Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS - MAGGIO 2013
****

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 disiscriversi
- 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- Standardizzazione - Aggiornamenti sulle norme ISO/IEC 270xx

La settimana del 22 aprile si è tenuto a Sophia Antipolis (vicino ad Antibes, Francia) il 46 Plenary Meeting del WG1 del SC27 del JTC1 dell'ISO/IEC; in poche parole, si è tenuto l'incontro semestrale del gruppo di esperti dedicato alla scrittura delle norme della famiglia ISO/IEC 270xx. Di seguito i risultati.

Per la cronaca, per la delegazione italiana eravamo in 5 (io, il Presidente Fabio Guasconi, Andrea Caccia, Dario Forte e Stefano Ramacciotti).

ISO/IEC 27000: si è avanzati nell'aggiornamento della norma dedicata ai termini e definizioni, soprattutto per includere le novità della futura 27001; difficile oggetto di discussione è stata la definizione di Statement of Applicability.

ISO/IEC 27001: la norma è passata in stato di final draft con un solo voto negativo; dovrebbe essere quindi pubblicata a ottobre-novembre 2013, dopo l'incontro previsto a Songdo in Corea del Sud la settimana del 21 ottobre; gli aggiornamenti sono stati minimali perché, dopo anni a discutere di Annex A, posizionamento del risk assessment (nel plan o nel do), obbligatorietà o meno dello statement of applicability, eccetera, è prevalsa l'idea che si è raggiunto comunque un buon compromesso e l'unico metro di giudizio potrà essere solo l'applicazione sul campo della nuova norma; per chi volesse ripassare gli argomenti di discussione, rimando ai miei post precedenti; aggiungo il fatto che i Paesi Bassi, pur approvando il passaggio della norma in final draft, si sono formalmente lamentati delle ambiguità presenti nel testo, che potranno essere negative per il mercato (personalmente, sono d'accordo con loro).

ISO/IEC 27002: anche questa è passata in stato di final draft con 2 voti negativi (uno perché le 1.000 proposte di modifica (!) non sono state tutte correttamente prese in carico e potrebbero avere introdotto delle incoerenze nel testo; l'altro perché la norma esplicita la possibilità di avere policy a diversi livelli); anch'essa dovrebbe quindi essere approvata a ottobre a Songdo.

ISO/IEC 27003: sono iniziati i lavori sulla revisione della "Implementation guidance" che dovrebbe, nella migliore delle ipotesi, essere pubblicata tra un paio di anni; questa norma è ora reputata molto importante perché fornirà una guida all'interpretazione dei requisiti della 27001 che alcuni, me incluso, reputano in molti casi troppo sintetici. Vedremo come avanzeranno i lavori.

ISO/IEC 27004: anche per questa norma (sulla misurazione dell'efficacia di un ISMS) sono proseguiti i lavori e si applicano le stesse considerazioni fatte per la 27003; con soddisfazione di molti (inclusi gli italiani), è passata l'idea che la seconda edizione deve essere più pratica e meno teorica, a differenza dell'attuale edizione del 2009.

ISO/IEC 27006: questa volta, l'incontro sulla 27006 è stato molto più affollato delle volte precedenti; con mia grande soddisfazione, il requisito di avere la versione del SOA sul certificato è stato eliminato e si cercherà di dare maggiori possibilità di riduzione dei tempi di audit (si manterrà l'impostazione attuale, ma dando più possibilità agli Organismi di certificazione di ridurre le giornate di audit; si studierà un meccanismo per evitare che alcuni organismi facciano audit non adeguati). Ricordo però che lo stato della 27006 è ancora di Working draft e quindi molte cose potranno ancora accadere.

ISO/IEC 27009: questa norma riguarda l'uso delle norme settoriali (27011, 27017, 27018, 27019 e altre) per le certificazioni ISO/IEC 27001; c'è stata molta discussione anche sul titolo (l'Italia si è anche opposta, con la maggioranza, alla modifica del titolo in "Application of ISO/IEC 27001 - Requirements") e sul suo campo di applicabilità.

