****
IT SERVICE MANAGEMENT NEWS - MARZO 2012
****

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: ISO/IEC 20000-2:2012

Il 15 febbraio è stata pubblicata la nuova versione della ISO/IEC 20000-2:2012. Il primo a darmene notizia è stato Attilio Rampazzo che ringrazio.

La ISO/IEC 20000-2 ha titolo "Information technology — Service management — Guidance on the application of service management systems". E' pertanto una linea guida e non uno standard certificabile.

La sua lettura è interessante ed è consigliabile a quanti intendono applicare la ISO/IEC 20000-1 senza avere una buona conoscenza di sistemi di gestione e/o una preparazione a livello di ITIL Foundation.

A dire la verità, leggendo il documento si notano alcune sbavature, soprattutto nei requisiti di sistema del capitolo 4 (responsabilità della direzione, gestione della documentazione e delle registrazioni, gestione delle risorse e gestione del miglioramento), a causa di alcune ripetizioni e concetti discutibili.

Gli approfondimenti sui 14 processi specifici sono invece più convincenti. Sono però rimasto perplesso dalla volontà di non parlare di workaround (si parla di known error con causa conosciuta, ma non di soluzioni temporanee a fronte di cause ignote) e di CAB e ECAB (anche se sono introdotti altri concetti tipici di ITIL e non presenti nella ISO/IEC 20000-1).

Faccio anche notare che queste linee guida sono di 94 pagine, mentre la versione precedente del 2005 ne aveva 42 per spiegare, più o meno, gli stessi processi. Ecco quindi che potremmo anche dire che tra la sintetica ISO/IEC 20000-1 (36 pagine) e il prolisso ITIL 2011 (quasi 2.000 pagine), un lettore potrebbe trovare in questo documento la giusta via di mezzo.

****

02- Privacy: precisazione sul Regolamento UE

Trattando sul futuro Regolamento UE sulla privacy, mi sono posto la seguente domanda: come sarà possibile tradurre "employing fewer than 250 persons", essendo questo il confine tra aziende che saranno obbligate a fare il DPS e quelle che non lo saranno?
- http://blog.cesaregallotti.it/2012/02/regolamento-ue-sulla-privacy-forse-il.html

Fabrizio Bottacin mi ha risposto inviandomi il link alla Raccomandazione della Commissione del del 6 maggio 2003 relativa alla definizione delle microimprese, piccole e medie imprese, da cui si deduce come calcolare le "250 persone" e che le PMI non dovranno fare il DPS, le altre sì:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:IT:PDF

****

03- Privacy: prescrizioni per i siti web dedicati alla salute

Il Garante il 25 gennaio ha emesso le "Linee guida in tema di trattamento di dati personali per finalità di pubblicazione e diffusione nei siti web esclusivamente dedicati alla salute".

Esse riguardano "i gestori dei siti web dedicati esclusivamente alla salute (specifici forum e blog, specifiche sezioni di portali che contengono informazioni sanitarie, nonché social network che si occupano di tematiche sulla salute attraverso specifici profili, aperti da soggetti privati con finalità di sensibilizzazione e confronto in tale ambito) in cui si svolge un'attività di carattere meramente divulgativo e conoscitivo, non solo con riferimento alle informazioni e ai commenti che si scambiano gli utenti, ma anche con riferimento ai consigli o alle "consulenze" mediche che vengono dagli stessi richieste."

Sono compresi due casi: i siti che richiedono e quelli che non richiedono la registrazione. In tutti i casi, devono essere fornite opportune avvertenze agli utenti. Sicuramente, tali avvertenze potrebbero essere fornite anche da siti non dedicati alla salute.

