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: Saturday, 16 May, 2009 15:20

To: Mailing list

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

Attachments: ATT00014.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
<http://mailman.ipnext.it/mailman/listinfo/it_service_management-news>

****
Indice

****
01- Metodologie di Risk Assessment

In questo ultimo mese mi sono imbattuto in qualche metodologia di interesse.

Magerit
Si trova su http://www.csi.map.es/csi/pg5m20.htm
Sul sito www.sgsi.it si trova la traduzione del primo libro ad opera di Fabio Guasconi.

Non ho avuto modo di studiare il metodo nella sua interezza, ma ho trovato molto interessante il catalogo (libro II) con minacce, tipologie di asset, tabelle di correlazione, scale di valutazione, eccetera.

E' possibile scaricarsi il software Pilar, seguendo i link. Anche in italiano, sempre da www.sgsi.it (grande Fabio!)

I miei contatti spagnoli dicono che in Spagna è molto usata. Spesso male, ma questo è il solito problema che affligge tutte le metodologie.

Ringrazio della segnalazione Alessandro Rodolfi di DataConSec, anche se ne avevo avuto notizia qualche tempo fa da parte di Fabio Guasconi, ma l'avevo colpevolmente ignorata.

Modulo
Dinesh O Bareja, della società indiana SM e che ho conosciuto su LinkedIn, mi ha segnalato Modulo:
http://www.modulo.com/products/modulo-risk-manager-overview.jsp

Da quello che capisco non sembra che sia disponibile al pubblico e le specifiche sono riportate solo sul sito o sulle brochures in pdf. Ma ho capito che i controlli di sicurezza, come in Defender Manager, sono legati alle tecnologie, cosa che può rendere il prodotto poco flessibile.

Fair
Sempre Dinesh O Bareja mi segnala FAIR (Factor Analysis of Information Risk)
http://fairwiki.riskmanagementinsight.com/

Potete scaricare il documento da
http://www.riskmanagementinsight.com/media/docs/FAIR_introduction.pdf

Mi pare interessante. Anche il blog ad esso collegato con varie riflessioni.

****
02- Windows 7

E' uscito e la Microsoft rende disponibile la versione beta fino a fine luglio. Attenzione che a marzo 2010 si metterà a fare le bizze se non avete comprato la licenza (o fatto qualche magheggio).

Potete scaricare Windows 7 da www.microsoft.com
Ho trovato un articolo che spiega come fare il dual boot Vista-Win7
http://www.techspot.com/guides/143-dual-boot-windows7/

Non l'ho ancora provato, ma da Sans Newsbyte scopro che Win7 ha mantenuto la cattiva abitudine di nascondere di default le estensioni dei files (ricordate Iloveyou?), ma non ha più l'AutoPlay attivo.

Le prime vulnerabilità "serie" sono già state trovate: http://support.microsoft.com/kb/970789
Tra bachi e polemiche, cominciamo bene...

Raccomando di fare il backup prima degli esperimenti: io, per il mio ultimo esperimento, non lo feci e sto ancora pagando le conseguenza, da bravo ciabattino con le scarpe rotte :-(

****
03- Data retention

Ho scoperto recentemente che il termine "data retention" viene usato in alcuni ambiti per i soli dati di traffico telefonico e telematico, esclusi i contenuti. Io gli davo un significato più ampio, ma tant'è.

Questo argomento è trattato dalla Legge 155/2005 (già DL 144/2005 o Legge Pisanu), dal Decreto del Ministero dell'Interno del 16 agosto 2005, dal Dlgs 109/2008 di attuazione della Direttiva 2006/24/CE, nonché dalla Legge 48/2008. Tutto ciò come misure di contrasto al terrorismo.

Queste normative, in poche e imprecise parole, richiedono che i fornitori di servizi informatici, telematici o di telecomunicazioni devono conservare una serie di dati sul chiamante e sul ricevente di telefonate, nonché sugli indirizzi IP che hanno originato "conversazioni" informatiche. A tutto ciò si collegano disposizioni del Garante sui tempi di conservazione di tali dati che rendono le cose ancora più complicate di quelle che possono essere dopo essere state modificate e rimodificate da 4 dispositivi di legge.

Sul web ci sono diversi articoli di critica e interpretazione.

La notizia che leggo da NewsByte è che gli ISP Svedesi si stanno rifiutando di conservare gli indirizzi IP come richiesto dalle normative.

http://www.computerworld.com/action/article.do?
command=viewArticleBasic&articleId=9132324&source=rss_null17
http://arstechnica.com/telecom/news/2009/04/second-swedish-ip-decides-to-nuke-ip-address-logs.ars

****
04- Privacy e Amministratori di Sistema

Propongo un piccolo elenco dei dubbi sul Provvedimento del Garante per la Protezione dei Dati Personali del 27 novembre 2008 sugli Amministratori di Sistema.