ISO/IEC 27011 (telecomunicazioni) e 27013 (uso congiunto di 27001 e 20000): è stato approvato l'inizio dei lavori di revisione.

ISO/IEC 27016 ("Organizational economics") e ISO/IEC 27017 (sul cloud computing): sono proseguiti i lavori

E' stato approvato l'inizio dei lavori per un nuovo standard sulla certificazione dei professionisti dediti all'information security management.

Infine, si è parlato della norma ISO 34001 "Security Management System", proposta dal ISO/TC 247 "Fraud countermeasures and controls", perché sembra voler essere in competizione con la ISO/IEC 27001.

****

02- Standardizzazione - Pubblicata la ISO/IEC 27014 "Governance of information security"

Franco Ferrari del DNV Italia mi ha segnalato che è stata pubblicata con data 15 maggio la ISO/IEC 27014 dal titolo "Governance of information security".

Mi chiederò sempre perché lui sappia queste cose con questo anticipo, visto che la segnalazione è del 7 maggio.

Detto ciò, posso dire quanto segue:
- la norma non dice, a mio parere, nulla di nuovo;
- rigira il modello PDCA in "Evaluate-Direct-Monitor-Communicate-Assure", a sua volta ripreso da quello proposto dalla ISO 38500 (che però si limitava alle sole prime 3 aree);
- utilizza alcuni concetti (risk appetite, information security status) non rintracciabili nelle altre norme della serie ISO/IEC 27000 in vigore e quindi potrebbero generare confusione.

Vedremo comunque come questa norma sarà accolta dal mercato e se io l'ho letta troppo distrattamente e non ne ho colto tutti gli aspetti.

****

03- Standardizzazione - Pubblicata la ISO/IEC TS 17021-3 sulle competenze degli auditor qualità

La ISO ha comunicato la pubblicazione della "ISO/IEC TS 17021 Conformity assessment – Requirements for bodies providing audit and certification of management systems, Part 3: Competence requirements for auditing and certification of quality management systems".

La parte 2, pubblicata ad agosto 2012, riguardava le competenze degli auditor dei sistemi di gestione ambientale (ISO 14001). Ricordo inoltre che queste sono norme applicabili ai soli organismi di certificazione e non alle "normali" imprese.

E' comunque interessante osservare come stia aumentando l'attenzione sulle competenze degli auditor, anche con norme dedicate. In effetti, le norme di requisiti (ossia quelle certificabili) come la ISO 9001 o la futura ISO/IEC 27001 sono sempre meno dettagliate, per garantire la loro applicabilità a tutte le tipologie di organizzazioni, e richiedono sempre più una valutazione dell'adeguatezza del sistema di gestione e delle misure adottate.

Ovviamente, per valutare l'adeguatezza di un sistema di gestione bisogna essere competenti sulla materia.

Tutto ciò, però, pone dei problemi alle organizzazioni oggetto degli audit e agli auditor: se un auditor non ritiene adeguata una misura, risulta difficile sostenere la propria tesi se quanto visto è in effetti strettamente conforme al requisito della norma; dall'altra parte, se un auditor pretende misure eccessive rispetto alle reali esigenze dell'organizzazione, diventa difficile per quest'ultima contestarle visto che la valutazione è basata su parametri spesso non scritti nella norma di riferimento (può però inoltrare reclamo e ricusare l'auditor per le successive verifiche).

Solo un auditor competente, tranne casi estremi, può avviare un reale confronto con l'organizzazione oggetto dell'audit per valutare l'adeguatezza di quanto attuato e non essere successivamente contestato quando i propri rilievi sono pertinenti.

****

04- Novità legali - Conseguenze se non si ha una PEC

Come già detto in precedenza, il DL 5 del 2012 ha introdotto l'obbligo per le società di avere una PEC.

Ora in Consiglio di Stato ha chiarito quali sono le conseguenze se non si ha una PEC: la società non può essere iscritta al Registro delle imprese!