Le Linee Guida:
- http://www.garanteprivacy.it/garante/doc.jsp?ID=1870212

Il commento su Filodiritto:
- http://www.filodiritto.com/index.php?azione=archivionews&idnotizia=3613

****

04- Legislazione italiana: Certificazioni ISO 9001 e controlli

Edmea De Paoli mi segnala l'articolo 14 del DL Semplifica Italia (DL 5 del 2012), per cui:
- le amministrazioni pubbliche sono tenute a pubblicare la lista dei controlli a cui sono assoggettate le imprese
- i controlli potranno essere ridotti per le imprese in possesso della certificazione UNI EN ISO 9001

Già la Legge 133/2008 prevedeva che "i controlli periodici svolti dagli enti certificatori sostituiscono i controlli amministrativi o le ulteriori attività amministrative di verifica". Era un evidente orrore, in quanto è ben noto che la ISO 9001 non copre i controlli amministrativi in modo da coprire quanto opportuno.

Commento 1: dobbiamo vedere come sarà trattata la questione dalle Linne Guida in materia che saranno prodotte più o meno in ottobre 2012 e pubblicate su www.impresainungiorno.gov.it

Commento 2: il punto f) del comma 4 fornisce un ottimo punto di partenza per i requisiti da chiedere ad un qualsiasi fornitore ("certificazione del sistema di gestione per la qualità da un organismo di certificazione accreditato da un ente di accreditamento designato da uno Stato membro dell'Unione europea ai sensi del Regolamento 2008/765/CE, o firmatario degli Accordi internazionali di mutuo riconoscimento IAF MLA); visti i bandi di gara che si vedono in giro, c'è da fare i complimenti a chi ha scritto questo paragrafo per l'inusuale correttezza.

****
05 -Sentenza su danneggiamento di informazioni mediante cancellazione di file

La Cassazione Penale ((Corte di Cassazione - Sezione Quinta Penale, Sentenza 5 marzo 2012, n.8555), ha stabilito che, sussiste il reato previsto dall'articolo 635 bis Codice Penale (danneggiamento di informazioni, dati e programmi informatici) anche qualora i file cancellati possano essere oggetto di recupero.

La sentenza riguarda un caso in cui, comunque, alcuni dei file cancellati non sono stati recuperati lo stesso.

La notizia l'ho trovata sulla newsletter di Filodiritto:
- http://www.filodiritto.com/index.php?azione=archivionews&idnotizia=3640

Per chi avesse la pazienza di leggere l'orrendo italiano della sentenza originale, ho trovato questo link:
- http://www.cnai.it/allegati/novita/85_sentenza%20cassazione%208555%205.03.2012.pdf

****
06- Sentenza utilizzo di software duplicati per i computer aziendali

Se qualcuno avesse avuto ancora dei dubbi: è illegale "aver installato software su computer aziendali senza averne previamente acquistato la relativa licenza". Lo ha stabilito la Cassazione, Sezione Terza Penale, con sentenza 5879 del 15 febbraio 2012.

L'articolo su Filodiritto:
- http://www.filodiritto.com/index.php?azione=archivionews&idnotizia=3618

Secondo me (non sono un legale!), l'accusato poteva pagare i 1.000 Euro e farsi convertire i 4 mesi di reclusione in qualcosa d'altro. O l'accusato aveva soldi e tempo da spendere in processi (primo, secondo e terzo grado!), o aveva scelto un avvocato furbetto che l'ha consigliato male.

****

07- Sentenza su controllo legittimo ex post di email del dipendente

La Cassazione Lavoro, con sentenza del 23 febbraio 2012, ha dichiarato legittimo, in certe condizioni, il controllo delle e-mail del dipendente.

Sentenza molto interessante per chi si occupa di sicurezza, 231 e privacy.

Segnalo l'articolo su Filodiritto:
- http://www.filodiritto.com/index.php?azione=archivionews&idnotizia=3619

L'articolo si conclude con un interessante commento: "sarebbe stato interessante conoscere nel dettaglio l'attività di indagine sull'infrastruttura informatica posta in essere dal datore di lavoro".

****

08- Analisi minacce - Rapporti MELANI

Quando si analizzano i rischi alla sicurezza delle informazioni, è necessario analizzare, tra gli altri elementi, la possibilità di accadimento delle minacce. Per questo dovrebbero essere prese in considerazioni le esperienze passate dell'organizzazione oggetto dell'analisi, le esperienze passate di organizzazioni in contesti geografici o di business simili, l'appetibilità delle proprie informazioni e le caratteristiche delle fonti di rischio.

