Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – FEBBRAIO 2019
****

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.

La newsletter è inviata via MailUp, offerta da Team Quality S.r.l.

Per iscriversi, cancellarsi e leggere l'informativa privacy: http://www.cesaregallotti.it/Newsletter.html.

Sulla stessa pagina è possibile consultare l'informativa sul trattamento dei dati personali.

****
Indice

****
00a- Miei libri "Sicurezza delle informazioni" e "Information security" edizione 2019

Ho pubblicato da poco la versione del 2019 del mio libro "Sicurezza delle informazioni". Infatti ho voluto tradurlo in inglese e, nel farlo, ho corretto alcuni errorini e aggiornato alcune cose. Niente di fondamentale, insomma (la cosa più importante è che ho accreditato in copertina l'aiuto che avevo ricevuto nel 2014 da Massimo Cottafavi e Stefano Ramacciotti; il mio ritardo è inqualificabile e me ne scuso).

E' disponibile in cartaceo e in digitale (epub, mobi, kindle e anche pdf). E' pubblicato in self-publishing presso:
- Streetlib per il formato digitale (https://store.streetlib.com);
- Lulu per il formato cartaceo (http://www.lulu.com/shop).

Alcuni appunti:
- prestate attenzione all'edizione; siamo ancora in fase di transizione dalla vecchia del 2017 alla nuova e alcuni negozi virtuali le vendono tutte e due; guardate quindi con attenzione le copertine e anche la

descrizione dell'articolo (dice esplicitamente che si tratta della versione aggiornata nel 2019);
- su Streetlib, per motivi a me ignoti, non è ancora disponibile la versione in italiano (con anche il pdf); in questi giorni cercherò di ovviare al problema;
- su Lulu, c'è un'edizione cartacea più economica; per motivi a me ignoti, è possibile creare una versione più economica (avendo gli stessi guadagni) vendibile solo su Lulu e così ho fatto;
- Lulu in questo momento è molto lenta nell'inviare la versione in italiano (ho avuto conferma della spedizione il 31 gennaio ma non mi è ancora arrivato il 18 febbraio).

Appena avrò i link di tutte le versioni, aggiornerò questa notizia.

Intanto ringrazio quanti hanno comprato o compreranno il libro.

****

00b- Milano, 10 aprile 2019: DFA Open day 2019

Il 10 aprile pomeriggio si terrà a Milano l'annuale DFA Open day (gratuito). Per iscriversi:
- https://www.eventbrite.it/e/biglietti-dfa-open-day-2019-56637583537.

Il programma non lo abbiamo ancora stabilito completamente, ma parleremo di digital forensics (lato tecnologico e lato legale), di GDPR e chissà che altro.

Per la cronaca, sono presidente dell'associazione.

****

01- ENISA e misure di sicurezza per le app per smartphone

ENISA pubblicò a inizio 2017 un documento dal titolo "Smartphone Secure Development Guidelines". Lo segnalo, con colpevole ritardo:
- https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016.

Ora ha reso in formato xls le misure di sicurezza e, forse un po' troppo pomposamente, lo ha denominato SMASHING Tool. Al di là della mia ironia sull'eccesso di enfasi, penso che l'iniziativa sia più che apprezzabile:
- https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smartphone-guidelines-tool.

****

02- ENISA e sicurezza per IoT

ENISA (l'agenzia europea per la sicurezza informatica) ha pubblicato negli anni alcuni documenti e raccomandazioni per l'IoT.

In una pagina web è possibile accedere alle raccomandazioni per gli ambiti finora trattati (città, automobili, industria, aeroporti, ospedali). Queste raccomandazioni possono anche essere scaricate in formato Excel.

La pagina "ENISA Good practices for IoT and Smart Infrastructures Tool":
- https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool

****

03- Mio articolo - Differenza tra sicurezza IT e OT

Ho scritto questo breve articolo dal titolo "Differenza tra sicurezza IT e OT":
- https://www.ictsecuritymagazine.com/articoli/differenza-tra-sicurezza-it-e-ot/.

****

04- ENISA e materiale di formazione tecnica

Ho notato la recente pubblicazione di ENISA del materiale di formazione tecnica "Introduction to network forensics".