Maggiori dettagli su Filodiritto:
- http://www.filodiritto.com/consiglio-di-stato-senza-la-pec-la-societa-non-si-iscrive-nel-registro-delle-imprese/#.UZCW4spWXj4

****

05- Novità legali - Cassazione: non esiste un dovere di omertà aziendale

La sentenza n. 6501 del 14 marzo 2013 della sezione Lavoro della Cassazione è interessante per due motivi: il primo riguarda il non dovere di omertà del lavoratore, il secondo la legittimità di accuse anonime.

Se ho capito correttamente il caso, un lavoratore ha denunciato la propria azienda all'Autorità e poi questo fatto è stato segnalato all'azienda stessa da una lettera anonima. Il lavoratore è stato quindi licenziato, ma poi ha fatto ricorso alla Cassazione basandosi su due punti: il non dovere di omertà (per cui la Cassazione si è pronunciata a favore del lavoratore) e sull'inutilizzabilità di denunce anonime (su cui la Cassazione si è pronunciata a sfavore del lavoratore... al quale però bastava vincere su uno solo dei punti).

Sul primo punto, la Cassazione si è pronunciata come segue: "Non costituisce giusta causa o giustificato motivo di licenziamento di un dipendente l'aver reso noto all'Autorità Giudiziaria fatti di potenziale

rilevanza penale accaduti presso l'azienda in cui lavora né l'averlo fatto senza averne previamente informato i superiori gerarchici, sempre che non risulti il carattere calunnioso della denuncia o dell'esposto". "Non costituisce giusta causa o giustificato motivo di licenziamento l'aver il dipendente allegato alla denuncia o all'esposto documenti aziendali". In altre parole: non esiste un dovere di omertà del lavoratore.

Sul secondo punto la Cassazione ha scritto "nessuna norma di legge vieta che l'esercizio del potere disciplinare possa essere sollecitato (non anche provato, ovviamente) a seguito di scritti anonimi".

La notizia da Filodiritto:
- http://www.filodiritto.com/cassazione-lavoro-no-al-licenziamento-del-dipendente-perche-rivela-allautorita-fatti-dellazienda-di-rilevanza-penale-non-esiste-un-dovere-di-omerta/#.UX5gx8pWX3U

La sentenza sul sito della Cassazione:
- http://www.cortedicassazione.it/Notizie/GiurisprudenzaCivile/SezioniSemplici/SchedaNews.asp?ID=3219

****

06- Sony.it e internazionalizzazione

Inizio con un caso personale, che forse interesserà a pochi, per poi fare qualche riflessione più generale.

A marzo ho comprato un pc on-line sul sito della Sony.it. Seguo le semplici istruzioni, inserisco il "indirizzo di fatturazione", inserisco il codice fiscale, pago e non mi accorgo che il sito non mi ha mai chiesto la partita IVA. Mi arriva la fattura con partita IVA italiana e la consegno pochi giorni fa alla mia commercialista. La quale mi fa notare che, non c'è la mia partita IVA e quindi non potrà recuperare l'IVA di quell'acquisto e mi insulta. Io penso di essermi fidato di un operatore come Sony e di avere ridotto le attenzioni mentre facevo l'acquisto. Chiamo il servizio clienti e mi rispondono che sul sito c'è scritto che, se volevo la fattura, dovevo telefonare. Ho verificato e non ho trovato da nessuna parte questa dicitura. La fattura, inoltre, contrariamente a quanto previsto dalla normativa in vigore dal primo gennaio 2013, non riporta neanche il mio codice fiscale.

Ovviamente, la Sony ha solo tradotto in italiano il proprio sito di e-commerce e ha imposto SAP per la contabilità worldwide.

Pensate quello che volete di me, ma mi è venuto da pensare più in generale ai progetti di internazionalizzazione e di consolidamento dei servizi IT: molte aziende sviluppano un software, con le specifiche fornite dal personale della casa madre, e poi lo impongono a tutte le filiali nel mondo, senza prima fare uno studio serio sulle specificità, anche implicite, di ciascun Paese (se da qualche parte scrivi "fatturazione" a me risulta implicito che poi ti venga chiesta la partita IVA).

