****
IT SERVICE MANAGEMENT NEWS - APRILE 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- Spammer o vittima degli filtri?

Il 15 marzo, stranamente puntuale, ho inviato la newsletter con titolo "[IT Service Management] Newsletter del 15 marzo 2012". Il mio client di posta, in un millisecondo, mi ha avvisato che la mail non poteva essere recapitata a nessuno dei destinatari causa errore SMTP 554 (ho guardato: errore generico di "messaggio rifiutato"). Ho riprovato più volte, fino a quando ho inviato la stessa mail togliendo dal titolo la preposizione articolata "del".

Risultato: la mail è partita (curioso come una preposizione articolata possa avere certi effetti), ma ho ricevuto parecchi messaggi di errore, dal maledetto SMTP 554 a notifiche di filtri (per esempio il 550 5.7.1 Message rejected due to content restrictions). Altri, hanno ricevuto la newsletter senza problemi. La cosa buffa è che non l'ho ricevuta neanche io stesso.

Il "colpevole" era un link dell'articolo 14. Per trovarlo, ho fatto numerose prove (meno male che uso diversi indirizzi di mail!) e mi è costato diverso tempo. Il 23 marzo ho quindi riinviato la newsletter corretta e spero sia arrivata a quanti non l'avevano ricevuta.

I filtri alle mail sono oggi uno strumento necessario e io per primo non ho proposte alternative per sostituirli. Dei messaggi di errore più significativi mi avrebbero però aiutato.

Mi rimane solo da scusarmi con quanti hanno ricevuto la medesima mail per 4 (quattro!) volte. Spero non si ripeta più.

****

02- Legale: Le responsabilità nella certificazione

Con colpevole ritardo, segnalo questo articolo del Presidente dell'Organismo di vigilanza di Accredia sulle semplificazioni introdotte nel 2008:
- http://www.uni.com/index.php?option=com_content&view=article&id=572%3Ale-nuove-responsabilita-nella-certificazione-ambientale-e-di-qualita&Itemid=741&lang=it

L'articolo è apparentemente obsoleto, ma è invece validissomo perché anche il nuovo Decreto Semplificazioni del Governo Monti prevede che i controlli amministrativi potranno essere ridotti per le imprese in possesso di certificazioni ISO (articolo 14 del DL 5 del 2012, convertito con Legge 35 del 2012). La notizia la diedi a marzo:
- http://blog.cesaregallotti.it/2012/03/certificazioni-iso-9001-e-controlli.html

L'aricolo fa notare che "Questa interpretazione, se verrà confermata nella sua estensione applicativa dalla determinazione regolamentare degli ambiti nei quali dovrà trovare applicazione l'efficacia sostitutiva della certificazione, comporterà necessariamente conseguenze rilevanti, non tutte al momento prevedibili, soprattutto in tema di responsabilità amministrativa degli enti certificatori e di responsabilità diretta, anche sul piano penale, del personale di questi enti addetto alle verifiche ed ai controlli".

Il punto problematico per il "sistema certificazione" sarà la corretta formazione del personale, forse attualmente non adeguato per questo genere di responsabilità.

Il tutto dovrà essere meglio specificato in regolamenti di cui, al momento, non si ha notizia.

****

03- Legale: DPS addio; è ufficiale

Il 4 aprile, la Camera ha definitivamente approvato con modificazioni il DL 5/2012 "Semplifica Italia" con la Legge 35 del 2012.

Per quanto riguarda la sorte del DPS, non ci sono state sorprese: è stato abrogato.

Il testo attuale del Dlgs 196 del 2003 è reperibile su www.normattiva.it.

Ricordo due miei post sul tema:
- http://blog.cesaregallotti.it/2012/01/dps-addio-secondo-tentativo-quasi.html
- http://blog.cesaregallotti.it/2012/02/regolamento-ue-sulla-privacy-forse-il.html

Simone Tomirotti mi ha anche segnalato questo link:
- http://www.ipsoa.it/News/PA/privacy_il_dps_non_serve_piu_id1067535_art.aspx

Max Cottafavi di Reply mi ha ricordato che alla fine la formazione non è stata salvata. Peccato.

****

04- Legale: Lavoro al videoterminale

Il tema dei rischi della sicurezza dei lavoratori videoterminalisti è un tema appartenemente marginale alla qualità e alla sicurezza delle informazioni. Di fatto, è importante capire come un buon ambiente di lavoro porti poi ad avere migliore efficienza ed efficacia nell'esecuzione delle attività.

