Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – FEBBRAIO 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

****

01- GDPR in italiano

Da Twitter inoltro il link della traduzione in italiano del (futuro e quasi sicuro) Regolamento europeo sulla privacy:
- https://t.co/HmYCBTC7Qy

Mi scuso per il link "corto" ma non riesco a trovare quello completo.

Qualcuno ha fatto notare che nella traduzione si parla di "Responsabile" al posto di "Titolare" e di "Incaricato del trattamento" al posto di "Responsabile del trattamento". Il Data protection officer è poi stato tradotto con "responsabile della protezione dei dati", giusto per creare confusione tra i responsabili (grazie a Pierfrancesco Maistrello di Vecomp per avermi sottolineato questo problema).

In inglese, poi, questi termini sono completamente diversi: "Controller", "Processor" e "Data protection officer". Certo che tradurre "Controllore", "Processore" o "Elaboratore" e "Ufficiale per la protezione dei dati" poteva sembrare ridicolo, ma la soluzione attuale non mi convince lo stesso.

Questo può far riflettere su come comunicano i legislatori nazionali con i traduttori europei. Da notare, comunque, che la traduzione del Regolamento è in linea con quella della Direttiva del 1995 e quindi la confusione tra titolari, responsabili e incaricati tra normativa europea e normativa italiana c'è già da anni.

****

02- Slide su GDPR di EuroPrivacy

EuroPrivacy ha organizzato un evento lo scorso 29 gennaio per discutere del futuro e quasi sicuro Regolamento europeo sulla privacy (General data protection regulation o GDPR). Le slide delle presentazioni sono (quasi) tutte molto interessanti, preparate da persone che hanno seguito con attenzione e professionalità la materia:
- http://www.slideshare.net/EuroprivacyDataProtection.

Segnalo in particolare:
- "Misure di sicurezza e risk management", in cui si trovano preziose indicazioni per la valutazione del rischio;
- "Profilazione versus anonimizzazione", per chi avesse ancora dei dubbi (come me) su alcuni termini e come applicarli;
- "Data protection officer", per chi fosse confuso dai troppi venditori di certificazioni-fuffa nate in questi anni;
- "Data processor nuove responsabilità per i fornitori", in cui si fa il punto sui mitici "responsabili esterni".

****

03- EU-US Privacy Shield

L'UE e gli USA si sono accordati sul nuovo Safe Harbour, rinominato Privacy Shield (notizia e link dal SANS NewsBites):
- http://www.scmagazine.com/privacy-shield-is-here-now-orgs-lawmakers-must-take-action/article/471452/;
- https://www.washingtonpost.com/news/the-switch/wp/2016/02/02/the-massive-new-privacy-deal-between-u-s-and-europe-explained/;
- http://www.darkreading.com/cloud/eu-us-agree-on-new-data-transfer-pact-but-will-it-hold/d/d-id/1324150.

Deve essere ancora approvato dagli Stati membri e quindi non si sa ancora come andrà a finire.

Io continuo a pensare che si dovrebbe puntare a contratti o regole di gruppo suggerite dalla UE e che ho illustrato in altro post (http://blog.cesaregallotti.it/2015/11/guida-della-commissione-europea-per-il.html). È anche vero che i contratti stipulati dai grandi fornitori IT degli USA sono spesso carenti e quindi i loro clienti dovrebbero prestarci più attenzione, a prescindere dall'entrata in vigore del nuovo accordo.

****
04- Novità CAD e eIDAS

Segnalo qualche novità in tema di Codice dell'amministrazione digitale e del Regolamento europeo sulla stessa materia.

Il Consiglio dei ministri ha approvato una bozza di nuovo CAD, ossia le modifiche al Dlgs 82 del 2005:
- http://www.agendadigitale.eu/identita-digitale/nuovo-cad-le-poche-e-confuse-novita-all-orizzonte_1947.htm.