Questo succede sia ai software utilizzati internamente, che ai servizi offerti al pubblico: ho alcuni amici che hanno passato mesi a litigare con la casa madre perché il sistema di contabilità non è adeguato alla normativa italiana, ho visto molte imprese preoccupate per dei software imposti dalla casa madre che non rispettano alcuna misura prevista dalla normativa privacy, e molte case madri non rilasciano alcun documento che possa essere utilizzato dalle imprese italiane per dimostrare la correttezza degli adempimenti privacy.

La Sony ha perso un misero ma (ex) affezionato cliente; ma sarebbe bello si sviluppassero meglio i software e i servizi IT con impatto internazionale e che i responsabili di tali progetti non si improvvisassero tali.

****

07- Discussioni sul monitoraggio

Dopo il mio articolo su "Se non lo misuri non lo conosci?", in cui criticavo l'impostazione del controllo aziendale basato su misurazioni, promuovendo quello basato sul monitoraggio, ho ricevuto due commenti.

Il primo di Andra Rui che non è d'accordo con me perché "il monitoraggio è una forma meno precisa di misurazione (riporta gli andamenti nel tempo)". Io intendo come "monitoraggio" l'analisi continua dei processi e delle attività dell'impresa, di modo da arrivarne alla conoscenza profonda. Infatti i numeri nascondo spesso inefficienze e problemi e i manager passano troppa parte del proprio tempo a mettere a posto i numeri e non le inefficienze.

Come sempre, non sempre i termini sono interpretati da tutti nello stesso modo (i tecnici informatici, infatti, intendono il monitoraggio come
andamenti). Io mi scuso per l'ambiguità del mio scritto.

Fabrizio Monteleone, invece, ricorda: "il principio di indeterminazione di Heisenberg implica che ad una particella non è possibile assegnare, e quindi anche conoscere, nello stesso momento un definito valore della posizione e della velocità o quantità di moto. Tale principio implica che quanto più è precisa la misura di una grandezza tanto maggiore sarà l'errore nella misura dell'altra, per cui l'osservatore dovrà scegliere quale misura privilegiare e tarare gli strumenti di conseguenza (Wikipedia)". E aggiunge "il mio modestissimo parere di studente svogliato e poco proficuo: ciò implicherebbe che nei sistemi di gestione è inutile bearsi di moltitudini di indicatori spesso tra loro collegati o derivati...". Condivido la perplessità quando vedo alcuni auditor o consulenti richiedere di misurare sempre più cose.

Da tutto ciò, mi è venuto in mente l'esempio dell'automobile. Per guidarla abbiamo normalmente bisogno di: 2 o 3 indicatori (velocità, livello di benzina e numero di giri; possiamo aggiungere la distanza per arrivare a destinazione e l'ora), dei sistemi di allarme se qualcosa non va bene e tanta tanta attenzione alla strada, ai cartelli e al traffico (che non dobbiamo contare o misurare). Lo stesso per guidare un'azienda: pochi indicatori, dei sistemi di allarme e tanta tanta attenzione a cosa sta succedendo.

Non è farina del mio sacco: segnalo già per la seconda volta il libro "Contro il management" di Francesco Varanini.

****

08- Qualche strumento per la sicurezza informatica

Mercoledì, in occasione dell'interessantissimo DFA Open Day (ero tra gli organizzatori... perdonate l'aggettivo...), mi sono confrontato con Valerio Vertua di DFA e ho steso questo piccolo elenco di software free.

Truecrypt (www.truecrypt.org)
Serve per creare dischi, partizioni, cartelle cifrate (ma le possibilità sono ancora più ampie) e ne esistono versioni portable per pc e mac; se le persone non rinunciano ad usare una chiavetta USB per farsi i backup e, cosa ancora peggiore, la usano anche scambiare file con altre persone, allora che creino un contenitore crittografato sulla chiavetta e lo affianchino alle versioni portable di Truecrypt in modo da potervi accedere da qualsiasi computer (ed evitare che le persone con cui scambiano file accedano anche a quelli non destinati a loro).

