Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS –SETTEMBRE 2014

****

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- Consiglio di Amministrazione e rischi aziendali

A giugno, Protiviti ha pubblicato un interessante documento dal titolo "Il ruolo del Consiglio di Amministrazione nel governo dei rischi aziendali". Esso analizza le disposizioni del Codice di Autodisciplina per le società quotate, che richiede al CdA di definire le linee di indirizzo affinché i principali rischi risultino correttamente identificati, misurati, gestiti e monitorati.

Il documento è di 36 pagine e mi sembra completo e ben fatto, considerando le diverse tipologie di rischio da affrontare (includendo ovviamente quelli di sicurezza delle informazioni). Si capisce bene, leggendolo, quanto sia importante avere un orizzonte ampio, senza però essere dei tuttologi.

Il documento sottolinea come l'analisi del rischio di impresa non debba ridursi al soddisfacimento del compitino richiesto dal Codice, ma debba essere visto come potente strumento di governo.

Il link per scaricare il documento:
- http://www.protiviti.com/it-IT/Documents/Protiviti-Il-ruolo-del-CdA0-nel-governo-dei-rischi-ed-luglio-2014.pdf

****

02- Privacy: Dei danni della violazione della privacy

Interessante sentenza della Corte di Cassazione: non si può avere un risarcimento del danno per diffusione impropria dei propri dati personali se non si prova che questo è grave e non futile.

Mi pare una buona sentenza perché toglie un po' di arbitrarietà.

La notizia l'ho avuta da Filodiritto. L'articolo che segnalo riporta anche il link alla sentenza della Corte di Cassazione:
- http://www.filodiritto.com/news/2014/cassazione-civile-per-il-risarcimento-della-violazione-della-privacy-la-lesione-deve-essere-grave-e-il-danno-non-futile.html

****

03- Privacy: Manuale sul diritto europeo in materia di protezione dei dati

A luglio avevo ricevuto dalla newsletter di Filodiritto la notizia della pubblicazione del "Manuale sul diritto europeo in materia di protezione dei dati", ma l'avevo ignorata. Massimo Cottafavi di Reply mi ha segnalato a sua volta la notizia e quindi non posso fare a meno di darla.

La pubblicazione si trova a questo indirizzo:
- http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law.

Essa è curata dalla "European Union Agency for Fundamental Rights" o EU FRA. La guida mi sembra fatta molto bene, con molti esempi e molte informazioni.

Perché l'avevo ignorata? Perché di fronte alla domanda "chi nominare responsabili (interni e esterni) del trattamento?" ho trovato risposte troppo vaghe. Inoltre ho il sospetto che non aggiunga molto alla letteratura già diffusa (anche se questo manuale è gratuito e fatto bene) e che sia in ritardo, vista la probabile e futura approvazione del Regolamento Europeo.

****

04- Standard: ISO/IEC 27036-2:2014 sulla gestione dei fornitori

È stata recentemente pubblicata la ISO/IEC 27036-2:2014 dal titolo "Information security for supplier relationships — Part 2: requirements":
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=59680.

A rigore si tratta quindi di una norma "certificabile", anche se non mi sembra che i requisiti siano tali da poter essere utilizzati in questo modo. Tra l'altro, la norma stessa non riporta alcun metodo per valutare la conformità di adozione.

La norma riporta cosa prevedere per stabilire delle relazioni tra acquirente e fornitore, fornendo requisiti sia per gli uni sia per gli altri. Anche da questo punto di vista mi sembra di difficile valutazione, anche se molti spunti sono interessanti.

****

05- Standard: ISO 9001:2015 DIS report dell'IRCA

In molti prevedono la pubblicazione della nuova ISO 9001 nella prima metà 2015 e questo è confermato dalla velocità con cui i lavori stanno andando avanti. A maggio 2014 è stato pubblicato il draft della norma, ossia il penultimo passo prima della pubblicazione (l'ultimo passo è il final draft).

In molti stanno studiando le bozze e si interrogano sugli impatti dei molti cambiamenti che la norma subirà. In particolare, bisogna discernere i cambiamenti formali da quelli sostanziali.