Non sono un estimatore dell'analisi delle bozze, visto che poi sono soggette ad ampi cambiamenti. Ma se qualcuno vuole perderci tempo, faccia pure (se però qualche mio lettore riesce a fare lobby e migliorare il testo, credo lo ringrazieremo in tanti).

Molto più interessante è questo articolo più tecnico su "I primi cinque atti di Esecuzione previsti dal Regolamento eIDAS (UE n. 910/2014)". Si fa il punto di norme fondamentali per chi si occupa della materia:
- https://www.linkedin.com/pulse/eidas-al-decollo-pubblicato-mio-articolo-scritto-con-tumietto.

Segnalo un altro articolo (da tweet di @GAffinito) su alcune lacune e possibili problemi della bozza attualmente disponibile:
- http://www.forumpa.it/pa-digitale/infrastruttura-riforma-del-cad-formati-aperti-e-continuita-operativa-da-rivedere.

****

05- Firmare documenti a mano!

In questi giorni un gestore di carte di credito mi ha chiesto di inviare la documentazione relativa a movimenti fraudolenti via fax. Pensavo di aver raggiunto il colmo della comicità. Poi però una pubblica amministrazione mi ha inviato una convocazione via PEC e mi ha chiesto di confermare... via fax!

Non ne capisco il motivo. Come se nel 2016 il fax (che è una scansione e poi una stampa di un documento su due dispositivi diversi) possa ancora essere l'unico mezzo di comunicazione.

Forse perché sperano che firmiamo a mano i documenti prima di inviarli? Hanno ovviamente torto: chi non ha una scansione della propria firma sul pc? chi non può acquisire una scansione di una firma altrui e copiarla su un documento da mandare via email o fax?

Pensavo che però i pdf fossero particolarmente molesti. E invece, ecco qui un articolo che mi dice di no:
- https://www.achab.it/achab.cfm/it/blog/achablog/come-inserire-la-tua-firma-in-un-file-pdf-gratis-e-in-un-minuto.

Quando la pubblica amministrazione e i privati smetteranno di applicare procedure antiquate (e quindi, oggi, stupide)?

****

06- Legale: Gestore di sito web è responsabile anche per i commenti

Questa notizia è inquietante, se il riassunto dell'Espresso è completo:
- http://scorza.blogautore.espresso.repubblica.it/2016/02/11/diffamazione-online-responsabile-il-gestore-del-sito-anche-per-i-commenti/.

In poche parole, un Onorevole Paniz trova un commento "diffamatore" su un sito web. Lo segnala al suo gestore che era in vacanza e quindi gli risponde che lo cancellerà al suo ritorno, dopo 10 giorni. Cosa che puntualmente ha fatto.

L'Onorevole Paniz, nonostante ciò, lo denuncia e il giudice... gli dà ragione!

Io vado in vacanza senza pc e senza le password del mio blog. Quindi, ve ne prego, continuate a NON commentare i miei blog sul sito; continuate pure a scrivermi via email come avete quasi sempre fatto.

Nota: questa notizia mi è arrivata via Twitter da @meobaldo, "Responsabile stampa del Garante privacy", con il commento "Da leggere". Da buon adulatore l'ho letto e lo sto anche diffondendo :-)

****

07- Legale: legittimità del controllo dell'email aziendale

Notizia da Altalex: il datore di lavoro che controlla l'email aziendale del dipendente non viola la privacy, entro certi limiti:
- http://www.altalex.com/documents/news/2016/01/28/datore-che-controlla-email-aziendale-del-dipendente-viola-la-privacy.

A inizio articolo sono riportate gli accorgimenti seguiti dal datore di lavoro che hanno portato la Corte europea dei diritti umani a decidere della liceità del controllo. Riporto i più importanti:
- informativa;
- monitoraggio delle mail limitato nel tempo e nell'oggetto;
- monitoraggio strettamente proporzionato allo scopo di provare l'inadempimento contrattuale del lavoratore (desunto da altri elementi), la cui scarsa produttività aveva determinato e legittimato il licenziamento;
- non accesso ad altri documenti archiviati sul computer del lavoratore.

