Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – MARZO 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

****

16 marzo: sarò al Security summit

Mercoledì 16 marzo alle 16.30 terrò un intervento al Security summit di Milano su "Norme tecniche nazionali e internazionali sulla sicurezza delle informazioni: ultime novità":
- https://www.securitysummit.it/milano-2016/seminari-associazioni/talk-244/.

****

01- Fornitori e ruoli privacy

Tempo addietro mi ero lamentato di come la normativa privacy attuale (non) tratta compiutamente le filiere di fornitura (il post iniziale, a cui ne sono seguiti altri 3, è il seguente:
- http://blog.cesaregallotti.it/2011/04/privacy-dei-titolari-e-dei-responsabili.html).

In sostanza, un titolare (controller) può scegliere un responsabile (processor), ma un responsabile (processor) non può scegliere un sub-responsabile (sub-processor) per gli stessi trattamenti.

In molti casi si vedono dei responsabili che nominano i propri fornitori come... responsabili, anche se solo il titolare può nominare i responsabili.

Questi casi, purtroppo, non sono stati discussi compiutamente in questi 20 anni di normativa privacy, nonostante le filiere di fornitura diventino sempre più lunghe a causa del principio di specializzazione. In Italia, senza pensarci troppo, si nominano i fornitori come "responsabili esterni", nonostante questo sia discutibile.

L'ultima bozza d dicembre del Regolamento europeo sulla privacy sembra considerare il problema e permette ai responsabili di "coinvolgere altri responsabili", purché ne informino il titolare.

Però anche questa soluzione non è ottimale, né è adeguata ai nostri tempi. Si pensi ad una PMI che usa dei servizi di un grande operatore di telecomunicazioni o di servizi cloud: deve essere aggiornata su ogni cambiamento operato dal grande operatore? il grande operatore deve informare tutti i suoi clienti?

Pensiamo ad una normale catena di fornitura: un'azienda ha un fornitore per i servizi di predisposizione buste paga, il quale ha un fornitore per il servizio applicativo con cui predisporre le buste paga, il quale ha un fornitore di hosting, il quale ha un fornitore di manutenzione (per non parlare poi di consulenti, legali, auditor e altri coinvolti nelle attività).

Ma pensiamoci bene. Un operatore di telecomunicazioni non è un titolare? È lui quello che "determina le finalità e i mezzi per elaborare i dati personali". Un suo cliente compra quei servizi e, nella migliore delle ipotesi, dovrebbe chiedere dettagli su tali finalità e mezzi, valutare se sono allineate con le proprie finalità e misure di sicurezza, decidere se continuare ad averlo come fornitore. Il viceversa (ogni cliente chiede ai propri fornitori di seguire le proprie regole) è inapplicabile quando i numeri diventano grandi, ossia quando un fornitore ha tanti clienti e non può modificare i propri processi e meccanismi di sicurezza per ogni singolo cliente.

La bozza di Regolamento introduce le "terze parti", ma non è chiaro come interpretarle.

Speriamo questo argomento sia discusso con maggiore attenzione nel prossimo futuro.

****

02- Privacy: Check list amministratori di sistema

Luciano Quartarone (che ringrazio per la seconda volta) mi ha segnalato un'altra sua pubblicazione: una checklist per i controlli sugli Amministratori di sistema previsti dal Provvedimento del Garante privacy:
- http://www.lucianoquartarone.it/wp/?p=687.

Sono contento che abbia ripreso e migliorato il mio lavoro di qualche anno fa. Mi dimostra che si può fare sempre di meglio. E io da domani userò la sua check list.

Luciano teme che la normativa sugli Amministratori di sistema abbia "i giorni contati". Io non ne sono così convinto perché dovremo vedere gli impatti del Regolamento europeo privacy (se e quando sarà approvato) sulla normativa secondaria fin qui prodotta dal Garante. Se qualcuno ha già delle idee, lo/la prego di condividerle.

****

03- Privacy: Scheda informativa del Garante sul Regolamento EU

Il Garante privacy ha tradotto il manifesto dell'Art. 29 WP sul futuro (forse!) Regolamento EU privacy (GDPR). Lo si trova a questo link, sotto "Altri documenti":
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4443361.