Andando a vedere di cosa si tratta, ho visto che il materiale è pubblicato insieme a tante altre cose in una pagina "Online training material":
- https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational.

Mi sembra tutto molto interessante e pertanto lo segnalo.

****

05- ENISA Threat Landscape 2018 report

Tempo di report (solitamente non molto utili, ma molto apprezzati) sulla sicurezza. Ecco il primo del 2019: "ENISA Threat Landscape 2018 report":
- https://www.enisa.europa.eu/news/enisa-news/exposure-to-cyber-attacks-in-the-eu-remains-high/.

Questo rapporto ha il pregio di elencare 15 minacce ritenute particolarmente significative (dal malware allo spionaggio) e di collegarle a misure di mitigazione.

La mia perplessità è che sembra (anche se è faticoso capirlo dal documento) che queste 15 minacce sono state selezionate non sulla base di dati, ma sulla base delle percezioni degli esperti di ENISA. Tutto ragionevole, ma da sapere.

****

06- Il business della sicurezza (nelle scuola USA)

Segnalo questo articolo del Corriere della sera dal titolo "Usa, il business sicurezza nelle scuole":
- https://www.corriere.it/editoriali/19_febbraio_07/usa-business-sicurezza-scuole-667de962-2afb-11e9-8bb3-2eff97dced46.shtml.

Mi occupo di sicurezza delle informazioni e, con le dovute cautele, alcuni parallelismi li possiamo fare. In particolare ho riflettuto sull'unione di due direzioni contrapposte: da una parte quella della sfiducia completa nei confronti del prossimo, per cui è necessario armarsi di armi reali o di forme di controllo sempre più sofisticate, dall'altra quella della fiducia totale nei confronti dei venditori delle tecnologie che hanno già dimostrato di potersene approfittare (vedere caso di Cambridge Analytica).

E da questa storia si nota anche la tendenza a rifugiarsi, per la sicurezza, in tecnologie sempre più sofisticate, complesse da mantenere e che lasciano sempre più spazio di manovra ai fornitori. Un tempo era caratteristica degli informatici rispondere, ad ogni problema di sicurezza informatica, "ho un tool"; oggi sembra la risposta comune. Invece spesso basterebbe risparmiare su qualche gadget o consulente e investire di più negli stipendi del personale che c'è già, nella sua formazione e nella sua crescita numerica.

Penso che in molti casi costerebbero di meno (anche se, ahinoi, nelle spese fisse), e avrebbero maggiori benefici, due persone in più, con la riduzione dello stress in quelli che ci sono già e quindi degli errori, al posto del continuo ricorso a super-fornitori, super-consulenti e super-tecnologie.

Dico questo con l'esperienza di chi ha visto aziende con tanti tecnici sovraccarichi di lavoro e che investono in tecnologie spesso inutili (qualcuno si ricorda i DLP? oggi sono, a ragione, quasi dimenticati) e in consulenze altrettanto inutili (per esempio su fantistici modelli organizzativi che non vedono mai la luce, nonostante gli enormi costi sostenuti per farsi dire che è necessaria un'organizzazione "matriciale" (perché è così che finisce nella maggior parte dei casi; mi si scusi lo spoiler)).

****

07- Assicurazioni IT - 2 articoli

Roberto Gallotti (mio papà!) mi ha segnalato un articolo del The Economist dal titolo "The market for cyber-insurance is growing":
- https://www.economist.com/finance-and-economics/2019/01/26/the-market-for-cyber-insurance-is-growing.

La sostanza è che il mercato delle assicurazioni IT (o cyber-insurance) è ancora immaturo.

Ne avevo scritto già prima del 2011, poi nel 2011 e poi, grazie ad uno studio di ENISA, nel 2012 (http://blog.cesaregallotti.it/2012/08/assicurazioni-e-sicurezza-informatica.html). Nulla è cambiato, neanche quelli che, senza aver studiato l'argomento, continuano a promuovere assicurazioni ancora inadeguate.