Questa sentenza mi sembra da correlare ad un'altra della Cassazione italiana, che aveva reputato eccessivo il licenziamento per gli stessi motivi:
- http://blog.cesaregallotti.it/2014/05/legale-uso-di-pc-e-mail-aziendali-per.html.

Qui forse bisogna distinguere tra legittimità del controllo (che non mi pare sia messo in dubbio neanche dalla sentenza della Cassazione italiana) e delle sanzioni successive, ossia il licenziamento (ritenuto esagerato nel secondo caso e neanche considerato nel primo).

****

08- VERA 4.2.1

Ho ripubblicato il VERA in italiano per correggere qualche errore.

Lo trovate sempre sul mio sito. Però sono stato pigro e non ho rinominato il file che quindi rimane come 4.2 (ho comunque aggiornato l'elenco degli aggiornamenti!):
- pagina web: http://www.cesaregallotti.it/Pubblicazioni.html;
- file: http://www.cesaregallotti.it/Pdf/Pubblicazioni/2015-VERA-4.2-ITA.xlsx.

Ringrazio Vito Losacco, Carlotta Landi, Luigi Fasani e Luciano Quartarone per avermi segnalato alcune correzioni di italiano, di formula e di usabilità.

Luciano, poi, mi ha proposto di aggiornare il VERA con le minacce proposte da ENISA. Non ho accettato questa proposta perché le minacce di ENISA sono 169 (se ho fatto bene il conto) e già i miei clienti si annoiano con le attuali 41. Spero però che Luciano pubblichi la sua proposta.

Ricordo che VERA è nata come una base, non come prodotto finito e buono per tutti. Mi aspetto, ovviamente, che ciascuno lo personalizzi sulla base del contesto in cui opera e la propria esperienza (io stesso lo faccio per ogni progetto!).

****

09- BCI Horizon Scan Report 2016

Segnalo la pubblicazione del "Horizon Scan Report 2016" del Business Continuity Institute:
- http://www.thebci.org/index.php/about/news-room#/pressreleases/cyber-attack-top-business-threat-for-second-year-running-1310591.

Secondo me è stato compilato soprattutto da "informatici", vista l'attenzione elevatissima verso le minacce informatiche (ovviamente, si tratta anche di "mode", visto che il termine usato è "cybersecurity").

A parte questo, rimane una valida lettura.

****
10- Report: ENISA Threat Landscape 2015

Luciano Quartarone mi ha segnalato la pubblicazione dell'ENISA Threat Landscape 2015 (ETL 2015):
- https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl2015.

Confesso che trovo un po' troppo numerose queste pubblicazioni.

Però Luciano fa notare che la tassonomia delle minacce (peraltro disponibile su un documento a parte e disponibile allo stesso indirizzo web) è molto interessante.

****
11- OWASP Incident response

Segnalo, da Tweet di @techn0cratic (che a sua volta si riferisce ad un post su LinkedIn, https://www.linkedin.com/pulse/owasp-incident-response-tactical-guidance-tom-brennan), la pubblicazione di OWASP "Top 10 Considerations For Incident Response":
- https://www.owasp.org/index.php/OWASP_Incident_Response_Project.

Nulla di sensazionale, ma la guida è completa e molto sintetica. E già questi sono pregi.

****
12- Uso dell'utenza di amministrazione aumenta gli incidenti

C'era bisogno di un rapporto di Avecto per sapere che, per ridurre di parecchio gli incidenti, i pc dovrebbero essere usati da "utenti base" e non come "utenti amministratori":
- http://www.zdnet.com/article/most-windows-flaws-mitigated-by-removing-admin-rights-says-report/.

Non so chi sia Avecto, ma la notizia è stata diffusa dal SANS NewsBites e tanto basta. Il SANS ricorda che una simile affermazione fu fatta nel 2009, dicendo che se i pc Windows fossero usati come "utenti base", il 92% delle vulnerabilità sarebbe mitigata:
- http://www.zdnet.com/article/report-92-of-critical-microsoft-vulnerabilities-mitigated-by-least-privilege-accounts/.

