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: Monday, 16 February, 2009 17:03

To: Mailing list

Subject: [IT Service Management] Newsletter del 16 febbraio 2009

Attachments: ATT00190.txt

****
IT SERVICE MANGEMENT NEWS
****

Newsletter mensile con novità in materia di sicurezza delle informazioni, IT Service Management, Qualità.
E' possibile diffonderla a chiunque; è 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

****
1- Sicurezza: attacchi
(da SANS NewsBites Vol. 11 Num. 9 e 11)

Questo mese ho visto tre interessanti attacchi.

Il primo è un attacco al database di Monster.com da cui hanno rubato userid e password degli utenti. Non sono dati dettagli sulla vulnerabilità sfruttata.
http://fcw.com/Articles/2009/02/02/Government-jobs-site-is-hacked.aspx

Il secondo è un attacco al Kaspersky Database, sottoposto ad una SQL Injection via sito web. Tiro a indovinare: il sito è stato testato solo per le funzionalità e non per verificare la presenza di vulnerabilità note.
Non credo sia il caso di discutere delle cause di queste brutte abitudini, ma ricordo a tutti che per lo sviluppo web sono disponibili le linee guida dell'OWASP (www.owasp.org). Da leggere!
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127640&source=rss_topic17

Il terzo riguarda un virus che ha colpito il tribunale di Houston (Texas, USA). Il tribunale è rimasto chiuso per almeno 3 giorni. Pare che il "colpevole" sia il worm Downadup, per il quale era disponibile la patch da ottobre 2008.
La discussione sul "patchare-subito/aspettare-a-patchare" è sempre viva. Ma i rischi sono questi ed è il caso di conoscerli.
http://www.chron.com/disp/story.mpl/front/6250411.html

****
2- Business Continuity: rilasciata la BS 25777

Il BSI ha rilasciato la BS 25777 "Code of practice for ICT continuity management".

Per me è inutile (perché è un "Code of practice", perché la linea guida del NIST è migliore e gratuita) e l'avevo già detto.

Se proprio ci tenete a comprarla: www.bsigroup.com/bs25777

****

3- Sicurezza: Patch Management
(dalla Newsletter del Clusit del 31 gennaio 2009)

Vi segnalo l'interessante guida per il patch management per i sistemi di controllo (sistemi utilizzati in ambito industriale, molte volte basati su tecnologia Wintel).

La cosa è meno banale di quello che potrebbe sembrare a prima vista, dato che si tratta di sistemi in funzione 24/7/365 e, si sa, il patching è un'attività rischiosa.

"Recomended Practice for Patch Management of Control Systems"
http://csrp.inl.gov/Documents/PatchManagementRecommendedPractice_Final.pdf del US-CERT e Department of Homeland Security USA.

Inoltre, il Clusit ci ricorda anche il Quaderno Clusit su "Introduzione alla protezione di reti e sistemi di automazione e controllo (PLC, SCADA, DCS, ecc.)" disponibile su www.clusit.it/download

****

4- Convego AIEA: gli atti

Gli atti del XXII Convegno di Parma dell'AIEA (Associazione Italiana IS Auditors) sono disponibili sul sito.
http://www.aiea.it/html/5_giugno_2008.html
http://www.aiea.it/html/6_giugno_2008.html

****

5- Sicurezza: Metodologia VERA

Ho pubblicato sul mio sito la metodologia VERA (Very Easy Risk Assessment).

In realtà non si tratta di una metodologia completa: le modalità di raccolta dei dati non sono descritte e sarà possibile scegliere il metodo preferito prendendo spunto dalle modalità collaborative di Octave (www.cert.org/octave) o basate su questionari del Mehari (www.clusif.asso.fr) o su assessment condotto da personale specializzato.

Alcune considerazioni:
1- a differenza di quasi tutte le metodologie in circolazione, è basata sui servizi e non sulle componenti IT e non-IT; questa è una metodologia più orientata verso il business e potrebbe essere utile per sviluppare un ISMS (SGSI, in italiano). Metodologie utili per analisi a livello di componenti potranno essere la FTA (Fault Tree Analysis) o la FMEA/FMECA
2- richiede un discreto livello di competenza da parte di chi conduce l'analisi: non ci sono questionari "a prova di junior"
3- presenta la correlazione tra minacce e controlli, cosa importante per capire il perché si implementa un certo controllo.

www.cesaregallotti.it/art_pres/2009-Vera.xls

Confesso che vorrei scrivere meglio alcune riflessioni sulle metodologie in uso e sul perché, nella maggior parte dei casi, non mi piacciono. Ma questa è solo una buona intenzione.

****

6- Privacy: chi può semplificare?

Max Cottafavi (Spike Replay) mi ha fatto notare che non è facile capire quali sono i soggetti che possono

semplificare gli adempimenti richiesti dal Codice Privacy.