Non so quanto sia chiaro per i profani, ma le illustrazioni mi piacciono.

****

04- Privacy: Un articolo di presentazione del forse futuro GDPR

Da un suggerimento di Franco Ferrari di DNV GL, segnalo questo articolo dal titolo "Sul regolamento europeo per la protezione dei dati":
- http://www.puntosicuro.it/security-C-124/privacy-C-89/sul-regolamento-europeo-per-la-protezione-dei-dati-AR-15630/.

Rispetto ad altre cose che ho letto (spesso elenchi puntati o approfondimenti di singoli punti), questo articolo affronta tutti i punti della bozza di regolamento fornendo degli spunti di lettura.

PS: successivamente a questo articolo, lo stesso autore (Adalberto Biasotti) ne ha pubblicato un altro dedicato alla Direttiva relativa al trattamento dei dati in ambito giudiziario che affiancherà il Regolamento:
- http://www.puntosicuro.it/security-C-124/privacy-C-89/il-trattamento-di-dati-per-finalita-investigative-giudiziarie-AR-15745/.

****

05- Privacy shield: testo finale ma ancora non approvato

Stanno girando molte notizie sull'approvazione del Privacy shield, ossia dell'accordo EU-USA per il trasferimento di dati personali che dovrebbe sostituire l'abrogato Safe harbour.

L'ultima notizia riguarda l'accordo sul testo, che però deve essere ancora approvato, come riportato dal comunicato stampa del 29 febbraio (segnalo il testo in inglese, perché quello in italiano è ottenuto tramite traduzione automatica):
- http://europa.eu/rapid/press-release_IP-16-433_en.htm.

****

06- eIDAS: domande e risposte

Da un tweet di @andreacaccia, segnalo la pagina della Commissione EU dedicata ai servizi fiduciari del Regolamento eIDAS:
- https://ec.europa.eu/digital-single-market/news/questions-answers-trust-services-under-eidas.

Per chi si fosse perso qualche puntata: i servizi fiduciari sono quelli di firma elettronica, di sigilli elettronici, di marca temporale e di autenticazione dei siti web. Questi servizi sono oggi oggetto del Regolamento europeo eIDAS (e quindi il nostro CAD, o Codice dell'amministrazione digitale, dovrà essere emendato).

****

07- SPID al via

SPID è il "Sistema pubblico di identità digitale", che dovrebbe permettere un più facile interfacciamento con la Pubblica amministrazione. Nelle prossime settimane gli identity provider inizieranno a rilasciare le prime identità digitali.

Per saperne di più, segnalo questo articolo (da tweet di @FrankFormisano):
- http://www.chefuturo.it/2016/03/le-5-cose-da-sapere-su-spid/.

****

08- Materiale per verifiche presso CA

Luciano Quartarone (che ringrazio perché distribuisce il proprio sapere) mi ha segnalato il suo post "Framework per Certification Authority che pubblicano Certificati di Root". Oltre alla solita sbrodolata di link necessari per mettere in fila i requisiti normativi, in fondo c'è una checklist che ho utilizzato come self-assessment per impostare degli audit presso alcune CA: spero possa essere interessante.

Questo è il link:
- http://www.lucianoquartarone.it/wp/?p=670.

****

09- Ricette mediche elettroniche

Segnalo questo articolo del Sole 24 Ore dal titolo "La ricetta diventa elettronica. Su carta solo un promemoria":
http://www.ilsole24ore.com/art/norme-e-tributi/2016-02-28/la-ricetta-diventa-elettronica-carta-solo-promemoria-183542.shtml.

Mi paiono interessanti alcune questioni:
- il sistema prevede un piano di continuità operativa basato sulla "vecchia" ricetta cartacea;
- come sempre si vede resistenza al cambiamento;
- però si è cautamente ottimisti ("una semplificazione delle procedure è ancora possibile"), cosa rara.

Non ne so altro (se per esempio sono state fornite indicazioni ai medici di base su come garantire la sicurezza del sistema). Sarà un tema da osservare nel tempo.

