Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – SETTEMBRE 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- Gli esperti credono alle bugie
02- I manager parlano di sicurezza, ma poi...
03- Check list
04- Standardizzazione: Qualche commento sulla futura ISO 9001:2015
05- Standardizzazione: ISO/IEC 27023 - Confronto versioni 27001 e 27002
06- Standardizzazione e business continuity: ISO/TS 22317 e BIA
07- Standardizzazione: ISO/IEC 27033-1, 27034-2, ISO/IEC TS 3014 e ISO/IEC TS 38501:2015
08- Privacy: ISO/IEC 29190 - Privacy capability assessment model
09- Novità legali: Regolamenti SPID
10- Novità legali per la PA: protocollo IT e privacy
11- Legale: Tripadvisor non risponde della veridicità delle recensioni
12- Tecnologia: Hacking e automobili
13- Tecnologia: Sicurezza applicativa
14- Tecnologia: Corso di sicurezza IT del MIT
15- Tecnologia: Windows 10

****
01- Gli esperti credono alle bugie

La mia traduzione del titolo della notizia è scorretta. Quello giusto sarebbe: "Quelli che si auto-proclamano esperti, hanno più probabilità di credere ad asserzioni false":
- http://www.washingtonpost.com/news/speaking-of-science/wp/2015/07/20/self-proclaimed-experts-more-likely-to-fall-for-made-up-facts-study-finds/

In sostanza: se elenchi ad un fan del rock indie dei gruppi inesistenti, ti rispondono che li conoscono o ne hanno sentito parlare; se chiedi a degli esperti di finanza se conoscono alcuni termini, più si sentono esperti, più è elevata la probabilità che conoscono anche quelli inesistenti (anche se dici loro che si tratta di un esperimento e alcuni termini sono inventati!).

L'articolo si conclude dicendo che, una volta ci si reputa un esperto, si smette di imparare e questo ci porta a non essere più esperti e a fare figuracce.

Mi è venuto in mente che, quando avete a che fare con dei consulenti (che si proclamano esperti), potreste chiedere loro di cose inesistenti e vedere l'effetto che fa (questo quando non sono già abbastanza esaltati di loro stessi e non dicono sciocchezze senza alcun invito...).

****

02- I manager parlano di sicurezza, ma poi...

La notizia è sempre la stessa, ma mi piace ribadirla perché un po' di polemica non guasta:
- http://www.csoonline.com/article/2978020/security-leadership/do-boards-of-directors-actually-care-about-cybersecurity.html.

In sostanza:
- una ricerca di CSO dice che il 60% dei responsabili della sicurezza delle informazioni fanno almeno una presentazione annuale ai manager;
- il 42 dei manager pensa che la sicurezza delle informazioni non sia un problema della Direzione.

Ognuno tragga le proprie conclusioni.

****

03- Check list

A luglio, con perfetto tempismo, ben tre clienti mi hanno chiesto cosa ne pensassi dell'uso di check list per gli audit. La mia risposta è stata: "non le ritengo utili, anzi, le ritengo dannose". Non sono un genio e a questa conclusione sono arrivato dopo aver usato delle check list e averne visto i difetti.

Come auditor di certificazione, la mia check list dovrebbe essere la norma di riferimento. Ovviamente, negli anni, ho creato degli appunti relativi ai requisiti più sintetici e ad alcuni settori merceologici; però non costituiscono assolutamente una check list.

Come auditor interno, i requisiti da verificare sono le procedure e regole interne, e quindi svolgo l'audit con quelle, non con un'altra cosa (le check list). Infatti: perché dovrei avere un documento di riferimento (la check list) diverso da quello che hanno le persone da intervistare (le politiche e le procedure)? Se ho difficoltà ad orientarmi tra regole e procedure, perché dovrei pretendere che non ne abbiano gli intervistati? Se ci sono regole scritte solo sulla mia check list e non nelle regole e procedure consegnate al personale, come posso pretendere che le seguano? Perché, quando necessario, invece di aggiornare un solo documento bisogna aggiornarne due? Come faccio a capire se una procedura è scorretta, incompleta o poco chiara se non la leggo insieme alla persona intervistata e mentre mi illustra come applica i requisiti stabiliti?