Per questo segnalo due rapporti tecnici di MELANI, la Centrale d'annuncio e d'analisi per la sicurezza delle informazioni della Svizzera:
- il Rapporto semestrale 2011/1 dell'ottobre 2011,
http://www.melani.admin.ch/dokumentation/00123/00124/01128/index.html?lang=it
- il Rapporto "Minacce attuali su Internet, autori, strumenti, perseguimento penale e Incident Response" del gennaio 2012, http://www.melani.admin.ch/dokumentation/00123/01132/01134/index.html?lang=it

****

09- Attacchi: Change Oracle e blocco di un ospedale

Sandro Sanna mi segnala questa notizia:
- http://messaggeroveneto.gelocal.it/cronaca/2012/02/15/news/ospedale-computer-ieri-di-nuovo-in-tilt-poi-il-sistema-riparte-1.3183320

In poche parole, sembra che il fine settimana del 12 e 13 febbraio, siano state fatte delle modifiche al database (dall'articolo pare sia Oracle) e che poi il sistema si sia bloccato fino a ripartire lentamente il martedì.

Non ho nulla contro Oracle: chi non fa non falla. Ho però qualche appunto da fare a chi dice che "i change ai database non sono critici", "fare e documentare i test è una perdita di tempo" e "le procedure di roll-back sono facili". In realtà nessuno lo dice con queste parole, ma lo pensa.

A pensarci bene, qualcosa contro Oracle ce la potrei avere, ma non ho dati a sufficienza. Vorrei capire se ci sono dei prezzi agevolati per l'acquisto di licenze per gli ambienti di test e per gli ambienti di DR. A pensar male ho ragione o torto?

Chissà chi è il colpevole (il manager che aveva fretta? il commerciale che aveva fatto male i conti e bisognava chiudere per non perdere "giornate uomo"? il cliente che aveva chiesto tempi irragionevoli? Il project manager non abbastanza prudente? il responsabile qualità che non aveva fatto correttamente la procedura?).

Di queste notizie ne abbiamo abbastanza, ma ne vedremo ancora. In Italia e all'estero. In troppi penseranno comunque che "questo a me non potrà capitare".

****

10- Associazione Nospammer.info

Luca De Grazia mi segnala l'associazione No Spammer (http://www.nospammer.info/). Si occupano di fornire assistenza legali a quanti sono infestati dallo spamming, a quanti hanno a che fare con siti web non regolari, a quanti hanno problemi a far valere i propri diritti quando acquistano via web, eccetera.

Al momento, l'associazione pare appena costituita e quindi non ci sono notizie interessanti. Ma l'idea è buona e non ci aspetta che vedere l'effetto che fa.

****

11- NIST SP 153 - Guidelines for Securing WLANs

Il NIST ha pubblicato la Special Publication 800-153 dal titolo "Guidelines for Securing Wireless Local Area Networks (WLANs)".

In questa pubblicazione si richiamano soprattutto le criticità legate al personale interno che potrebbe usare la doppia connessione wireless e wired, aprendo delle vulnerabilità.

Per ulteriori specifiche di sicurezza sulle WLANs, bisogna fare riferimento a:
- SP 800-97 "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i"
- SP 800-48 "Guide to Securing Legacy IEEE 802.11 Wireless Networks"

Rimangono i soliti concetti base:
- verificare i requisiti di sicurezza dei prodotti per creare gli Access Point
- configurare gli accessi via meccanismi crittografici
- installare le reti per gli ospiti in modo che non abbiano visibilità sulla rete interna

Banalità, certamente. Fino a quando si scopre che non sono sempre seguite.

****

12- COSO Internal Control Framework (draft)

Il COSO Internal Control Framework è il punto di riferimento (per lo meno, nominale) per la progettazione, realizzazione e valutazione di controlli efficaci per le attività di business. Ovviamente, fa riferimento alla tecnologia. Esso è molto citato da chi si occupa di IT (è molto celebre il "cubo"), quando si lascia intendere che il business deve essere controllato secondo i principi del COSO Internal Control Framework e l'IT dal CobiT e le due attività devono essere tra loro connesse.