Ho avuto conferma che i dubbi sono gli stessi in tutti gli ambienti, dalle grandi alle piccole imprese, da tecnici a avvocati.

Elenco:
- la definizione di Amministratore di Sistema è lacunosa
- non si capisce bene a che livello raccogliere gli "access log" (solo Sistemi Operativi, anche applicativi, db?)
- la difficoltà di allegare l'elenco degli Amministratori di Sistema (in costante cambiamento) al DPS (di aggiornamento annuale)
- nel caso di outsourcer, la difficoltà (e la pericolosità) del rendere disponibili ai clienti l'elenco aggiornato degli Amministratori di Sistema
- la non chiarezza su cosa si intenda per "Verifica dell'operato" degli Amministratori di Sistema: audit? software di event correlation e di segnalazione anomalie? analisi dei soli access log? altro?

Da più parti c'è la voce che il Garante chiarirà i vari punti a fine giugno e prorogherà di almeno altri 6 mesi l'adozione del Provvedimento.

****

05- Computer forensics

In questo periodo mi sono occupato di computer forensics, grazie anche al Corso di perfezionamento post-laurea in computer forensics e investigazioni digitali organizzato dall'Università degli Studi di Milano.

Vi segnalo quindi qualche sito, nel caso foste interessati alla materia:
- http://www.iisfa.it/ del capitolo italiano dell'International Information Systems Forensics Association
- www.marcomattiucci.it, pieno di cose interessanti
- http://www.dfrws.org/, della conferenza internazionale di digital forensics, con molte presentazioni interessanti
- www.accessdata.com, del produttore del prodotto commerciale FTK (ma se andate in Support - Previous Releases potete scaricare qualcosa con cui fare esperimenti)

****

06- Convegno a Pescara il 19 e 20 giugno

I giuristi informatici italiani presentano << Internet e diritto - Il futuro dell'informatica giuridica e del diritto delle nuove tecnologie in Italia: prospettive de jure condendo e urgenza di una "ricostruzione normativa">>

Questo è un Congresso Nazionale di benerficenza per gli studenti abruzzesi e si terrà il 19 e 20 giugno 2009 c/o Università degli Studi "G. d'Annunzio" di Chieti-Pescara, Viale Pindaro 42 – Pescara

Il sito Web è http://donaunnetbook.org.

Partecipate!

****

07- BS 25777:2008 - Information and communication technology continuity management

Questo code of practice è stato pubblicato nel novembre del 2008. Mi scuso per la tardiva comunicazione.

E' un "code of practice", quindi è una norma non certificabile, a differenza della BS 25999-2.

****

08- Certificati ITIL

Finalmente la Exin ha avviato il registro consultabile da web delle persone certificate ITIL. Iniziativa importante per ridurre il proliferare di certificazioni non accreditate.

Potete consultarlo da: http://www.itil-officialsite.com/ITILEISCRSquery.asp

Le persone certificate non sono automaticamente inserite nel registro, ma ne devono far richiesta. Quindi, se non trovate qualcuno, non vuol dire che questi non è certificato, ma solo che non ha fatto richiesta o sono ancora in corso le pratiche di verifica di Exin (2 settimane circa).

****

09- Lavori ISO/IEC 27001 e 27002
(di Fabio Guasconi)

Il 38° meeting del sottocomitato 27 (SC27) si è aperto nella cornice della calda primavera pechinese. Il gruppo di lavoro 1 (WG1), orientato ai Sistemi per la Gestione della Sicurezza delle Informazioni continua a registrare un incremento di partecipazione costante, includendo ora oltre 30 delegazioni nazionali attive.

Revisione 27001 e 27002
Sicuramente tra queste la prima parola spetta all'attesa revisione congiunta di ISO/IEC 27001 e 27002. In questo ambito i contributi (tra cui anche quello nazionale, finalmente!) sono stati decisamente consistenti, andando anche a proporre cambiamenti di struttura sostanziali dello standard. A questo proposito, per esempio, il primo working draft della nuova 27001 sarà riscritta non più con una struttura coerente con la 9001, ma, applicando le linee guida del JTCG (Joint Technical Coordination Group) che coinvolgeranno d'ora in avanti tutti i sistemi di gestione, avrà una suddivisione diversa in capitoli, schematizzabile a grandi linee come segue:

1. Context of the organization
2. Leadrship and planning
3. Support
4. Operations
5. Performance evaluation
6. Improvement