Anche qui non sono completamente impreparato: sul piano di audit riporto le procedure applicabili ad ogni intervista e prima di ogni intervista rileggo le procedure e mi segno i punti più importanti da verificare.

Certamente le check list compilate possono dimostrare che l'audit è stato fatto completamente. Ma anche un rapporto di audit, con riportate le procedure analizzate e le prove raccolte, lo può fare.

****

04- Standardizzazione: Qualche commento sulla futura ISO 9001:2015

IRCA ha pubblicato un documento dal titolo "ISO 9001:2015: understanding the international standard". Purtroppo è disponibile solo agli iscritti.

Il documento riepiloga i cambiamenti maggiori rispetto all'edizione del 2008: l'adozione dell'Annex SL e, quindi, un maggiore allineamento con gli altri standard relativi ai sistemi di gestione; il maggiore coinvolgimento della Direzione, anche se solo attraverso il cambiamento del termine "impegno" con "leadership"; la necessità di analizzare non solo l'organizzazione ma anche il contesto in cui opera; l'introduzione di tecniche di valutazione del rischio e la promozione di un "pensiero basato sul rischio"; l'integrazione dei requisiti per i fornitori con quelli per gli outsourcer; l'uso di "informazioni documentate" al posto di "documenti" e "registrazioni".

Trovo molto interessante la parte relativa alle cose NON richieste a chi adotta il nuovo standard;

- non è necessario rimuovere il "referente della Direzione per il sistema qualità"; la norma non lo più richiede esplicitamente, ma non lo vieta neanche; si osservi che oggi è molto più chiaro il fatto che la responsabilità del sistema di gestione per la qualità è della Direzione, ma è anche vero che alcune attività di coordinamento e supervisione dovranno essere assegnate a qualcuno (segnalo che in passato mi divertivo molto ad osservare alcuni auditor perplessi perché in alcune aziende in cui ero consulente il "responsabile qualità" era il Direttore Generale o l'Amministratore Delegato; purtroppo non potrò più godere di questo discutibile divertimento);

- non è necessario buttare via tutti i manuali e le procedure già fatti: se li avete fatti bene, vuol dire che sono utili e vanno mantenuti; osservate che i processi e le attività devono comunque essere stabili e, quindi, un minimo di documentazione è raccomandata; forse vedremo meno documenti inutilmente lunghi per essere "a prova di auditor" e questo sarà un beneficio per tutti;

- rinumerare i documenti esistenti per allineamento con la nuova struttura della norma: io ho sempre pensato che fosse un errore numerare e ordinare i documenti come i capitoli della norma perché su certe cose è l'azienda che deve guidare, non la norma; comunque nessuno vi vieta di rinumerarli;

- riordinare i documenti per allinearli al nuovo standard: ancora una volta ho sempre pensato fosse molto stupido avere il manuale qualità numerato secondo la norma (ma, in Italia, Accredia l'aveva raccomandato...) perché un manuale scritto così spesso era di difficile lettura per il personale medio di un'azienda (e infatti non era usato come "manuale", ma come "presentazione" neanche tanto chiara, come ricordo bene dalle mie precedenti esperienze di lavoratore dipendente);

- modificare i documenti esistenti per adottare la nuova terminologia: non ho mai condiviso l'idea che chi adotta la ISO 9001 debba anche adottarne la terminologia (e, per esempio, usare "non conformità" e non "difettosità" o "azioni correttive e preventive" e non "azioni di miglioramento"), ma non la ritengo infondata; bisogna però evitare di modificare termini chiari ("procedure", "istruzioni", "registrazioni") con termini oggettivamente poco chiari ("informazioni documentate").

