easy risk assessment (VERA) relativo alla sicurezza delle informazioni, ora è alla versione 4.1:
- http://www.cesaregallotti.it/Pdf/Pubblicazioni/2015-VERA-4.1.xlsx.

Reperibile anche sulla mia pagina web:
- http://www.cesaregallotti.it/Pubblicazioni.html.

Ringrazio Francesca Lazzaroni di Spike Reply per i contributi.

****

14- Mia presentazione ISO/IEC 27001

Introduzione alla ISO/IEC 27001: una mia presentazione per l'Ordine Ingegneri Pavia (pdf, 1,4MB):
- http://www.cesaregallotti.it/Pdf/Pubblicazioni/2015-Intro-ISMS.pdf

Potete anche trovarla sulla pagina web:
- http://www.cesaregallotti.it/Pubblicazioni.html.

****

15- Minacce: KeeFarce

KeeFarce è uno strumento per recuperare le password gestite da KeePass. KeePass, a sua volta, è uno strumento per memorizzare le tante password in modo sicuro.

KeeFarce, quindi, rende meno sicuro KeePass. Però alla condizione che il pc su cui è installato KeePass sia compromesso e l'utente legittimo lo abbia sbloccato. Rimane un prodotto di sicurezza da adottare (molte sue alternative, comunque da considerare, possono ritenersi allo stesso livello di sicurezza e insicurezza), purché si sia consapevoli dei suoi limiti.

Per saperne di più:
- http://arstechnica.com/security/2015/11/hacking-tool-swipes-encrypted-credentials-from-password-manager/.

Grazie a Pasquale Stirparo che annunciato la notizia.

Per la cronaca: io preferisco scrivere le password su un file testo e cifrarlo; ma io non sono amministratore di una rete complessa di sistemi informatici.

****

16- Minacce: Rapporto semestrale MELANI

È pubblicato il 21o 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/MELANI-21-rapporto-semestrale.html.

Si trova anche in inglese.

In questo numero il tema principale è la sicurezza dei siti Web. Ma non c'è solo questo: analisi degli ultimi attacchi e approfondimenti su altri temi come i dispositivi medici.

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

****

17- Attacchi: Intrusione nell'email del direttore della CIA

La notizia è pubblica: degli hacker sono entrati nell'email (quella su America On Line, AOL) del direttore della CIA e ne hanno diffuso i contenuti su Wikileaks.

Io vi segnalo questo articolo dal titolo "teen who hacked CIA director's email tells how he did it":
- http://www.wired.com/2015/10/hacker-who-broke-into-cia-director-john-brennan-email-tells-how-he-did-it/.

In estrema sintesi: scoprono che John Brennan ha un cellulare Verizon; chiamano Verizon spacciandosi per colleghi e ottengono delle informazioni; chiamano AOL e, con le medesime informazioni, si fanno dare una nuova password per accedere all'email di Brennan.

Qualche veloce, e semplice, considerazione:
- il direttore della CIA teneva quindi email critiche su AOL?
- spero che questo caso porti ad un innalzamento di sicurezza del meccanismo "reset password" dei fornitori di email.

Un dubbio. Forse a tutto il personale della CIA era stato vietato di usare servizi pubblici per archiviare o scambiare documenti critici. Ovviamente questa regole non si è applicata ai vertici dell'organizzazione... Chissà perché.

****

18- Il boom della sicurezza informatica

Questo articolo del The Economist ("The cost of immaturity: The business of protecting against computer-hacking is booming") è quasi banale: a seguito del crescere degli attacchi informatici, si sta avendo un boom dei servizi di sicurezza informatica:
- http://www.economist.com/news/business/21677639-business-protecting-against-computer-hacking-booming-cost-immaturity.

Il boom fa sì che molti "professionisti" non sono competenti e molti servizi sono di scarsa qualità. Questo anche perché non sono disponibili certificazioni professionali riconosciute.

Mi permetto di fare tre appunti:
- il dilagare dell'incompetenza lo vedo dal 1999 (tra i tecnici e i consulenti), quando ho cominciato a lavorare in questo settore, quando il "boom" era sempre previsto per l'anno dopo;
- evidentemente bisognava aspettare il 2014 per dire, con ragione, che il boom della sicurezza informatica sarebbe stato l'anno successivo (i fanfaroni c'erano anche allora, anche se non usavano i social network per diffondere messaggi profondi di 144 caratteri);
- le certificazioni non sono troppo poche, sono invece troppe, forse giustamente, vista la vastità dell'argomento; chi cerca servizi di qualità fa fatica ad orientarsi (ricordo però il Quaderno Clusit "Certificazioni Professionali in Sicurezza Informatica 2.0", di cui sono co-autore, scaricabile da http://www.clusit.it/download/index.htm).

Avendo commentato sarcasticamente, mi trattengo dal tediare ulteriormente i miei lettori con la solita geremiade sulle competenze già presente in molti miei post precedenti.

PS: ho ricevuto un commento, che condivido, sul blog: "Personalmente il Boom della Sicurezza Informatica e non solo, magari anche un adeguamento alle leggi, lo aspetto... ancora, aggiorniamo norme e decreti ma purtroppo le patch per far "aprire gli occhi" non sono previste. Ritengo che, almeno per la mia esperienza, solo quando è troppo tardi si corra ai ripari".

****

19- AgID cerca personale

AgID cerca personale (scadenza per le candidature il 6 novembre):
- http://www.agid.gov.it/agid/avvisi

La segnalo perché noto un profilo decisamente tecnico delle figure cercate. Mi pare, dai documenti che ho criticato nel tempo, siano anche necessari delle competenze più gestionali (non dirigenziali, ma con competenze per capire gli impatti di alcune misure anche da un punto di vista organizzativo, nelle aziende private che oggi operano nel mercato).

Critico spesso i lavori di AgID, ma credo che molti degli errori siano originati da due cause (ricordo che non so assolutamente nulla dell'organizzazione di AgID): a) il personale con competenze più gestionali è poco numeroso; b) il personale con esperienza reale e capacità (e tempo) di confronto con le aziende private coinvolte è poco numeroso.

****

20- Startup

Si parla molto di startup. Avevo già letto un articolo che diceva che le startup non rappresentano il meccanismo di crescita di un Paese.

Segnalo quindi questo articolo, più recente, che riassume bene la questione:
- http://www.agendadigitale.eu/startup/tante-chiacchiere-sull-innovazione-e-dimentichiamo-cio-che-serve-davvero_1758.htm.