Cesare Gallotti

From: it_service_management-news-bounces@mailman.cesaregallotti.it on behalf of IT Service Management NewsLetter [it_service_management-news@mailman.cesaregallotti.it]

Sent: Wednesday, 05 August, 2009 13:36

To: it_service_management-news@mailman.cesaregallotti.it

Subject: [IT Service Management] Newsletter del 5 agosto 2009 (la prossima:15 settembre 2009)

Attachments: ATT00015.txt

****
IT SERVICE MANAGEMENT NEWS
****

Newsletter mensile con novità in materia di sicurezza delle informazioni, IT Service Management, Qualità.
E' possibile dare il proprio contributo e diffonderla a chiunque secondo la licenza http://creativecommons.org/licenses/by-nc/2.5/it/.
E' possibile iscriversi, disiscriversi e modificare le proprie opzioni, oltre a vedere l'informativa sul trattamento dei dati personali, all'indirizzo
http://mailman.ipnext.it/mailman/listinfo/it_service_management-news

****
Indice

****
01- Novità legali (231 e Diritto d'autore)

Decreto Legislativo 231/2001

Come preannunciato, sono state apportate modifiche al Dlgs 231/2001.

In particolare:
- è stata approvata la Legge 94 del 2009 "sulla Sicurezza" che introduce nel 231 l'Art. 24-ter "Delitti di criminalità organizzata"
- è stata approvata la Legge 99 del 2009 che introduce nel 231 gli articoli 25-bis.1 e 25-novies sul diritto di autore.

La mia versione consolidata del Dlgs:
http://www.cesaregallotti.it/normativa/Dgls_231/2001_Dlgs_231.htm
(se ci sono errori, avvisate!)

Dettagli dalla newsletter Insight 26 del luglio 2009 di Protiviti, che dovrà essere disponibile alla pagina http://www.protiviti.it/it-IT/Insights/Newsletters/Insight%20-%20Newsletter-di-Protiviti-Italia/Pagine/default.aspx

Purtroppo continuo a trovare articoli di interpretazione dei reati, ma nessuno sufficientemente approfondito sulle possibili misure preventive. D'altra parte, se la teoria dice che "se c'è reato, il modello organizzativo è inefficace", è anche vero che troppi comportamenti dei "subordinati" sono incontrollabili dagli "organi apicali".

Forse ancora pochi processi sono stati condotti su questo tema.

Diritto d'autore

Interlex annuncia che è stato "finalmente ricostruito il testo vigente della legge sul diritto d'autore".

http://www.interlex.it/testi/l41_633.htm

Ne approfitto per farvi notare che ho aggiunto un link a inizio lettera per garantirmi i diritti d'autore. Il progetto Creative Commons (http://creativecommons.org) non è una novità, ma se avete interesse per la materia, è molto interessante leggere il sito.

****

02- Documenti tecnici - Novità (ISO 27799 e NIST)

ISO 27799

Max Cottafavi di Reply mi ha segnalato l'esistenza della ISO 27799:2008 "Health Informatics - Information Security management in health using ISO/IEC 27002".

Questa norma (non certificabile!) è molto interessante perché propone alcuni paragrafi non generali, ma specifici per il settore sanitario.

In particolare, illustra con buon dettaglio gli asset e le minacce specifiche del settore. Nell'allegato A sono descritte 25 minacce.
Nell'allegato B, inoltre, viene proposto un riassunto delle attività e dei documenti necessari al funzionamento di un Sistema di Gestione per la Sicurezza delle Informazioni conforme alla ISO/IEC 27001.

Ci tengo poi a copiare una frase significativa, applicabile a tutti: "Un errore comune è dichiarare la propria conformità alla ISO/IEC 27002 sulla base della compilazione di check list. Per essere veramente conformi, le organizzazioni devono essere capaci di dimostrare un ISMS operativo, con incluso un processo di auditing interno". Aggiungo che la "conformità alla 27002" è una frase con nessun senso proprio per quanto appena detto; una dichiarazione di conformità (auto-dichiarazione o certificazione di terze parti che sia) può essere esperessa solo a fronte della ISO/IEC 27001.