****

05- Standardizzazione: ISO/IEC 27023 - Confronto versioni 27001 e 27002

La ISO ha pubblicato la ISO/IEC 27023:
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61005

Questa norma, dal prezzo di 118 Franchi svizzeri, riporta le tabelle di correlazione tra le versioni del 2005 e 2013 delle ISO/IEC 27001 e 27002.

Confesso che non ne ho seguito i lavori, visto che era già stato pubblicato un documento ufficiale a inizio 2014, tra l'altro liberamente scaricabile:
- http://www.jtc1sc27.din.de/cmd?level=tpl-bereich&languageid=en&cmsareaid=wg1sd3.

Per questo motivo non capisco perché sia stata pubblicata ora questa versione a pagamento, ben due anni dopo la pubblicazione delle nuove ISO/IEC 27001 e 27002.

****

06- Standardizzazione e business continuity: ISO/TS 22317 e BIA

Franco Ferrari di DNV GL mi ha segnalato la prossima pubblicazione della ISO/TS 22317 dal titolo "Business continuity management systems -- Guidelines for business impact analysis (BIA)":
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50054.

Rimango dell'idea che la SP 800-34 del NIST, dal titolo "Contingency Planning Guide for Federal Information Systems", è più chiara e utile (propone anche un modello da usare per la BIA):
- http://csrc.nist.gov/publications/PubsSPs.html#800-34.

****

07- Standardizzazione: ISO/IEC 27033-1, 27034-2, ISO/IEC TS 3014 e ISO/IEC TS 38501:2015

Segnalo la pubblicazione di altre due norme internazionali di tipo tecnico:
- ISO/IEC 27033-1:2015: "Information technology -- Security techniques -- Network security -- Part 1: Overview and concepts" (http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63461);
- ISO/IEC 27034-2:2015: "Information technology -- Security techniques -- Application security -- Part 2: Organization normative framework" (http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63461).

Sicuramente è stato interessante per gli autori scriverle. Per capire la sicurezza delle reti e delle applicazioni IT, raccomando però la lettura di altri manuali più pragmatici, pratici ed economici.

Un'altra norma di tipo tecnico è la ISO/IEC TS 30104 dal titolo "Physical security attacks, mitigation techniques and security requirements", di cui già scrissi nel 2012:
- http://blog.cesaregallotti.it/2012/05/andamento-delle-norme-della-famiglia.html.

Questo standard è stato pubblicato a maggio 2015 (grazie a Franco Ferrari di DNV GL per l'informazione).

Speravo si trattasse di un documento relativo alla sicurezza fisica in generale (controllo accessi fisici, sorveglianza, anti-intrusione, eccetera), invece riguarda solo la sicurezza fisica dei dispositivi crittografici (HSM, smart card, eccetera).

Infine, segnalo la norma ISO/IEC TS 38501:2015 dal titolo "Information technology - Governance of IT - Implementation guide" (ringrazio Tony Coletta che mi ha permesso di leggerla).

Si tratta di 19 pagine. Se togliamo la parte introduttiva e la bibliografia, si riducono a 10.

Io segnalo che, prendendo spunto dal nuovo "testo unico" per norme dedicate ai sistemi di gestione (l'attuale ISO/IEC 27001, l'imminente nuova versione della ISO 9001), elenca i fattori che compongono il contesto dell'organizzazione, dividendoli in interni (strategie generali, propensione al rischio, prestazioni, cambiamenti strategici previsti e in corso, relazione tra i processi di "business" e IT, risultati degli audit cultura dell'organizzazione, impegno della Direzione, maturità, livelli di competenza, modello di erogazione dei servii informatici, rapporti con le organizzazioni partner) ed esterni (norme, leggi e regolamenti, tecnologia disponibile e come questa può ridefinire i modelli di organizzazione e la partecipazione delle persone, rischi e opportunità poste dalle nuove generazioni, mercato in cui opera l'organizzazione e concorrenza, aspettative dei clienti e dei consumatori, requisiti delle parti interessate).