E ancora sono guardato come un pazzo idealista quando segnalo come estremamente pericolosa la pratica di usare il pc come amministratore. Per la cronaca, io uso da sempre il pc come "utente base" e

non ho mai avuto problemi (ho anche imposto ai miei genitori di usare Windows 7 o successivi proprio perché permettono di impostare utenze base; da allora le chiamate di aiuto si sono ridotte quasi a zero).

Continuo a pensarlo: non sono pazzo io, sono pazzi (e incompetenti) quegli altri.

****

13- Mettere in sicurezza le utenze privilegiate

Da un retweet di @pstirparo, segnalo questo articolo di Microsoft "Securing Privileged Access":
- https://technet.microsoft.com/en-us/library/mt631194.aspx.

È molto tecnico, ma non troppo. È un po' complicato da leggere perché richiede spesso di passare da una pagina web ad un'altra. Per i lettori di libri come me è un po' faticoso.

Però ne vale la pena, è pragmatico e andrebbe letto da tutti quanti si occupano di sicurezza informatica. Spero che si diffonda e diventi un punto di riferimento per gli amministratori di sistema.

Notate, per esempio, che smitizza alcune pratiche seguite dai sistemisti (per esempio, usare macchine virtuali).

Almeno leggete lo "stage 1". Penso sia più che sufficiente per cominciare a lavorarci.

****

14- Vulnerabilità dell'IoT

Sono tanti gli articoli che parlano di (in)sicurezza dell'Internet of Things o IoT. Questo in italiano, breve e non molto tecnico mi sembra tra i migliori (da un Tweet di @alexgiovannini):
- http://www.wired.it/gadget/computer/2016/01/29/facile-hackerare-le-videocamere-di-sicurezza/.

****

15- Le 25 peggiori password del 2015

SplashData ha pubblicato l'aggiornamento dell'elenco delle peggiori password:
- https://www.teamsid.com/worst-passwords-2015/.

Pensavo fosse un esercizio inutile, poi Francesca Lazzaroni di Spike Reply mi ha fatto notare che è molto utile quando si fanno sessioni di formazione presso le aziende.

Si può anche leggere l'articolo del The Guardian (segnalato da un tweet di @leliosimi):
- http://www.theguardian.com/technology/2016/jan/20/123456-worst-passwords-revealed.

****

16- Agenzie web e fornitori vulnerabili

Era da tanto che volevo segnalare questo articolo dal titolo "Le web agency sono il nuovo cavallo di troia?":
- https://codiceinsicuro.it/blog/le-web-agency-sono-il-nuovo-cavallo-di-troia.

L'autore segnala vulnerabilità relative a fornitori particolari, ossia le web agency; le aziende si preoccupano quasi soltanto dei fornitori cloud; forse dovrebbero pensare anche agli altri (questa è una mia battaglia da lungo tempo).

Dissento dalla conclusione dell'articolo (bisogna formare e sensibilizzare gli sviluppatori) perché credo che il problema siano i manager: se decidono di esternalizzare un servizio, gli sviluppatori non possono farci niente. Se il manager o il cliente dice loro di essere veloci e costare poco, non possono miracolosamente assicurare un buon livello di qualità e sicurezza.

Noi dobbiamo parlare di ITIL, ISO e processi ai clienti, affinché non pensino solo alla sicurezza dei sistemi informatici che gestiscono direttamente, ma anche a quelli gestiti dai fornitori.

Quanti mi dicono, facendo spallucce, che "è responsabilità del fornitore"? Però non dicono la stessa cosa di un'automobile: vogliono che il fornitore ne garantisca la sicurezza!

Dobbiamo parlare ai manager di queste cose affinché capiscano che possono spendere un po' meno in consulenti che scrivono procedure perfette e possono spendere un po' di più per controllare i fornitori a avere garanzie sulla qualità del servizio.