Sulla decisione immediatamente successiva si è poi acceso un confronto molto serrato sull'Annex A. Le posizioni principali in merito erano quella di mantenerlo aggiornandolo alla nuova 27002 oppure di rimuoverlo. I vantaggi e svantaggi di ogni soluzione sono stati dibattuti ma alla fine ha prevalso di stretta misura la posizione, sostenuta principalmente da Giappone e Brasile, di lasciare l'Annex A, senza operare in questo caso una modifica che avrebbe fatto chiarezza e avrebbe permesso una separazione più netta tra le due norme.
Il punto successivo è stato inerente al conflitto tra "ISMS Policy" e "Information Security Policy", sicuramente da risolvere e derivante da una 17799 che non era ancora appaiata a nessuna norma di requisiti (come poi è stata la 27001). Fatto sta che attualmente non c'è una separazione netta tra questi documenti e, nel corso della discussione, è passata la posizione Anglo-Italiana di revisionare il controllo 5.1.1 della futura 27002 al fine di separare concettualmente questi due documenti.
L'ultimo dei punti principali di interesse è costituito dal capitolo 4 della 27002, anche lui figlio dell'impostazione "unica" della 17799. Questo capitolo (integrato ed ampliamente esteso nella 27005) verrà rimosso e la 27002 diventerà esclusivamente un catalogo di contromisure (controls).
Essendo stata data priorità agli argomenti di cui sopra, i numerosi commenti sul testo sono stati visionati solo in minima parte e rinviati per la maggioranza al prossimo meeting.

27008
Oltre alla 27007 (Guidelines for ISMS Audits), è da poco entrata in lavorazione una nuova norma sull'auditing, che però abbraccia le attività di verifica più in generale e non solo ristrette a quello che è l'audit di terza parte rivolto alla certificazione. Nell'ambito di questa norma, dai contenuti decisamente interessanti, l'Italia ha tenuto una breve presentazione ai delegati sulla metodologia OSSTMM di Isecom (www.isecom.org) che è assolutamente rilevante per la raccolta di informazioni sulla sicurezza basata su attività di test. La reazione è stata positiva e si sta valutando quale possa essere il modo migliore di legarla al nascente standard.

27010

Dopo un avventuroso avvicendamento del gruppo di editing, che ora vede impegnati Canada e UK, la nascente norma (Information security management for inter-sector communications) verrà divisa in una parte generale e una parte specifica per gli SCADA, a fronte del crescente interesse che questa tematica sta giustamente guadagnando a livello nazionale e internazionale. Nella seconda parte si è deciso però di non limitare l'argomento alle sole infrastrutture critiche, considerando tutte quelle che possono essere di importanza significativa (anche solo localmente).
E' da sottolineare che questo lavoro non vuole assolutamente andare a duplicare gli ottimi lavori che stanno venendo intrapresi da altre organizzazioni, tra cui NERC, NIST, OASIS etc.
27015
Nonostante si trovi ancora a uno stato iniziale, questa norma specifica per il settore finanziario e assicurativo sta già destando molte attenzioni. Gli USA hanno, a fronte della crisi del settore, abbandonato la guida del progetto, che sarà probabilmente raccolta dal Lussemburgo il quale si troverà a dover lavorare a stretto contatto con il TC68 del SC2 (già autore di .).

Altri aspetti di interesse
Considerando un po' a volo d'uccello le altre norme in gestione al WG1, si può finalmente notare come i lavori alla 27004 siano in fase di conclusione, tanto da prevedere l'emissione di un FDIS entro il prossimo meeting. La 27011, pronta già da tempo, è in fase di pubblicazione mentre la 27007 di cui già si accennava precedentemente passerà allo stato di CD.
La 27000 è già stata pubblicata ma, per errore, figura come norma a pagamento. Il SC27 aveva votato che fosse liberamente disponibile e sono state avviate le azioni necessarie a fare in modo che questo vada ad essere vero nel più breve tempo possibile. Potranno essere effettuate aggiunte nel prossimo futuro di tale norma, man mano che le componenti della famiglia 27000 sono completate.
La 27012, specifica per i servizi di e-government, ha invece subito una battuta d'arresto registrando la forte opposizione di USA e Nuova Zelanda e la poca convinzione della sua necessità presso gli altri national bodies.
Durante il meeting, presieduto da Ted Humphreys (papà della BS 7799), quest'ultimo ha annunciato le modalità del suo progressivo ritiro dalla guida del WG1. Questo ritiro avverrà entro i prossimi due anni e lascerà il gruppo di lavoro nelle mani dei capacissimi John Dale e Angelika Plate.
Il prossimo meeting è previsto per novembre e sarà ospitato da Microsoft, in quel di Redmond (Seattle) e sarà sicuramente decisivo per diversi aspetti di capitale importanza, a cui l'Italia, con una posizione speriamo ancora più forte, non si sottrarrà di certo.

_____
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