Tony, a sua volta, mi ha segnalato l'appendice A, che riporta uno schema molto sintetico (una pagina) di assessment, evidentemente ispirato dalle norme SPICE, in 5 livelli: sconosciuto, non applicato, applicato parzialmente, applicato quasi completamente, applicato completamente.

****

08- Privacy: ISO/IEC 29190 - Privacy capability assessment model

È stata pubblicata la ISO/IEC 29190:2015 dal titolo "Privacy capability assessment model":
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45269.

L'intenzione è quella di presentare un metodo per valutare i processi relativi alla privacy, in linea con quanto già proposto dalla ISO/IEC 15504.

L'ho letta rapidamente e l'ho trovata: inutile (non aggiunge molto rispetto a quanto già presente nella ISO/IEC 15504 e nel Cobit) e pasticciata (dove aggiunge, si trova solo confusione).

Ora, però, i venditori di "assessment" hanno un'altra cosa da proporre.

****

09- Novità legali: Regolamenti SPID

Franco Ferrari di DNV GL mi ha segnalato la pubblicazione dei regolamenti AgID per i gestori dell'identità digitale (SPID). Una pagina web per capire di cosa si tratta e trovare i regolamenti è la seguente:
- http://www.agid.gov.it/notizie/2015/07/28/spid-al-il-sistema-laccesso-semplice-sicuro-ai-servizi-line-pa.

Franco Ferrari di DNV GL mi ha segnalato questo articolo, che mi pare chiarisca bene cos'è lo Spid e cosa succederà nel prossimo futuro:
- http://www.wired.it/attualita/2015/07/29/guida-spid-sistema-identita-digitale/.

Copio la descrizione di SPID fornita da AgID: SPID è la nuova "infrastruttura paese" di login che permette a cittadini e imprese di accedere con un'unica identità digitale, in maniera semplice e sicura, ai ervizi on line della pubblica amministrazione e dei privati che aderiranno.

Il Regolamento tecnico richiede le certificazioni ISO 9001 e ISO/IEC 27001. Ad una prima lettura, le richieste mi sembrano fatte in modo corretto. Finalmente!

Ci sono altre bizzarrie, giusto per non sbagliare, tipo la necessità di prevedere, in certe occasioni, verifiche da parte di due organismi di certificazione.

****

10- Novità legali per la PA: protocollo IT e privacy

Segnalo questo articolo (grazie a Giovanni Francescutti e Franco Ferrari di DNV GL) dal titolo "Gestione dei documenti informatici nella PA: scatta tra un mese (11 ottobre 2015) una scadenza cruciale":
- http://www.agendadigitale.eu/egov/gestione-dei-documenti-informatici-nella-pa-scatta-tra-un-mese-una-scadenza-cruciale_1660.htm

I toni sono molto giornalistici, ma il contenuto è interessante.

Per quanto riguarda la privacy, il 2 luglio 2015 il Garante ha pubblicato il Provvedimento dal titolo "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche" (doc web 4129029):
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4129029.

In sintesi, il Garante richiede alle pubbliche amministrazioni di "comunicare al Garante, entro 48 ore dalla conoscenza del fatto, tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati".

Insomma, si tratta di un'estensione della misura cosiddetta "data breach", finora prevista solo per i fornitori di servizi di telecomunicazione.

****

11- Legale: Tripadvisor non risponde della veridicità delle recensioni

Sono sempre molto prudente quando leggo le recensioni di Tripadvisor e di siti simili. E ora ho confermata questa mia attitudine:
- http://www.altalex.com/documents/news/2015/07/22/tripadvisor-recensioni-tar-roma-9355-del-2015.