Eraser (http://eraser.heidi.ie)
Quasi tutte le imprese dicono al proprio personale di cancellare i dati in modo sicuro, ma non forniscono loro alcun software per farlo. Eraser è free e fa benissimo il lavoro. Da impostare affinché effettui solo un passaggio di cancellazione perché è più che sufficiente e non dannoso per l'hardware. Se poi dovete anche cancellare in modo sicuro un intero disco, fa anche quello (in Windows, basta cliccarci con il tasto destro per trovare l'opzione).

Wuala (www.wuala.com)
Mi dicono che, secondo le analisi attuali, è uno dei servizi cloud di storage per backup e scambio di file più sicuro di tutti. Perché cifra sul client, perché la chiave crittografica non lascia mai il proprio device (sia esso il pc, mac, il tablet o lo smartphone) e perché non è possibile accedere al servizio cloud mediante browser (ma solo attraverso un'interfaccia java) e per tanti altri motivi. Gratis fino a 5GB.

Tails (https://tails.boum.org/)
Se usate un pc non vostro per lavoro, è meglio usare un "vostro" pc portable che poi non lasci tracce sul pc ospite. Tails occupa meno di 1GB e può essere installato su chiavetta USB o DVD. Tra le tante caratteristiche uniche di questa distribuzione live: tutto il traffico Internet avviene attraverso la rete TOR, è possibile creare una partizione cifrata per salvare i propri dati e le proprie impostazioni ed, infine, viene pulita la RAM, con tecniche wiping, quando viene spento, per qualsiasi motivo, il "vostro" pc portable. Se, per caso, sul pc ospite sono installati dei keylogger, Tails vi protegge: basta infatti usare la tastiera virtuale prevista di default.

PGP e GPG (www.gnupg.org/)
Da quando PGP è stato acquistato dalla NAI (ora è proprieta della Symantec) e non è più free, l'uso di questo strumento è diventato sempre meno popolare fra i più "diffidenti". Ma GPG è free! E ne esistono anche le versioni con interfaccia grafica per Windows (Gpg4win) e Mac (GPGTools)! Da usare per le mail riservate o i file critici da scambiare con altri.

PS: ringrazio ancora Valerio Vertua per aver ricontrollato e molto corretto il mio articolo iniziale.

****

09- Green IT

Continuo a professare a mia incompetenza nel campo del Green IT o, se vogliamo chiamarlo in italiano, dell'uso razionale dell'energia nei centri di calcolo.

Ma trovo che capirne un po' aiuti a capire meglio le aziende IT con cui parlo di gestione dei servizi IT e ISO/IEC 20000-1 o ISO 9001. Anche quando parlo di ISO/IEC 27001, mi sono trovato impelagato in dibattiti sul free cooling e amenità del genere.

Ancora una volta, mi è venuto in aiuto Franco Ferrari che mi ha segnalato delle interessanti pubblicazioni che mi hanno permesso di capire meglio alcuni termini e argomenti.

La prima è dell'ENEA e della FIRE e ha il titolo che ho appena copiato e incollato: "Uso razionale dell'energia nei centri di calcolo" e il link si trova nella pagina che segue:
- http://www.fire-italia.it/caricapagine.asp?target=studi.asp

Il secondo è dell'ENEA e ha titolo "Definizione di algoritmi e indicatori per l'efficientamento dei centri di elaborazione dati (CED)" (il report è del 2011, ma è sotto la dicitura "2008"):
- http://www.enea.it/it/Ricerca_sviluppo/ricerca-di-sistema-elettrico/Risparmio-energia-elettrica/tecnologie-per-lefficienza-energetica-nei-servizi/report

Il terzo è di CISCO, Panduit, APC e riporta alcuni elementi sul cablaggio. E' del 2007 e l'ho trovato solo al link che segue:
- www.cisco.com/web/IT/products/dc/pdf/facility_consideration_for_datacenter_ita.pdf

****

10- Sui corsi Privacy Officer

Negli ultimi giorni mi sono arrivate delle richieste per dei corsi da Privacy Officer, figura richiesta dal Regolamento Europeo sulla privacy. Tali corsi sono già offerti da alcune aziende. In casi ancora più particolari, tali corsi sono dichiarati "conformi alla ISO/IEC 17024 sulla certificazione del personale".