Un altro articolo, segnalatomi da Pierfrancesco Maistrello, è molto simile e ha titolo "Data breach insurance: A three-part problem":
- https://iapp.org/news/a/data-breach-insurance-a-three-part-problem/.

Questo secondo articolo prende le mosse da una sentenza (credo di un tribunale inglese) che ha imposto ad un'azienda di sottoscrivere un'assicurazione per le multe derivanti dal GDPR. Il fatto è che la questione non è banale per vari motivi: è in dubbio la possibilità di prevedere assicurazioni per inadempimenti legali, sono carenti le statistiche sugli incidenti, è incerta la definizione di "cyber risk", l'assicuratore può non pagare anche per minime carenze dell'assicurato nel seguire le procedure.

L'articolo parla, incidentalmente, anche delle assicurazioni da DPO dicendo che non sono sostanzialmente disponibili.

Due riflessioni:
- la cosa sull'impossibilità di assicurarsi per inadempimenti legali mi è nuova e spero di trovare ulteriori articoli in merito per approfondire la questione (pare purtroppo che gli esperti legali italiani trovino più gusto a ripetere il concetto di accountability);
- le altre cose le so da tempo, eppure troppi "esperti" continuano a proporle e mi chiedo come mai; non si aggiornano o non approfondiscono le cose di cui parlano? si aggiornano facendo affidamento a "esperti" che non sono esperti ma solo imbonitori? sono essi stessi imbonitori senza vera competenza?

****

08- ITIL 4 in uscita

In questi mesi (primo trimestre 2019) è prevista l'uscita di ITIL 4. Sicuramente è frutto di varie riflessioni (incluso il nome, dato che nel 2011 avevano decretato che le future versioni di ITIL non avrebbero più avuto una "versione" e invece oggi si parla di ITIL 4).

Per prepararsi (anche per capire come mantenere le certificazioni personali), segnalo questo articolo dal titolo "ITIL 4: aria di rinnovamento" che, mi pare, dica tutto (segnalo che Deborah Monaco è anche mia amica, ma lei non mi ha segnalato il suo articolo e per questo le ho già fatto le mie rimostranze):
- https://www.zerounoweb.it/cio-innovation/organizzazione/itil-4-aria-di-rinnovamento/.

La pagina ufficiale sull'aggiornamento di ITIL è quella del sito di Axelos:
- https://www.axelos.com/itil-update.

****

09- Manutenzione impianti elettrici

La sicurezza degli impianti elettrici è un elemento, non principale e spesso dimenticato, della sicurezza informatica. Per questo, ricordando che le competenze in materia di sicurezza dei lavoratori e di sicurezza delle informazioni sono diverse, è bene saperne qualcosa.

Franco Vincenzo Ferrari di DNV GL mi ha segnalato questo articolo di PuntoSicuro dal titolo "Linee guida per la verifica e il controllo degli impianti elettrici":
- https://www.puntosicuro.it/sicurezza-sul-lavoro-C-1/tipologie-di-contenuto-C-6/linee-guida-buone-prassi-C-62/linee-guida-per-la-verifica-il-controllo-degli-impianti-elettrici-AR-18793/.

L'articolo riassume i punti salienti di una linea guida del CNPI sulla sicurezza degli impianti elettrici. La pagina del CNPI è la seguente:
- http://www.cnpi.eu/dal-cnpi-la-linea-guida-sulla-sicurezza-degli-impianti-elettrici/.

Nel 2008 avevo copiato un articolo di Filodiritto (www.filodiritto.it) che, ahimé, non riesco più a trovare. Segue quindi quanto avevo copiato (e forse sintetizzato... non ricordo). Segnalo che la linea guida del CNPI non cita il DPR 392 del 1994, che sembra comunque in vigore.

Il Decreto Ministeriale n. 37 del 22 gennaio 2008 è stato emanato al fine di riordinare tutte le disposizioni in tema di attività di installazione e di sicurezza degli impianti all'interno di edifici di diversa tipologia. Il riordino delle disposizioni vigenti in materia ha comportato l'abrogazione delle norme contenute:
- nella Legge n. 46 del 5 marzo 1990 "Norme sulla sicurezza degli impianti" (ad eccezione degli articoli 8, 14, 16 sulle sanzioni applicabili);
- nel Decreto del Presidente della Repubblica n. 447 del 6 dicembre 1991 "Regolamento di attuazione della legge 46/1990 in materia di sicurezza degli impianti";
- nel Capo V parte II artt. dal 107 al 121 "Norme per la sicurezza degli impianti" del Testo Unico in materia edilizia di cui al Decreto del Presidente della Repubblica n. 380 del 6 giugno 2001.