Innanzitutto, di cosa si parla?
- dell'articolo 34 comma 1-bis del Dlgs 196/2003 (Codice Privacy), modificato dal DL 112/2008 del 25 giugno 2008 convertito in Legge dalla L 133/2008 (http://www.cesaregallotti.it/normativa/privacy/2003_Dlgs_196.htm)
- provvedimento del Garante numero 1526724 del 19 giugno 2008 (http://www.garanteprivacy.it/garante/doc.jsp?ID=1526724)
- provvedimento del Garante numero 1571218 del 27 novembre 2008 (http://www.garanteprivacy.it/garante/doc.jsp?ID=1571218)

I provvedimenti indicano come "soggetti che possono semplificare" chi soddisfa le condizioni a) e b) riportate dal provvedimento del 27 novembre:
- a) utilizzano dati personali non sensibili o che trattano come unici dati sensibili riferiti ai propri dipendenti e collaboratori anche a progetto quelli costituiti dallo stato di salute o malattia senza indicazione della relativa diagnosi, ovvero dall'adesione a organizzazioni sindacali o a carattere sindacale;
- b) trattano dati personali unicamente per correnti finalità amministrative e contabili, in particolare presso liberi professionisti, artigiani e piccole e medie imprese (cfr. art. 2083 cod. civ. e d.m. 18 aprile 2005, recante adeguamento alla disciplina comunitaria dei criteri di individuazione di piccole e medie imprese, pubblicato nella Gazzetta Ufficiale 12 ottobre 2005, n. 238).

Per quanto riguarda il DM 18 aprile 2005, si può semplificare dicendo che il Provvedimento del Garante indica aziende PMI, ossia con meno di 250 addetti e meno di 50 milioni di Euro all'anno di fatturato. (http://gazzette.comune.jesi.an.it/2005/238/5.htm)

Il dubbio è che il testo non è chiaro: si tratta di soggetti che soddisfano tutte e due le caratteristiche riportate (a AND b) oppure è sufficiente una sola delle due (a OR b).

Io opterei per un "AND", perché ogni impresa con almeno un dipendente tratta sia i dati di cui al punto a) sia quelli del punto b) per la gestione dei clienti. Nel caso l'impresa non abbia dipendenti, allora potrebbe rientrare nella categoria di azienda che "utilizza dati personali non sensibili".

Si osserva che rimarebbe una "zona grigia" di interpretazione: aziende non-PMI che trattano dati personali dei clienti per scopi solo amministrativi e contabili. Pensiamo a qualche azienda manifatturiera o di distribuzione di prodotti o qualche studio di consulenza organizzativa o di architettura.

A questo punto, nel dubbio, direi che sarebbe meglio che non semplificassero.

Qualche considerazione sulle misure "semplificate":
- il DPS può essere un documento di 10-15 pagine, anche semplice. Ci sono in giro DPS di centinaia di pagine, spropositati per le realtà a cui si riferiscono. E' il caso di smettere di vedere il DPS come un adempimento "complicato e dispendioso", di eccedere in zelo, di aver paura del Garante perché il DPS potrebbe non essere perfetto, di interpretare il dispositivo di legge oltre il suo dettato, oppure, di affidarsi a consulenti incompetenti.
- le altre misure "tecniche" dovrebbero essere applicate ai soli dati sensibili, ossia ai pc e agli archivi dell'ufficio del personale, oltre che agli informatici; per le imprese della "zona grigia" si tratterebbe di poche persone
- le altre misure "procedurali" richiedono istruzioni scritte anziché orali, facilmente componibili in 2 o 3 pagine.
- tra le misure "semplificate" non viene richiesto ai fornitori di IT "una descrizione scritta dell'intervento effettuato", cosa che invece sarebbe auspicabile, viste poi le esperienze di cui ho già parlato a dicembre e gennaio.

Forse io ho esagerato in semplicità in alcuni casi?
Non mi pare, ma accetto controdeduzioni che pubblicherò.

Per chi non si accontentasse del mio parere, vi segnalo l'articolo di Paolo Ricchiuto su Interlex. Mi pare che lui interpreti il dispositivo con la "OR", ma non ne spiega le ragioni. Per il resto, si tratta di un articolo interessante che fa riferimento anche ad ulteriori articoli interessanti sempre su Interlex.
http://www.interlex.it/675/ricchiu30.htm

****

7- Privacy: altri provvedimenti

ISP e TLC: conservazione dei dati di traffico
A gennaio mi ero perso il Provvedimento del Garante del 17/01/2008 sulla conservazione dei dati di traffico

telefonico e telematico.
http://www.garanteprivacy.it/garante/doc.jsp?ID=1482111

Sanzioni
Il Decreto Legge 207/2008, all'articolo 44, modifica alcuni articoli del Codice Privacy in materia di sanzioni non è ancora stato promulgato.
Trovate il DL sul sito del Parlamento: http://www.parlamento.it/parlam/leggi/decreti/08207d.htm

Piano ispettivo del Garante
Come indicato dalla Newsletter del Garante del 12 febbraio 2009, è stato varato il piano ispettivo per i primi sei mesi. I tre settori maggiormente interessati saranno: sistema informativo del fisco, banche, sistema sanitario.

****

8- Altre novità normative

Decreto 185/2008 "Anti-crisi"
Il decreto, con le novità in materia di Posta Elettronica Certificata e archiviazione ottica non è stato ancora convertito in Legge.

Normativa applicabile alla crittografia
Questo sito presenta un'analisi delle diverse normative applicabili alla crittografia nel Mondo. Utile per chi deve gestire questo aspetto con partner, filiali o conoscenti all'estero.
http://rechten.uvt.nl/koops/cryptolaw/

****

9- Presentazioni ISO/IEC 20000 e 27000

Il 23 gennaio ho presentato la ISO/IEC 20000 e le norme della serie ISO/IEC 27000 per la Exin.

Ringrazio la Exin per l'opportunità.

Le presentazioni le trovate su:
http://www.cesaregallotti.it/art_pres/2009-Exin-ISOIEC20000.pdf
http://www.cesaregallotti.it/art_pres/2009-Exin-ISOIEC27002.pdf

_____

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