Interessanti sono anche le riflessioni in merito alle connessioni tra sicurezza delle informazioni e information governance. Tema caro in alcuni ambiti, ma non in tutti.

In conclusione, non mi è possibile citare tutto il documento, ma trovo che sia un'ottima lettura. Un solo difetto: benché tratti di "sicurezza delle informazioni", il titolo segnala solo un approccio a livello informatico.

NIST SP 800-53

Il NIST annuncia la pubblicazione della rev 3 della Special Publication 800-53 "Recommended Security Controls for Federal Information Systems and Organizations"
http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf

****

03- Analisi del rischio: approfondite o no?

Da CRYPTO-GRAM del 15 luglio vi segnalo un bell'articolo di Bruce Schneier
http://www.schneier.com/blog/archives/2009/06/imagining_threa.html

Schneier discute in merito ad un articolo di Magne Jørgensen
http://simula.no/research/engineering/publications/Simula.SE.621

L'articolo presenta i risultati di una ricerca sul risk assessment di progetti software condotti da alcuni gruppi di lavoro.

Sembra che i gruppi a cui è stato chiesto di svolgere un risk assessment "veloce" hanno ottenuto risultati più pessimistici di quelli a cui è stato chiesto di svolgere un risk assessment approfondito.

La cosa è molto interessante, visto che io, quando si parla di sicurezza delle informazioni, sono fautore del "veloce" e ricevo numero contestazioni basate sul fatto che un'accurata analisi è fondamentale per ottenere risultati precisi e utilizzabili. Posto che di utilizzabilità nelle analisi "approfondite" non ne ho mai vista molta (zero progetti di sicurezza scaturiti dal risk assessment, altri progetti di sicurezza scaturiti da altre fonti non ben

definite), qui sembra che alla fine il metodo "veloce" faccia emergere i problemi con maggiore evidenza. Che è quello che ci si aspetta da un'analisi del rischio.

****

04- Sul numero di persone di un'organizzazione

Sempre su CRYPTO-GRAM del 15 luglio si trova una riflessione su come il numero di persone di un'organizzazione debba essere un input nella scelta dei controlli di sicurezza da adottare.
http://www.schneier.com/blog/archives/2009/07/security_group.html

In pochissime parole, se un'azienda supera le 150 persone, allora è necessario introdurre un sistema di badges: oltre quel numero è impossibile che ciascuno riconosca tutti i propri colleghi e, quindi, riconosca gli intrusi.

Io sapevo (ma non ricordo più da dove l'ho letto) che i numeri critici erano 8, 80 e 120: oltre gli 8 non è più possibile sapere esattamente che lavoro stiano facendo gli altri, oltre gli 80 non si associano più le facce con i nomi, oltre i 150 non si riconoscono più tutti i colleghi.

Questo fa sì che, a queste soglie, si hanno dei momenti di malumore nel personale ("ah, un tempo riuscivo a stare dietro a tutti gli aspetti dell'azienda", "ah, un tempo qui ci si conosceva tutti") e di difficoltà di controllo da parte del management. Con la conseguenza che è necessario cambiare il modello di gestione o, se vogliamo parlare in termini ISO, i sistemi di gestione (della qualità, della sicurezza, dei servizi IT, eccetera).

L'effetto di malumore nel personale, va detto, non è un aspetto da sottovalutare: è proprio in questi momenti che si ha un aumento del turn over, con tutte le conseguenze del caso.

_____

Cesare Gallotti
Ripa Ticinese 75
20143 Milano (Italy)
+39.02.58.10.04.21 (Office)
+39.349.669.77.23 (Mobile)
www.cesaregallotti.it
cesaregallotti@cesaregallotti.it