Cesare Gallotti

From: IT_Service_Management@yahoogroups.com on behalf of Cesare Gallotti [c.gallotti@quintgroup.com]
Sent: Monday, 15 September, 2008 20:08
To: IT_Service_Management@yahoogroups.com
Subject: [IT_Service_Management] Newsletter "alfa" del 15 aprile 2008
Categories: Studio

****

IT SERVICE MANGEMENT NEWS

****

Indice

****

0- Presentazione

Buongiorno a tutti,
questo è il primo numero di una newsletter tecnica con gli aggiornamenti su nuovi standard, novità in ambito legislativo e riflessioni su tutto quanto concerne l'IT Service Management e non solo.

Questo è il numero alfa, per amici.
Vi chiedo quindi di segnalare se vi interessa, se avete dei consigli per renderla più interessante, se la scelta di yahoogroups per la sua gestione è buona, se la visualizzazione è buona (txt, htm,...), se il vostro antispam è troppo severo, se vi sembra che la sicurezza di yahoogroups sia sufficiente, eccetera.

Fate conto che anche io riceverò la prima mail, assieme a voi...

Vi ricordo che ogni collaborazione (non pubblicitaria!) è benvenuta e sarà opportunamente accreditata.

Il prossimo appuntamento sarà tra un mese circa.

Vi ringrazio anticipatamente.
Cesare

****

1- IT Service Management

ITIL Compliance

Segnaliamo questo articolo che discute sui prodotti software "IT compliant"
http://www.itsmwatch.com/itil/article.php/11700_3765751_1

Dichiarare la compliance ad una best practice è certamente una scelta di marketing non supportata da ITIL stesso. Perché "essere compliant con ITIL" è una dichiarazione vaga, visto che è quasi impossibile essere aderenti a tutti i punti della best practice.

Per quanto riguarda i software "ITIL compliant", si raccomandano le solite regole: innanzitutto capire di che software si ha bisogno, poi leggere attentamente le funzionalità supportate e considerare se sono quelle effettivamente necessarie all'organizzazione, infine valutare come questo software potrà essere integrato nei processi in essere e a quali esigenze future potrà venire incontro. Abbiamo già visto troppi prodotti acquistati dalle aziende e mai installati o mal utilizzati (con perdite di operatività) perché inadatti all'organizzazione.

Per quanto riguarda un'organizzazione "ITIL compliant", si ripetono gli stessi discorsi relativi alla "compliance alla ISO/IEC 17799": si tratta di un'autodichiarazione e riflette una situazione quasi impossibile da attuare, visto che una best practice, per sua natura, riporta anche più modalità per soddisfare la stessa esigenza. Le persone possono essere certificate per le competenze in merito a ITIL, non le aziende. Per questo c'è la ISO/IEC 20000.

****

2- Nuovi documenti

BS 25777 Code of practice for ICT continuity

Il BSI ha appena sottoposto a commento pubblico il draft della BS 25777 (Code of practice for ICT continuity).
http://drafts.bsigroup.com/?i=188&j=6323603&e=c.gallotti@quintgroup.com&l=546452_HTML&u=47920098&mid=60187&jb=0&WT.mc_id=

E' certo che il BSI sta investendo molto in questo campo. Dopo il recepimento della BS 7799 come ISO/IEC 27001 e ISO/IEC 27002, ora sta lanciando una serie di standard dedicati alla business continuity.

C'è da chiedersi come differenziare questa BS 25777 dalla BS 25999-1 (Code of practice for business continuity management), visto che questa seconda può, per sua natura, essere applicata a tutte le tipologie di business, inclusa l'erogazione di servizi IT. Ad una lettura più approfondita, si potrà valutare se l'iniziativa è interessante o rappresenta un altro tassello nella proliferazione degli standard.

NIST Performance Measurement Guide for Information Security

Il NIST scrive le migliori guide che ci siano sulla sicurezza informatica. Anche questa prima revisione della SP 800-55 non fa eccezione, soprattutto se la confrontiamo con il draft della ISO/IEC 27004, che risulta essere molto meno pragmatico.

Consigliata a quanti stanno riflettendo sul requisito 4.2.2.d della ISO/IEC 27001 ("Definire come misurare l'efficacia dei controlli o di gruppi di controlli selezionati") e a quanti vogliono misurare l'efficacia dei controlli di sicurezza.

http://csrc.nist.gov/publications/PubsSPs.html#800-55_Rev1

A quanti sono interessati all'argomento, poi, ricordiamo il lavoro fatto dal Clusif (Club de la Sécurité de l'Information Français)dal 2001 sugli indicatori di sicurezza. Il documento è in francese ed è scaricabile dal sito www.clusif.asso.fr.