Pertanto, a partire dal 27 marzo 2008 (data di entrata in vigore del Decreto Ministeriale n. 37/2008), tutta la materia dell'installazione e della sicurezza degli impianti è disciplinata:
- dal citato decreto 37/2008;
- dagli articoli 8, 14 e 16 della legge n. 46/1990;
- dal Decreto del Presidente della Repubblica n. 392 del 18 aprile 1994 "Regolamento per la disciplina del procedimento di riconoscimento delle imprese ai fini dell'installazione, ampliamento e trasformazione degli impianti nel rispetto delle norme di sicurezza".

Per la manutenzione degli impianti di ascensori e montacarichi in servizio privato continuano, invece, ad applicarsi le disposizioni del Decreto del Presidente della Repubblica n. 162 del 30 aprile 1999 e le altre disposizioni specifiche in materia.

****

10- Standard - Pubblicata la nuova ISO/IEC 27008

E' stata pubblicata a gennaio 2019 la nuova versione della ISO/IEC 27008 dal titolo "Guidelines for the assessment of information security controls":
- https://www.iso.org/standard/67397.html.

La precedente versione era la ISO/IEC 27008:2011. Questa è stata indicata come "revisione maggiore", anche perché ora si basa sui controlli della ISO/IEC 27002:2013.

Questo standard non mi piace perché in alcuni punti coglie l'occasione per "migliorare" la ISO/IEC 27002, creando quindi confusione.

****

11- Standard - Pubblicata la nuova ISO/IEC 27018

E' stata pubblicata a gennaio 2019 la nuova versione della ISO/IEC 27018 dal titolo "Code of practice for PII protection in public clouds acting as PII processors":
- https://www.iso.org/standard/76559.html.

La precedente versione era la ISO/IEC 27018:2014 e questa nuova versione è indicata come "revisione minore" e sembra dovuta al solo fatto che ci fossero dei riferimenti incrociati sbagliati (questo è quello che ho trovato scritto nella "giustificazione per la revisione"; mi limito a dire, per evitare denunce, che questa nuova edizione si poteva evitare).

Ricordo che questa norma riporta controlli privacy che possono essere usati per estendere quelli di sicurezza della ISO/IEC 27001 e ottenere una certificazione rispetto alla ISO/IEC 27001 "estesa" con la ISO/IEC 27018. È applicabile ai fornitori di servizi cloud pubblici, che agiscono con ruolo di responsabili (e non titolari!).

****

12- Legale - Cassazione: licenziamento lecito per troppo uso di Facebook

L'articolo ha titolo "Facebook per troppe ore al lavoro, la Cassazione ribadisce il licenziamento":
-
https://www.repubblica.it/cronaca/2019/02/01/news/facebook_per_troppe_ore_la_cassazione_ribadisce_il_licenziamento-218017328

Notare che i giudici hanno stabilito che non c'è stata nessuna violazione delle regole sulla tutela della privacy. Spero qualcuno possa segnalare qualche articolo di maggiore riflessione in merito a questa sentenza.

****

13- Legale - Cassazione: accesso a Facebook con le credenziali della moglie

Luca De Grazia mi ha segnalato, con il titolo "Condannato per essere entrato nel profilo Facebook della moglie e aver fotografato una chat", una sentenza della Cassazione.

Il commento sintetico mi pare dica tutto: "Evidente, secondo i Giudici, l'interferenza compiuta dal marito ai danni della vita privata della consorte. Irrilevante il fatto che le credenziali di accesso fossero state fornite tempo addietro dalla donna al marito".

Segnalo questo articolo (il primo che ho trovato):
- http://www.studiolegalezuco.it/accesso-abusivo-sistema-informatico-615-ter-profilo-facebook-conoscenza-credenziali-cassazione-penale-2905-2019/.