L'AGCOM aveva inizialmente individuato la diffusione di informazioni ingannevoli nelle recensioni su Tripadvisor e quindi scritto "Tripadvisor, infatti, pur dichiarando di non controllare i fatti contenuti nelle recensioni ed essendo a conoscenza che sul predetto sito vengono pubblicate false recensioni, sia di valenza positiva che negativa, da parte di utenti che non hanno effettivamente fruito dei servizi offerti dalle strutture presenti nel database...".

Poi il TAR del Lazio ha annullato la multa di AGCOM, basandosi sicuramente su aspetti legislativi corretti, ma a mio parere l'annosa questione della veridicità delle recensioni sui siti web rimane aperta.

Per chi volesse leggere la sentenza, l'ho trovata qui:
- http://www.eius.it/giurisprudenza/2015/196.asp.

****

12- Tecnologia: Hacking e automobili

La notizia è nota da tempo: è possibile accedere via wi-fi al sistema di controllo di certe vetture e comandarle a distanza:
- http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (in inglese);
- http://www.itespresso.it/fca-richiama-14-milioni-di-auto-hackerate-110191.html (in italiano, per quanto brutto).

La cosa incredibile, come già è stato dimostrato con gli aerei, è che l'attacco inizia con la compromissione del sistema di intrattenimento, da quale poi accedere al sistema di controllo. Questo la dice lunga sulla competenza di chi ha progettato questi sistemi (o dei loro responsabili che hanno imposto sistemi più economici): da sempre sappiamo che, per sicurezza, i sistemi più critici devono essere completamente isolati da quelli meno critici.

E, ancora una volta, si vede come gli sviluppatori (di qualunque livello) di sistemi informatici siano completamente disinteressati alla sicurezza, inclusi quelli che lavorano in ambienti da sempre attentissimi a questo aspetto.

Non avrei soluzioni da proporre. Forse nelle scuole e nelle università dovrebbero integrare meglio questo aspetto nelle materie (ma recentemente ho sentito presentazioni agghiaccianti da parte di "esperti di sicurezza" che tengono corsi in qualche università; dimostrando così che la selezione dei docenti per questa materia è ancora carente); forse dovremmo noi "esperti" trovare altre strade per promuovere la sicurezza (temo che i convegni con sole presentazioni commerciali o di tecniche "base" non siano sufficienti); forse Governo e Autorità varie potrebbero trovare ulteriori strade (ma ancora una volta si vede come in questi ambienti siano molto presenti degli "esperti" incompetenti).

Scusate lo sfogo.

Colgo l'occasione per riportare una cosa che mi ha scritto Andrea Rui: "Un tempo ero più disfattista, e pensavo che fosse un problema tutto italiano: vedendo ciò che è accaduto negli ultimi anni agli americani ed ai giapponesi mi sono reso conto che il problema è uniformemente distribuito, e che alcuni sono soltanto più bravi a far credere di essere migliori degli altri".

Negli USA vogliono proporre una normativa per la sicurezza informatica delle automobili. Ottima iniziativa, ma forse non sufficiente (anche perché riguarda solo le automobili):
- http://www.wired.com/2015/07/senate-bill-seeks-standards-cars-defenses-hackers/.

PS: segnalo anche questo articolo del The Economist (grazie a Roberto Gallotti!):
- http://www.economist.com/news/science-and-technology/21657766-nascent-internet-things-security-last-thing-peoples.

Nel finale ricorda il tempo, lungo, passato prima che la sicurezza ferroviaria e delle automobili fosse presa seriamente.

****

13- Tecnologia: Sicurezza applicativa

Un'altra puntata sulla sicurezza delle applicazioni informatiche.

Stefano Ramacciotti mi ha segnalato questo link con il commento "l'articolo dice un po' le solite cose, ma i link di approfondimento possono essere utili":
- https://www.checkmarx.com/2015/07/01/9-secure-coding-practices-you-cant-ignore/.

Vista l'ignoranza in materia, penso che anche l'articolo sia interessante (noto che alcuni link sono datati, ma incredibilmente attuali).