IRCA (International Register of Certificated Auditors) ha preparato un report di 65 pagine sulla nuova 9001 (a pagamento):
- http://www.irca.org/en-gb/resources/INform/INform-July-August-2014/Dont-miss-IRCA-ISO-90012015-DIS-report/

Personalmente non sono d'accordo con alcune interpretazioni perché aggiungono nuovi requisiti non previsti in realtà dalla norma stessa. Inoltre, trovo molto povera la parte relativa all'analisi dei rischi.

Questo report mi ha fatto riguardare i paragrafi relativi alle non conformità. Purtroppo sono scritti in maniera da lasciar intendere che per ogni non conformità si debba individuarne le cause e stabilire se attuare delle azioni correttive. Questo è un meccanismo perverso: se per ogni errore, senza alcuna selezione, bisogna ricercare le cause (attività che, se fatta correttamente, è onerosa), allora siamo sicuri che molte di queste non conformità saranno nascoste. Spero questi requisiti siano modificati.

Segnalo inoltre che non si parla più di "miglioramento continuo" (o "miglioramento in continuo"), ma solo di "miglioramento", perché la precedente espressione sembrava spingesse verso il solo "miglioramento a piccoli passi" o "kaizen".

Segnalo infine alcune cose che le organizzazioni non devono necessariamente fare:
- rimuovere i rappresentanti per la qualità, anche se la futura 9001 non li richiederà più: se le loro responsabilità erano funzionali agli obiettivi dell'organizzazione, nulla impedisce di mantenerli (o di nominarli);
- eliminare le procedure documentate che la futura 9001 non richiederà più (per esempio, quella sugli audit interni, che in Italia è comunque bene mantenere): se erano veramente utili, allora vanno mantenute; forse il fatto che non siano più esplicitamente richieste dalla norma spingerà le organizzazioni a scrivere procedure veramente utili;
- rinumerare i documenti per allinearli alla nuova disposizione dei requisiti della futura 9001: nessuno ha mai richiesto di numerare 7.2 la procedura per le attività commerciali, nessuno richiederà di rinumerarla 8.2 (ho sempre scoraggiato l'inserimento dei riferimenti delle norme nelle procedure perché le fanno interpretare come adempimenti formali e niente altro);
- modificare i documenti per usare i nuovi termini della nuova 9001 (per esempio, "informazioni documentate" al posto di "documenti", "procedure documentate" e "registrazioni" o "fornitori esterni" al posto di "fornitori").

Ricordo che quanto detto riguarda una bozza e non la versione finale; inoltre si prevede che per la transizione delle organizzazioni verranno lasciati 3 anni dalla pubblicazione. Suggerisco quindi di aspettare a trarre conclusioni e avviare progetti di modifica del proprio sistema qualità.

****

06- Sicurezza: Cloud forensics

Segnalo questo interessante articolo di Marco Mattiucci dal titolo "Le sfide del Cloud Forensics":
- http://www.marcomattiucci.it/cloud_challenges.php

Ci sono molti spunti da tenere a mente: la definizione di "domicilio informatico", la volatilità dei dati, le difficoltà di cancellazione, eccetera.

****

07- Sicurezza: HTTP Shaming

HTTP Shaming è un sito "gogna", dove sono riportati i siti che non proteggono adeguatamente e quando necessario le connessioni con meccanismi crittografici:
- http://httpshaming.tumblr.com/

Interessante osservare come regole architetturali di base non siano seguite.

Da quello ho trovato anche questo sito "gogna", in cui sono riportati i siti che rimandano via e-mail le password di registrazione (pratica inutile e potenzialmente nociva):
- http://plaintextoffenders.com/

La notizia l'ho ricevuta via SANS NewsBites del 19 agosto, che a sua volta segnala questo interessante articolo:
- http://arstechnica.com/security/2014/08/new-website-aims-to-shame-apps-with-lax-security/

****

08- Sicurezza: Metodi per costruire password complesse

Sono proposti sempre nuovi metodi per creare "facilmente" password complesse. Uno di questi prevede di utilizzare, con qualche variazione, le prime lettere di una frase.