****

10- Standardizzazione: ISO/IEC 27000:2016 - Vocabolario

Franco Ferrari di DNV GL mi ha segnalato l'uscita della nuova versione della ISO/IEC 27000 dal titolo "Overview and vocabulary".

Tra qualche tempo, credo, dovrebbe essere disponibile come standard pubblico al seguente sito (dove si trova ancora la versione del 2014):
- http://standards.iso.org/ittf/PubliclyAvailableStandards/.

****

11- Standardizzazione: ISO 9000:2015

Tony Coletta mi ha segnalato la nuova versione dello standard ISO 9000:2015 dal titolo "Quality management systems: Fundamentals and vocabulary".

Si tratta di uno standard fondamentale per chiunque si occupa di qualità e non solo.

La pagina web dell'ISO è la seguente (il prezzo è circa 160 Euro, che preferisco non commentare):
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45481.

****

12- Standardizzazione: ISO 5500x su Asset management

Il comitato ISO SC27 (più correttamente ISO/IEC JTC 1/SC 27/WG 1; quello che si occupa della ISO/IEC 27001) di cui faccio parte ha ricevuto un aggiornamento dal comitato ISO/TC 251, che si occupa di "Asset management".

Questa introduzione per spiegare come mi sono imbattuto nelle norme della serie ISO 5500x, dedicate all'asset management. Esse sono 3 e sono tutte del 2014:
- ISO 55000, di introduzione;
- ISO 55001, con i requisiti (certificabili) di un sistema di gestione per gli asset;
- ISO 55002, guida alla gestione degli asset.

Esse derivano dalla PAS 55 del BSI.

Mi sembrano norme decisamente generali, di cui non riesco a capire i confini. Sembra si occupino di tutto (il termine "asset" può denotare sia beni intangibili che beni tangibili di ogni tipo) e in effetti i requisiti sono decisamente generici.

Ho provato anche a leggere la pubblicazione "Asset Management – an anatomy" del The institute of asset management e i miei dubbi sono rimasti tali. Essa è reperibile su:
- https://theiam.org/what-is-asset-management/anatomy-asset-management.

Ogni contributo su questo argomento è benvenuto.

****

13- Verizon Data breach digest

Segnalo, anche complice la pubblicità che si sono fatti, il "Data breach digest. Scenarios from the field" di Verizon. Si tratta, in definitiva, di 20 scenari di attacco. Nulla di nuovo, ma utile:
- http://www.verizonenterprise.com/verizon-insights/data-breach-digest/2016/.

Un altro elemento interessante è la relazione tra le 20 minacce e i 20 CIS Critical Security Controls, di cui già scrissi qualche tempo fa (http://blog.cesaregallotti.it/2015/11/cis-critical-security-controls.html).

****

14- Studio sulle assicurazioni informatiche

Segnalo questo bello studio sulle "cyber-assicurazioni":
- http://www.fp7-camino.eu/assets/files/TR-17-2015.pdf.

Mi piace perché presenta una tabella con un'analisi delle assicurazioni oggi sul mercato (ne presenta 14) e ne specifica i limiti.

Ovviamente mi piace perché conferma cose che dico da tempo (come per esempio l'assenza di dati adeguati per calcolare la probabilità di una minaccia) e perché presenta uno studio approfondito sulle tecniche di gestione del rischio.

Ovviamente, non mi piace il termine "cyber-insurance" (che peraltro non viene definito), ma lo si sapeva già.

****

15- Continuità e resilienza

Il Business Continuity Institute (BCI) ha pubblicato una dichiarazione per chiarire la differenza tra continuità e resilienza:
- http://www.thebci.org/index.php/news#/news/the-business-continuity-institute-s-position-statement-on-organizational-resilience-150976.

La continuità operativa si occupa del ripristino delle attività a fronte di incidenti che le hanno interrotte e di prevenire le interruzioni.

La resilienza è una materia più ampia. Una definizione di resilienza è "capacità di adattamento di un'organizzazione in un ambiente complesso e mutevole". Non vuole dire molto, per la verità, ma si capisce che la continuità operativa (o business continuity) ne è solo una parte.