Il COSO ha pubblicato il draft per commenti:
- http://www.ic.coso.org/pages/exposure-draft.aspx

Il controllo interno deve seguire 17 principi, a loro volta collegati ai 5 componenti di controlli interni: ambiente di controllo, risk assessment, attività di controllo, comunicazione, monitoraggio.

La futura versione del COSO Internal Control Framework è destinata a sostituire quella attualmente in vigore, datata 1992 (20 anni!).

Il COSO, nel 2004, ha pubblicato anche il "Enterprise Risk Management - Integrated Framework". Secondo quanto dichiarato dal COSO stesso, "l'enterprise risk management è più ampio del controllo interno, perché espande e approfondisce il controllo interno e si focalizza maggiormente sui rischi".
Pubblicato da Cesare Gallotti alle 16:48 0 commenti

****

13- Tool di computer forensics

Dalla newsletter di Marco Mattiucci, segnalo il rilascio della DEFT 7, un toolkit (made in Italy) destinato ad operare nel Computer Forensics, Mobile Forensics, Network Forensics, Incident Response e Cyber Intelligence:
http://www.deftlinux.net/2012/01/31/deft-7-ready-for-download/

Pasquale Stirparo, della DFA, ha segnalato ai soci una "Crazy good list of free computer forensic tools":
http://forensiccontrol.com/resources/free-software/

In tutti i casi, rimane la regola aurea: non usateli per scopi "reali" se non avete l'adeguata competenza tecnica e legale e una buona esperienza anche a seguito di affiancamenti.

****
14- BYOD - Bring your own device

Il tema del BYOD (gli utenti aziendali che usano i propri strumenti informatici personali per svolgere attività lavorativa) mi ha sempre interessato. Venendo dai tempi in cui non era lecito usare gli strumenti aziendali per finalità personali, mi sorprende questa tendenza di volere usare gli strumenti personali per finalità aziendali.

Sempre più vedo manager (e non manager) compulsare la propria mail o scrivere documenti su tablet quasi sicuramente personali. Mi chiedo se abbiano configurato una password di accesso (dubito, vista la velocità con cui rispondono alle telefonate), se i dati siano cifrati, eccetera.

IBM, tra gli altri, propone una sua soluzione:
-
http://www.bitmat.it/articolo.php?aId=0000091292&cId=46&cpId=20&n=IBM%2Bpropone%2Bun%2Bnuovo%2Bsoftware%2Bper%2Bi%2Bdispositivi%2Bmobili%2Bsul%2Bluogo%2Bdi%2Blavoro

Non voglio fare pubblicità a IBM o ad altri, ma questo è un argomento che seguo da dicembre 2010 (http://blog.cesaregallotti.it/2010/12/lasciatemi-il-mio-pc.html), ho visto questa segnalazione nel gruppo Clusit di LinkedIn, in questi 14 mesi ho visto crescere veramente il fenomeno e ho colto l'occasione per ribadirlo.

****
15- Materiale Convegno AIEA settembre 2011

L'AIEA ha messo a disposizione sul suo sito il materiale del convegno del 29 e 30 settembre 2011:
- http://www.aiea.it/html/pqwert3256_29_settembre_2011.html
- http://www.aiea.it/html/ytrew87bvc_30_settembre_2011.html

Non ho trovato molto interessanti le slides della seconda giornata (cloud e social network). Invece segnalo quelle della prima giornata:
- "Sistemi di pagamento elettronici" di Domenico Gammaldi di Banca d'Italia, con riferimenti alla normativa vigente in Italia in materia
- "Infrastrutture critiche" di Daniele Perucchini - Fondazione Ugo Bordoni, con riportata la situazione attuale in materia
- "La sicurezza ICT e la protezione delle infrastrutture critiche" di Glauco Bertocchi di Isaca Roma, un articolo su SCADA e i sistemi di controllo di processo.

Buona lettura.