Dal NTT Security Blog, ho avuto invece notizia della pubblicazione (del 2014!) "OWASP Mobile Security Project - Top Ten Mobile Risks":
- https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks.

Per quanto riguarda le apps nello specifico, Ivo Trotti di TNS Italia mi ha segnalato questo articolo:
- http://blog.wired.it/dirittifuturo/2013/04/15/privacy-e-app-le-regole-europee.html.

Il documento segnalato, dell'Article 29 Data protection working party, ha titolo "WP 202 - Opinion 02/2013 on apps on smart devices" ed è del febbraio 2013. L'argomento, ovviamente, è: come progettare le app (e i sistemi e processi ad esse correlati) per dispositivi mobili in modo da rispettare la privacy degli utilizzatori.

La notizia è un po' vecchiotta, ma in questo periodo mi sono trovato spesso a discutere con dei clienti in merito a questo aspetto e pertanto mi sembra opportuna.

Per completare, segnalo un mio post di dicembre 2013 con ulteriori link:
- http://blog.cesaregallotti.it/2013/12/studi-sicurezza-apps.html.

****

14- Tecnologia: Corso di sicurezza IT del MIT

Il corso "Computer Systems Security" del 2014 MIT:
- http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-858-computer-systems-security-fall-2014/

Direi che bisognerebbe darci un'occhiata.

****

15- Tecnologia: Windows 10

È ora disponibile gratuitamente Windows 10 per chi ha Windows 7 e Windows 8. Probabilmente lo installerò, ma devo prima verificare se questo Windows 10 è anche "Pro" (come il mio Windows 8).

In molti mi hanno assicurato che è migliore di Windows 8, in termini di prestazioni e facilità d'uso.

Però ci sono almeno due problemi da approfondire.

Il primo riguarda la privacy: Microsoft ha capito che deve agire come Google, Facebook e Amazon, raccogliendo il maggior numero di dati possibili sui propri utenti e poterli usare (o rivenderli a chi li vuole usare) per finalità di marketing e pubblicità. Non riesco né ad esserne sorpreso né indignato, visto che il mercato dell'informatica è ormai questo e tutti, chi più chi meno, ci siamo adeguati. Per adeguarsi un po' di meno, o si passa a Linux o si configura con attenzione il proprio sistema operativo Windows 10, come suggerito da questi articoli (ricevuti dalla newsletter SANS News Bytes):
-
http://www.slate.com/articles/technology/bitwise/2015/08/windows_10_privacy_problems_here_s_how_bad_they_are_and_how_to_plug_them.single.html;
- http://www.wired.com/2015/08/windows-10-security-settings-need-know/.

Altro aspetto riguarda la gestione delle wi-fi e il meccanismo Wi-Fi Sense: Windows 10 permette di condividere le password di accesso alle wi-fi a cui ci si è collegati con tutti i propri contatti Sype e Outlook. Cioè: io invito un mio amico a casa, gli do la password wi-fi e automaticamente tutti i suoi amici ce l'hanno. Non ho capito se è comunicata anche agli amici degli amici:
- http://arstechnica.com/gadgets/2015/07/wi-fi-sense-in-windows-10-yes-it-shares-your-passkeys-no-you-shouldnt-be-scared/;
- http://www.zdnet.com/article/no-windows-10s-wi-fi-sense-feature-is-not-a-security-risk/.

Come fare, quindi, se, al contrario degli articoli citati, si pensa che questo sia un rischio? Modificare l'SSID della propria wi-fi aggiungendo "_optout":
- http://money.cnn.com/2015/07/30/technology/windows10-wifi-sense/

Problema: con i router ADSL Alice Telecom non è possibile modificare l'SSID (l'assistenza tecnica mi ha chiesto 9 Euro per dirmi come fare). Non mi sembra molto corretto, visto che si tratta di sicurezza...