Penso che sia utile avere chiare le differenze tra le varie materie (segnalo qui che la ISO 9004 parla di "successo sostenibile" e qualcuno un giorno ci spiegherà la differenza tra questo e la resilienza).

****

16- Scopre falla Facebook, premiato hacker buono

Una persona ha segnalato a Facebook una vulnerabilità (credo in una versione beta del software). Facebook ha riparato il bug e premiato il segnalante:
- http://www.ansa.it/sito/notizie/tecnologia/internet_social/2016/03/09/hacker-scopre-falla-facebook-premiato_b0fe4987-8fbf-4087-96dd-9112d5f96bfb.html.

Lo segnalo non tanto per il premio, ma per il fatto che, evidentemente, Facebook ha aperto un canale per ricevere segnalazioni e lo usa. Esempio da seguire.

****

17- DROWN

DROWN è una vulnerabilità dell'HTTPS e quindi di SSL e TLS:
- https://drownattack.com/.

La soluzione è aggiornare i server e disabilitare SSL. L'articolo fornisce chiare indicazioni.

Ovviamente sono ancora tanti (e ne ho ahimè le prove) gli amministratori di sistema che non hanno ancora disabilitato l'SSL, nonostante le numerose vulnerabilità. Anzi, alcuni amministratori di sistema non sanno neanche se l'SSL è attivo e se possono abilitare il TLS. Quando si parla della formazione...

****

18- Cambiare le password più raramente?

Da un tweet di @MarcoCiappelli, segnalo questo articolo dal titolo "Want safer passwords? Don't change them so often":
- http://www.wired.com/2016/03/want-safer-passwords-dont-change-often/.

In breve l'autore dice che, se si cambiano le password troppo spesso, queste risultano o banali o sempre le stesse (per esempio pippo01, pippo02, pippo03, eccetera). Si dovrebbe invece prevedere un cambio meno frequente, per esempio annuale, e chiedere di creare password più robuste e più lunghe.

Credo si debba riflettere su questo punto, non solo ricordando che la normativa italiana in materia di privacy richiede di cambiare la password ogni 3 o 6 mesi.

Se la password è lunga meno di 15 caratteri, un attaccante la individua dopo pochi minuti e quindi cambiarla dopo 3, 6 mesi o mai non cambia nulla. E oggi, forse, anche 15 caratteri non sono sufficienti.

Si potrebbe richiedere di usare dei generatori-archivi di password complesse (come ricordato dall'autore dell'articolo), ma poi nessuno vorrà bloccare il pc quando lo lascia incustodito per la pausa caffè.

In realtà, non dimentichiamocelo, uno dei motivi per chiedere di cambiare periodicamente la password è che troppi utenti, nonostante le regole fornite, la comunicano ad amici, colleghi e parenti. Cambiarla periodicamente, almeno riduce il numero di persone che ne è in possesso. Purtroppo gli amministratori di sistema sono i primi a condividere tra loro le password e non cambiarle mai, nonostante negli anni le persone che le conoscono, a causa dei cambi di mansione o di dimissioni, sono sempre più numerose.

****

19- Caso Apple - FBI

Il caso FBI - Apple è ormai noto a tutti. L'FBI ha chiesto all'Apple di creare delle backdoor sui propri prodotti in modo da poter condurre indagini quando necessario; Apple si è rifiutata, riaccendendo un dibattito in corso da decenni (ricordate Zimmermann e il PGP? era il 1991) ed evidentemente non concluso.

Mi astengo da ogni commento e segnalo questo confronto su Il quotidiano giuridico tra Giovanni Ziccardi (professore) e Patrizia Caputo (magistrato), forse il modo migliore per affrontare l'argomento senza inutili polemiche:
- http://www.quotidianogiuridico.it/documents/2016/03/02/apple-vs-fbi-voi-cosa-ne-pensate.

****

20- L'evoluzione della sicurezza nazionale italiana

Per chi fosse interessato, segnalo questo studio dal titolo "L'evoluzione della sicurezza nazionale italiana":
- http://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/levoluzioe-della-sicurezza-nazionale-italiana.html.

Si parla anche di sicurezza del cyber spazio (e, ahimè, anche di minacce "cibernetiche").