Stefano Ramacciotti mi ha segnalato questo link con questo commento che condivido: "Capisco che l'autore del libro sia un appassionato di sudoku, ma inventarsi un metodo così complesso per creare delle password... Molto meglio quello indicato nel tuo libro":
- http://www.infosecurity-magazine.com/view/39315/review-a-password-system-that-favors-puzzle-over-ease/

Stefano non dice che il metodo riportato sul mio libro me l'ha fornito lui insieme a tante altre idee (sarò sempre in debito).

****

09- Sicurezza: Flusso delle informazioni

Nel 1999 andai in vacanza in Irlanda. Formula fly & drive: volo fino a Dublino e poi macchina a noleggio prenotata via servizio web (c'erano anche allora!). Arrivati a Dublino, il noleggiatore non trova la mia

prenotazione; indaga un po' e poi scopre che avevano registrato Cork come luogo della consegna. Ho capito quindi che io avevo inserito i dati sul loro sito web e poi qualcuno li ha copiati manualmente nel loro sistema di prenotazione. L'avventura finì bene e mi diedero anche un'auto di categoria superiore.

Questa pratica (trasferimento manuale di dati da un sistema informatico ad un altro) non è tramontata negli anni, ma mi ero dimenticato dei rischi che pone, nonostante ne abbia avuto esperienza diretta.

Recentemente un mio cliente ha richiamato la mia attenzione su questo rischio e finalmente ho capito il significato del controllo A.10.8.5 "Business information systems" della ISO/IEC 27001:2005. Purtroppo il controllo era spiegato male e, evidentemente, in pochi ne avevano colto l'importanza. Fatto sta che nella nuova versione dello standard non c'è più. Ci rimane il controllo A.14.1.3 "Protecting application services transactions", anche se sembrerebbe applicabile alle sole applicazioni informatiche e non a tutto un flusso di informazioni.

****

10- Sicurezza: La lunga storia degli HSM

Vi ricordate degli HSM? Sono di dispositivi necessari al protocollo di firma digitale previsto dalla Legge italiana e dovrebbero essere certificati relativamente alla loro sicurezza da diversi anni.

Questo post, segnalatomi da Stefano Ramacciotti (che ringrazio), commenta l'ennesima proroga:
- http://sinetqnlap.wordpress.com/2014/07/11/hsm_ultima_spiaggia/

****

11- LinkedIn e social network

Questa è una delle mie piccole storie personali che propino ai miei lettori, ma ha una morale relativa alla sicurezza delle informazioni.

Negli ultimi mesi ho scritto, per dei clienti, delle regole in merito all'uso dei social network. Le solite cose: non parlate con gli sconosciuti, non scrivete cose relative all'azienda per cui lavorate, se dovete usare i social network per finalità aziendali prestate attenzione a questo e a quello.

Nello stesso periodo mi sono accorto delle e-mail di LinkedIn che mi consigliavano di fare gli auguri o di congratularmi con perfetti sconosciuti con cui però avevo una connessione. In effetti, anche con la speranza di farmi pubblicità, negli ultimi anni accettavo le connessioni da parte di tutti. Poi mandavo l'invito ad iscriversi alla mia newsletter e quasi nessuno accettava.

Non accettavo le connessioni solo quando avevo il sospetto che mi avessero scambiato per un altro Gallotti, anch'egli ex dipendente di DNV. A questi chiedevo se per caso avessero fatto confusione, ma anche qui le risposte sono state pochissime.

Infine ho fatto caso alle richieste che mi arrivavano: erano quelle standard. E quindi originate da persone intente a preparare qualche phishing o che per errore hanno premuto qualche bottone di troppo su LinkedIn o che semplicemente erano troppo pigre per scrivere "non ci conosciamo, però mi piacerebbe connettermi con te per queste ragioni:...".

Quindi, visto che un consulente deve essere il primo a dare l'esempio, ho deciso: a) di rispondere gentilmente agli sconosciuti che mi chiedono la connessione dicendo che mi connetto solo a persone che conosco nella vita reale; b) cancellare le connessioni con sconosciuti.

Una prima pulizia mi ha portato da 466 connessioni a 365. Mi scuso con quanti ho cancellato perché mi sono dimenticato di averli effettivamente conosciuti (però, se non ho mantenuto i contatti o i ricordi, un motivo ci sarà; o forse è solo l'effetto del mio impegno alla riservatezza che è diventato smemoratezza?).