****

17- Assicurazioni informatiche

Un amico (anonimizzo) mi ha segnalato il suo interesse per le assicurazioni informatiche. Finalmente ha "scoperto" una polizza, le cui caratteristiche sono presentate qui:
- http://www.padovasud.generali.it/71654/Presentazioen-Polizza-Informatica.pdf.

Non è mia intenzione scrivere un trattato in merito, ma mi piacerebbe tanto che qualcuno lo facesse, riportando esempi pratici e facendo gli opportuni confronti.

****

18- I primi 100 giorni del responsabile della sicurezza delle informazioni

Pierfrancesco Maistrello di Vecomp mi ha ricordato la pubblicazione del Clusit dal titolo "I primi 100 giorni del responsabile della sicurezza delle informazioni":
- http://100giorni.clusit.it.

Confesso che l'avevo bellamente sottovalutato quando, come socio Clusit, ne ricevetti notizia qualche mese fa. Però Pierfrancesco mi ha detto che lo consiglia soprattutto a responsabili IT di piccole e medi imprese che iniziano ad occuparsi di sicurezza e privacy e riceve sempre ringraziamenti.

Ecco quindi un'occasione per proporlo anche qui, seppure con ritardo.

****

19- Sicurezza e deviazioni

Bruce Schneier, nel suo Crypto-Gram di gennaio, riporta un articolo dal titolo "IT Security and the Normalization of Deviance":
- https://www.schneier.com/blog/archives/2016/01/it_security_and.html.

Si parla di "normalizzazione della devianza", ossia delle persone che si abituano così tanto ai comportamenti devianti da non considerarli più tali.

Ho già parlato in altre occasioni di questo aspetto della sicurezza, spesso dandone la colpa ai capi (se loro sono i primi a chiedere o operare eccezioni alle regole o ignorano gli avvisi di auditor o altre entità).

L'altra faccia della medaglia dovrebbe essere presa in considerazione: persone che seguono (o chiedono di seguire) regole e procedure senza chiedersene il senso. Alcune volte si tratta di regole necessarie in passato, quando la tecnologia o l'organizzazione erano diverse (pensate a quanti chiedono ancora di firmare a mano dei moduli, quando un'email potrebbe essere sufficiente), o tentativi di risolvere delle situazioni oggi non più verosimili.

Schneier raccomanda ulteriori articoli (alcuni non relativi la sicurezza delle informazioni, ma comunque pertinenti l'argomento). Tra questi segnalo il seguente di John Banja dal titolo "The normalization of deviance in healthcare delivery":
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2821100/.

Al paragrafo 4.3 sono fornite alcune indicazioni su come intervenire (ma nessun link è "facilmente" utilizzabile).

****

20- Carrai e la Sicurezza Cibernetica Nazionale

Io non ho mai voluto parlare di politica nei miei "luoghi" professionali (blog, newsletter, Twitter), ma questa notizia è veramente troppo diffusa per ignorarla.

Il Presidente del Consiglio Matteo Renzi prevede di nominare tal Marco Carrai come responsabile del "centro nazionale della sicurezza cibernetica". Sembra che Carrai non abbia quasi alcuna competenza in materia. Ecco alcuni articoli (tutti ben polemici; scusate ma è quello che gira in rete):
- http://www.lettera43.it/politica/renzi-la-nomina-di-carrai-ai-servizi-rischia-lo-stop_43675230574.htm;
- https://codiceinsicuro.it/blog/tra-conflitti-di-interesse-e-007-addio-meritocrazia/;
- http://limbeccata.it/la-polemica/10-mesi-di-lavoro-e-0-laurea-carrai-li-non-andrai/.

Io ho già qualche problema perché non riesco a capire cosa sia la "sicurezza cibernetica", visto che la "cibernetica" è la "Disciplina che si occupa dello studio unitario dei processi riguardanti la comunicazione e il controllo nell'animale e nella macchina" (www.treccani.it).