Mi sono sempre rifiutato di soddisfare queste richieste, così come formulate. Ovviamente, sono il primo a promuovere la formazione del personale, ma non in questi termini.

Spiego il perché:
- il Regolamento Europeo è stato appena approvato dalle Commissioni del Parlamento Europeo e quindi dovrà effettuare altri passaggi di revisione: qualsiasi cosa presente oggi nel testo potrà essere modificata o eliminata nella versione definitiva;
- l'uscita è prevista a inizio 2014 e prevederà un periodo di transizione tale da permettere alle organizzazioni di adeguarsi ai nuovi adempimenti rispetto alle normative nazionali attualmente seguite (in Italia, il Codice Privacy);
- il Regolamento potrà essere approvato in forma definitiva anche prima e potrebbe anche non essere mai approvato (ricordo che il Parlamento Europeo sarà sciolto nei primi mesi del 2014, secondo la sua normale scadenza).

Conseguenza di quanto detto sopra: il Privacy Officer potrebbe non essere più previsto nel testo definitivo o potrebbe avere compiti diversi da quelli attualmente previsti. Quindi: non trovo corretto sottindendere la necessità del corso o la sua adeguatezza rispetto ad una norma di cui non si conosce la forma finale.

Per quanto riguarda la conformità alla ISO/IEC 17024, preferisco limitarmi a copiare una dicitura vista sul web: "il corso è stato impostato in accordo allo standard UNI CEI EN ISO/IEC 17024:2004" e far notare che non si dice che il corso "è stato certificato rispetto alla ISO/IEC 17024", ma si usa una formula che da una parte non lo afferma, ma dall'altra parte lascia quel minimo di ambiguità utile ad ingannare le persone meno attente o meno preparate su questo singolo punto.

****

11- MELANI: Rapporto semestrale 2012/II

La Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI della Svizzera pubblica semestralmente un rapporto sulla situazione in Svizzera e a livello internazionale. Esso è sempre molto interessante.

L'ultimo numero, reso disponibile a inizio maggio, raccoglie notizie sugli eventi censiti nel periodo di riferimento e li commenta. In particolare segnalo i seguenti:
- attacchi agli impianti industriali (SCADA)
- il ritorno del phone phreaking
- aggiornamenti sui conflitti informatici in Medio Oriente, in particolare sui malware Flame, Gauss e Shamoon;
- attacchi alle porte elettroniche degli alberghi (la notizia dell'attacco ai sistemi aerei è del 2013, quindi in questo numero non se ne accenna);
- analisi degli app stores.

Gli articoli sono molti e molto ben fatti: sono mirabili per interesse e sintesi, visto che sono concentrati in 40 pagine.

Trovate il rapporto in questa pagina:
- http://www.melani.admin.ch/dienstleistungen/archiv/01536/index.html?lang=it

****

12- La formazione sulla sicurezza è utile?

Bruce Schneier ha scritto un articolo dicendo che la formazione degli utenti sulla sicurezza informatica non è generalmente utile:
- http://www.darkreading.com/hacked-off/on-security-awareness-training/240151108
- https://www.schneier.com/blog/archives/2013/03/security_awaren_1.html

I motivi: gli utenti non trovano benefici a breve termine per seguire le regole di sicurezza, è abbastanza raro avere problemi se non si seguono le regole di sicurezza, per adottare comportamenti corretti è necessario essere tecnologicamente abbastanza preparati.

L'unica possibilità per diffondere la sicurezza è sviluppare software sicuri o dare agli utenti dei servizi sicuri: è meglio spendere soldi per le attività di sviluppo che per la formazione (anche se un'oretta all'anno è sicuramente utile).

Confesso che do pienamente ragione a Bruce Schneier (e poca ragione al portafoglio di noi consulenti che eroghiamo anche corsi di sensibilizzazione). Questo principio me lo disse in modo chiarissimo nel 2005 Gigi Ferraris parlando dei processi di sicurezza: "se non li obblighi con la tecnologia, gli utenti non seguiranno mai i processi".