La morale finale credo sia ovvia: seguite voi stessi le regole che credete siano giuste per gli altri.

****

12- Minacce e attacchi: Poste Italiane devono rimborsare una vittima di phishing

Interessante sentenza del Tribunale di Firenze: Poste Italiane, nel 2010, non aveva previsto idonee misure di sicurezza per ridurre il rischio che i propri clienti fossero vittime di phishing. Già da tempo, Poste Italiane, come altre banche, ha previsto l'uso di one-time-password, ma il caso in questione è precedente.

Risultato: Poste Italiane deve rimborsare al proprio cliente la perdita economica conseguente alla comunicazione delle proprie credenziali ad un malintenzionato, dopo aver ricevuto una mail di phishing:
- http://www.altalex.com/index.php?idu=264948&cmd5=021c46ab76df2fd7050bbc8c56ed7fe1&idnot=68463.

Francamente, non riesco a dire se questa sentenza mi sembra giusta o sbagliata: da una parte è giusta perché Poste non aveva messo in atto le misure di sicurezza previste dalle "buone pratiche", dall'altra non capisco perché debbano essere ritenute responsabili di un errore di un loro cliente.

****

13- Minacce e attacchi: iCloud e il furto delle foto

È su tutti i giornali: sono state rubate delle foto da iCloud con celebrità nude:
- http://mashable.com/2014/08/31/celebrity-nude-photo-hack/

L'attacco è spiegato in questo articolo:
- http://www.wired.com/2014/09/eppb-icloud/

In breve (se ho capito correttamente): dei malintenzionati hanno fatto un attacco a forza bruta (cioè hanno provato tutte le password possibili) sugli account di iCloud con uno strumento del costo di circa 400 dollari e disponibile solo a forze di polizia. Gli attaccanti hanno quindi recuperato dati di diversa gente, tra cui foto di nudo di donne celebri, e li hanno pubblicati. La paura è che altri dati possano essere usati per ricattare altri utenti.

La cosa interessante è che Apple ha detto che questo non rappresenta un incidente di sicurezza dei loro sistemi. Forse perché non sono state violate delle politiche prestabilite da Apple stessa. Penso che avrebbe potuto fare qualche riflessione in più su come "aiutare" in futuro gli utenti a scegliere e gestire password più robuste e su come gestire i file oggetto di backup mantenuti dall'iCloud (ossia quelli acceduti dagli attaccanti). Ma soprattutto avrebbero dovuto immaginare che lo strumento "disponibile a forze di polizia" sarebbe prima o poi caduto in possesso di malintenzionati.

Questo ultimo aspetto è interessante: dall'articolo si capisce che la tecnica di attacco era descritta e suggerita in molti forum sul web. Mi viene quindi da pensare che Apple non abbia attuato tecniche di analisi su quanto pubblicato sul web in merito alle proprie vulnerabilità.

Per quanto riguarda gli utenti stessi, sarebbe il caso di riflettere sul falso senso di sicurezza che ci danno alcuni servizi disponibili su Internet e su quanto facciano per proteggersi (password robuste, selezione dei file da salvare, eccetera).

PS: oggi ho sentito che le prenotazioni del prossimo modello di iPhone hanno superato tutti i record. Dimostrando così come certi eventi, sebbene gravissimi non intaccano per niente l'immagine di un'azienda.

****

14- Minacce e attacchi: Patch Microsoft con problemi

Questa me l'ha segnalata Marco Fabbrini:
- http://www.hwupgrade.it/news/sistemi-operativi/patch-tuesday-di-agosto-disinstallare-l-aggiornamento-2982791-descritto-da-ms14-045%C2%A0_53641.html

In pochissime parole: un security update di Microsoft per Windows introduce instabilità ai sistemi fino, in alcuni casi, a bloccarli.

Marco aggiunge il commento: "quando mi dicono che le patch di sicurezza vengono installate senza nessuna prova, di solito mi limito ad una "faccia" strana; dopo questo articolo le argomentazioni potranno essere altre!"

_____

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
Mail: cesaregallotti@cesaregallotti.it
PEC: cesaregallotti@mailcert.it