Per la verità, come ho scritto in precedenza, non sopporto neanche il termine "cybersecurity", a prescindere dalla sua etimologia, perché viene usato in ogni contesto senza specificare cosa intende, quali sono i suoi confini e cosa la differenzia dalla "sicurezza informatica".

A parte i miei problemi terminologici, la nomina di Carrai è molto criticata, tanto che è stata scritta una "Lettera aperta al Presidente del Consiglio dei Ministri, Matteo Renzi, sulla "Sicurezza Cibernetica Nazionale"" e tutti gli "esperti del settore" sono stati invitati a sottoscriverla:
- https://www.cybersecuritynazionale.org/.

Cercando di non fare il finto modesto, mi sono sentito in causa e mi sono chiesto se firmarla.

Da una parte è opportuno prestare attenzione ai responsabili con elevate competenze tecniche. Ne ho avuti e ho visto che fungono da collo di bottiglia su tutti i temi di cui sono competenti.

Inoltre, i manager con competenze tecniche riducono tutto alla propria area di competenza (il sistemista IT ignora i problemi delle applicazioni e viceversa, l'esperto in organizzazione ignora i problemi tecnologici e viceversa, i non legali ignorano gli impatti normativi sulle proprie attività, e così via). In una realtà complessa come la sicurezza di Internet (forse è questo che si intende con "sicurezza cibernetica"?) questo può essere un limite.

Osservate, per esempio, i problemi del Garante privacy. Se pure tra il suo personale si trovano dei tecnici molto preparati, alcuni (non tutti...) Provvedimenti contengono sciocchezze tecnologiche inaudite. Segno che da Rodotà in poi i tecnici sono considerati vil razza dannata. E certamente il curriculum di Rodotà non lascia dubbi sulle sue elevate competenze giuridiche.

Dall'altra parte ho pensato che un manager deve essere soprattutto bravo a scegliere e gestire i collaboratori. Questa sarebbe la posizione di Renzi (mi dicono l'abbia esposta in qualche trasmissione televisiva). Però, mi chiedo, se una persona non ha un minimo di competenze, come può scegliere e coordinare correttamente le persone? Ho avuto capi non competenti della materia e ho visto i problemi che hanno causato.

Tra l'altro, ho sempre pensato, e ne ho visto le prove, quanto sia sciocca l'affermazione che un "manager è un bravo manager in qualunque settore lavori". Ritengo sia una baggianata messa in giro dagli stessi manager incompetenti e, purtroppo, presa per buona anche dalle persone competenti.

Qualche manager incompetente può sembrare bravo se, prima di lui, sono stati scelti e coordinati dei bravi tecnici, che possono lavorare bene anche senza i suoi interventi (preferisco non fare esempi...).

Ecco perché alla fine ho deciso di firmare la lettera.

Tra l'altro, spero che Carrai, visto che pare abbia conoscenze nel settore, abbia il buon gusto di rinunciare alla nomina e indicare persone più adatte di lui, con le giuste competenze e incompetenze, al ruolo di responsabile del "centro nazionale della sicurezza cibernetica".

****

21- Tecnologie digitali, tecnostress e pausa digitale

Franco Ferrari di DNV GL mi ha segnalato questo articolo di Gianni Alioti dal titolo "Tecnostress: il punto di vista del sindacato":
- http://www.rs-ergonomia.com/app/download/12132082896/Gianni Alioti.pdf.

Il documento è interessante perché tratta brevemente del problema della capacità di concentrazione e della produttività individuale.

Ovviamente è necessario leggerlo senza pensare che rappresenti "il punto di vista del sindacato", ma uno studio facilmente estendibile ad altri punti di vista.

_____

Cesare Gallotti
Ripa Ticinese 75
20143 Milano (Italia)
Tel: +39.02.58.10.04.21
Mobile: +39.349.669.77.23
Web: http://www.cesaregallotti.it
Blog: http://blog.cesaregallotti.it
Twitter: @cesaregallotti
Mail: cesaregallotti@cesaregallotti.it
PEC: cesaregallotti@mailcert.it