ISO/IEC 10779:2008 sull'accessibilità alle tecnologie informatiche

La ISO ha pubblicato questo standard con le linee guida per lo sviluppo delle

apparecchiature da ufficio, incluse stampanti e tastiere. Da considerare per tutte le attività di desktop management quando sono coinvolte persone anziani o disabili..

http://www.iso.org/iso/pressrelease.htm?refid=Ref1148

****

3- Sicurezza delle informazioni

Pubblicata la ISO/IEC 27005:2008

Pubblicata la norma della serie 27000 dedicata al "Information security risk management" e che sostituisce le parti 3 e 4 della ISO/IEC TR 13335. Interessante lettura per chi vuole avvicinarsi ai modelli di risk assessment utilizzati per la sicurezza delle informazioni.

Attacchi dall'interno o dall'esterno

Su Crypto-gram del 15 giugno 2008, viene segnalata un'altra puntata del dibattito "sono più numerosi gli attacchi dall'interno o dall'esterno?". Dibattito inutile, come sottolinea Bruce Schneier. E infatti: sappiamo bene che siamo oggetti di attacchi interni ed esterni e che dobbiamo proteggerci da essi; che senso ha, allora, fare una classifica?

In alcuni momenti siamo portati a pensare con più preoccupazione agli attacchi di origine interna, visto che mediamente sono più dannosi di quelli di origine esterna, come dimostrano i casi di Societé Générale o il caso delle cartelle pazze (qualche errore di qualche programmatore). In altri momenti, i giornali riportano con maggiore enfasi i casi di attacchi dall'esterno, con danni anche ingenti, come dimostrano alcune notizie relative alla compromissione di database di carte di credito e alcuni virus e worm del recente passato

Tutto ciò dimostra che dobbiamo considerare tutte le origini di attacco e che, per un corretto dimensionamento del sistema di sicurezza, sarebbe più utile valutare le motivazioni degli attaccanti e le possibilità che hanno di riuscire nel loro intento. Ma questo è un lavoro che va fatto realtà per realtà (con il risk assessment) e non può essere utilizzato per fare statistiche da pubblicare sui giornali.

http://www.pcworld.com/businesscenter/article/147098/insider_threat_exaggerated_study_says_.html

La percezione dei rischi

Altro articolo molto interessante di Bruce Schneier su come sono percepiti i rischi, secondo quanto stabilito da alcuni studi.

In breve: le persone, mediamente, preferiscono un piccolo guadagno sicuro, rispetto ad un grosso guadano possibile ma non sicuro (come dimostra la popolarità degli investimenti a basso rischio); dall'altra parte, preferiscono correre il rischio di una grossa perdita, piuttosto che subire una piccola perdita sicura (come dimostra lo scarso successo delle assicurazioni).

Nell'ambito della qualità e della sicurezza, tutto ciò vuol dire che è difficile convincere un'azienda a subire una piccola perdita sicura (costo dei consulenti, costo di progetto, costo di nuovi strumenti e costi di formazione), piuttosto che accettare un possibile grosso rischio (perdita di clienti perché insoddisfatti o

perché l'azienda ha subito troppi incidenti di sicurezza).

http://www.cio.com/article/367913/How_to_Sell_Security

****

4- Novità legali

Semplificazione privacy

E' stato approvato e pubblicato il Decreto Legge 112 del 2008, convertito dalla Legge 133/2008.
Viene quindi abolito il Documento Programmatico per la Sicurezza per alcune azienda, che poteva essere risolto con documenti di 15-20 pagine, come si può dedurre dalla guida del Garante.

Certamente, come i casi di cronaca insegnano, non è un documento a costituire la parte più complessa (avere una Dichiarazione di impatto aziendale o l'Analisi dei rischi dei lavoratori, o il DPS), ma mettere in atto le misure di sicurezza (ambientale, per i lavoratori, per la privacy) efficaci.