Mi pare interessante, anche perché ritorna sul caso in cui una persona condivide le proprie password con un'altra. Anche questo caso ci insegna che è sempre una cattiva idea.

****

14- Legale - Dipendente che usa registrazioni per scopi difensivi

Un cliente mi ha fatto una domanda per cui sono dovuto andare a ricercare questa notizia di Filodiritto dal titolo "Cassazione Civile: è illegittimo il licenziamento del dipendente che utilizza le registrazioni fonografiche occulte per scopi difensivi":
- https://www.filodiritto.com/news/2018/licenziamento-cassazione-civile-illegittimo-il-licenziamento-del-dipendente-che-utilizza-le-registrazioni-fonografiche.html.

Penso che possa di essere interesse anche per i miei lettori.

Mi ha stupito il fatto che la sentenza faccia riferimento al GDPR. Infatti mi sembrava dovesse essere escluso in quanto non "trattamento interamente o parzialmente automatizzato di dati personali" o "di trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi" e, anzi, "attività a carattere esclusivamente personale". Sicuramente ha ragione la Cassazione.

****

15- Privacy - Titolare e responsabile secondo il Garante (e i consulenti del lavoro)

Quest'estate era divampato il dibattito dal titolo "il consulente del lavoro è titolare o responsabile dei trattamenti svolti per i propri clienti?". Ne avevo scritto:
- http://blog.cesaregallotti.it/2018/07/circolare-dei-consulenti-del-lavoro.html.

Il Garante si è finalmente espresso su questo punto, dicendo (in accordo con tutti gli "esperti privacy" che io ritengo veramente tali e non con tanti altri cialtroni) che il consulente del lavoro ha il ruolo di responsabile quando tratta i dati per conto dei propri clienti:
- https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9080970.

Da notare che la risposta del Garante fornisce altri esempi di responsabili: il soggetto che fornisce servizi di localizzazione geografica, i servizi di posta elettronica, i servizi di televigilanza.

Aggiunge anche "la società capogruppo delegata da società controllate e collegate a svolgere

adempimenti in materia di lavoro, previdenza ed assistenza sociale per i lavoratori", ma su questo ho i miei dubbi, visto che la capogruppo è solitamente non delegata "volontariamente" dalle controllate.

****

16- Privacy - Google multata in Francia per 50 milioni per mancato rispetto del GDPR

Una prima multa milionaria per il mancato rispetto del GDPR. In questo caso, il Garante francese ha multato Google perché Android non presenta chiaramente i consensi necessari per il trattamento dei dati.

Un articolo in italiano dal titolo "Consenso alla privacy poco chiaro, in Francia multa da 50 milioni di euro per Google":
- https://www.lastampa.it/2019/01/21/tecnologia/consenso-alla-privacy-poco-chiaro-in-francia-multa-da-milioni-di-euro-per-google-aDmrdULxnqJU2oMdLJeBsI/pagina.html.

Un articolo in inglese dal titolo "GDPR: Google hit with €50 million fine by French data protection watchdog":
- https://www.zdnet.com/article/gdpr-google-hit-with-eur50-million-fine-by-french-data-protection-watchdog/.

****

17- Privacy - Ampliamento Registro delle opposizioni

Luca de Grazia mi ha segnalato l'entrata in vigore del DPR 149 del 2018 che estende il Registro delle opposizioni alla posta cartacea. Il registro era già stato esteso, con la Legge 5 del 2018, ai numeri di cellulari.

Il DPR che istituisce il Registro delle opposizioni è il 178 del 2010 e su Normattiva si trova la sua versione aggiornata. Similmente, si trova la Legge 5 del 2018.

L'indirizzo web di Normattiva è:
- www.normattiva.it.

Il Registro delle opposizioni è il servizio concepito a tutela del cittadino, il cui numero è presente negli elenchi telefonici pubblici, che decide di non voler più ricevere telefonate per scopi commerciali o di ricerche di mercato. Il suo indirizzo web è:
- http://www.registrodelleopposizioni.it/.