In particolare, l'articolo 29:
a) sopprime l'obbligo di tenere un documento programmatico sulla sicurezza in tutti i casi in cui vengano trattati solo dati personali e in cui l'unico eventuale dato sensibile sia costituito dalla malattia dei dipendenti senza indicazione della diagnosi;

b) prevede che le piccole e medie imprese possano redigere un documento programmatico sulla sicurezza a carattere semplificato come dovrà essere meglio esplicitato entro due mesi dalla conversione in Legge del DL 112 (avvenuto il 6 agosto 2008 con la Legge 133);

c) semplifica la notifica al Garante del trattamento di determinati dati personali, riducendo il numero di informazioni richieste, in linea con quanto previsto dalla disciplina comunitaria;

d) elimina ogni riferimento alla firma digitale nella sottoscrizione della notificazione.

http://www.parlamento.it/parlam/leggi/decreti/08112d.htm

Garante della Privacy - Necessità di prevedere tempi limite di conservazione dei dati

Il Garante per la protezione dei dati personali si è espresso in merito alla necessità che il titolare del trattamento preveda tempi limite di conservazione dei dati personali degli interessati.

Secondo il Garante, con riguardo sia alle anagrafiche della clientela che non effettua alcun acquisto, e rispetto ai quali "la società non ha stabilito un tempo di conservazione", sia ai dati relativi agli acquirenti, il titolare deve identificare i tempi massimi di conservazione dei dati trattati alla luce delle finalità in concreto perseguite (ad esempio, prenotazione dell'incontro dimostrativo, conclusione del contratto di vendita, gestione dell'eventuale sostituzione dei prodotti in garanzia), fatta salva la sussistenza di obblighi di legge (ad esempio, in relazione alla tenuta di scritture contabili: art. 2220 Codice Civile).

Il Garante ha aggiunto che "in relazione ai dati personali riferiti ai soggetti che

si siano resi acquirenti, potranno essere conservati a tempo indeterminato i dati relativi alla clientela a vantaggio della quale la società accordi una garanzia con durata illimitata; diversamente, i dati dovranno essere cancellati (o trattati in forma anonima) ove la loro conservazione non risulti altrimenti giustificata (art. 11, comma 1, lett. e), del Codice)" mentre "in relazione ai dati personali riferiti a soggetti che non si siano resi acquirenti, poi, non risulta giustificata la conservazione di dati personali per un tempo ulteriore rispetto a quello necessario alla prenotazione ed effettuazione dell'incontro dimostrativo; ciò, salvo che sia acquisito validamente il consenso informato degli interessati per una successiva attività di promozione commerciale o ricerca di mercato".

Nel caso di specie: "i dati relativi ai clienti [che hanno effettuato un acquisto] vengono conservati dall'azienda a tempo indeterminato, atteso che gli stessi hanno diritto, secondo le condizioni contrattuali, a una garanzia a vita con riferimento alle pentole vendute dalla società". Tali informazioni sono trattate, però, anche per effettuare attività di telemarketing. La società, inoltre, "non ha stabilito un tempo di conservazione" anche per i dati di chi, pur avendo concordato un incontro con i responsabili di zona, non abbia proceduto ad alcun acquisto. Tali informazioni sono utilizzate dalla società (nel cui data base risultano circa 400.000 anagrafiche) per contattare questa parte della clientela al fine di comprendere "se il mancato acquisto sia dipeso dal prodotto o dall'atteggiamento del venditore"".

(Garante per la protezione dei dati personali, Provvedimento 19 maggio 2008: conservazione dati a tempo limitato).
http://www.filodiritto.com/index.php?azione=visualizza&iddoc=1128

Decreto Legislativo 109/2008 sulla conservazione dei dati nell'ambito della fornitura di servizi di comunicazione elettronica

E' stato pubblicato il Decreto Legislativo n. 109 del 30 maggio 2008, che recepisce la direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione.

Le categorie di dati da conservare per gli operatori di telefonia e di comunicazione elettronica sono:
- i dati necessari per rintracciare e identificare la fonte di una comunicazione;
- i dati necessari per rintracciare e identificare la destinazione di una comunicazione;
- i dati necessari per determinare la data, l'ora e la durata di una comunicazione;
- i dati necessari per determinare il tipo di comunicazione;
- i dati necessari per determinare le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature;

- i dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile.

http://www.parlamento.it/parlam/leggi/deleghe/08109dl.htm

_____
Cesare Gallotti
Quint Wellington Redwood Group
Via Vincenzo Monti 8
20123 Milano (Italy)

http://www.quintgroup.com
+39.02.46.71.25.32 (Office)
+39.02.48.01.32.33 (Fax)
+39.349.669.77.23 (Mobile)
c.gallotti@quintgroup.com

====== D A R E T O C H A L L E N G E ======