Il riferimento migliore per trattare di questo tema è certamente quello dell'INAIL; in particolare l'opuscolo "Il lavoro al videoterminale" aggiornato al 2010:
-
http://www.inail.it/Portale/appmanager/portale/desktop?_nfpb=true&_pageLabel=PAGE_PUBBLICAZIONI&nextPage=PUBBLICAZIONI/Tutti_i_titoli/Prevenzione_e_sicurezza/Il_lavoro_al_videoterminale/index.jsp

Dalla pagina "Prevenzione e sicurezza" è anche possibile effettuare ricerche per trovare altro materiale in materia:
-
http://www.inail.it/Portale/appmanager/portale/desktop?_nfpb=true&_pageLabel=PAGE_PUBBLICAZIONI&nextPage=PUBBLICAZIONI/Tutti_i_titoli/Prevenzione_e_sicurezza/index.jsp

****
05- Sentenza: L'uso dell'identità di terzi è reato

La Corte di Cassazione - Sezione Terza Penale, con Sentenza n.12479 del 3 aprile 2012, ha stabilito che è reato utilizzare i dati anagrafici di terzi (veri ed esistenti) per aprire a loro nome un account di un sito.

Parrebbe cosa ovvia, però la difesa ha obiettato che "l'imputato avrebbe utilizzato i dati anagrafici della vittima solo per iscriversi al sito di aste on-line, partecipando poi alle aste con un nome di fantasia". Meno male che la Cassazione ha confermato che rimane comunque applicabile l'articolo 494 del Codice Penale ("Chiunque... induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato,...").

Per la cronaca: il danneggiato si è accorto della cosa perché il reo non ha pagato quanto acquistato e si è visto arrivare a casa una qualche richiesta di pagamento.

Ogni tanto la Legge conferma le nostre modeste intuizioni.

L'articolo e la notizia su Filodiritto:
http://www.filodiritto.com/index.php?azione=archivionews&idnotizia=3682

****

06- Sentenza: Furto di firma digitale

Valentino Privato mi segnala questa interessante notizia:
- http://www.ilsole24ore.com/art/notizie/2012-03-26/rubano-firma-digitale-intestano-181133.shtml?uuid=AbGTnUEF

Riassumo: due furbacchioni si presentano dal commercialista di un imprenditore, gli dicono che l'imprenditore ha bisogno di una copia della smart card per l'apposizione della firma digitale, ma non può essere presente perché all'estero; il commercialista ci crede e avvia la pratica; i due furbacchioni, con la nuova smart card, si intestano quindi l'azienda dell'imprenditore.

Come al solito, la vulnerabilità è nelle persone credulone e disponibili ad aiutare anche se questo richiede di forzare "un po'" le procedure, come già detto da Kevin Mitnick nella sua "L'arte dell'inganno".

****
07- Standardizzazione: ISO/IEC 27010:2012 - Comunicazioni intersettoriali e interaziendali

E' stata pubblicata la ISO/IEC 27010 dal titolo "Information technology - Security techniques - Information security management for inter-sector and inter-organizational communications".

Ci sono cose interessanti in questo documento, anche se non ritengo che siano tali da giustificare la spesa di 110 Euro per acquistarlo. L'impostazione è piuttosto teorica e si basa sulle "sharing community".

Non sono fornite linee guida sulla classificazione, sull'etichettamento e sul conseguente trattamento delle informazioni.

Peccato sia stata discussa e prodotta in questo periodo in cui le forze dei partecipanti al SC 27 sono concentrate soprattutto sulla revisione della ISO/IEC 27001.

****
08- Pubblicato COBIT 5

E' stato pubblicato il COBIT 5, che segue il COBIT 4.1.

Ricordo che COBIT è il riferimento per gli audit sui processi di governo dell'IT, in particolare quando compresi negli audit di revisione di bilancio, SOC e/o Accordi di Basilea.

Le pubblicazioni ufficiali sono le seguenti:
COBIT 5 Framework
COBIT 5: Enabling Processes
COBIT 5 Implementation
COBIT 5 Toolkit

Traduco l'annuncio di ISACA: "COBIT 5 fornisce una visione di business complessiva sulla governo dell'IT aziendale. I principi, le pratiche, gli strumenti di analisi e i modelli di COBIT 5 comprendono le direzioni e le guide di esperti in business, IT e governance di tutto il mondo. In breve, COBIT 5 aiuta coloro che lo utilizzano a ottenere il più alto ROI dalle proprie informazioni e risorse tecnologiche.

Per scaricarlo:
- http://www.isaca.org/COBIT/Pages/default.aspx

Segnalo anche le slide dell'interessantissima presentazione di Alberto Piamonte, a cui ho assistito l'8 marzo in occasione di una Sessione di Studio AIEA:
- http://www.aiea.it/pdf/sessioni%20di%20studio%20e%20di%20formazione/2012/Milano%2008032012%20Alberto%20Piamonte.pdf

****

09- Linee guida ABILab sulla Digital Forensics

Max Cottafavi di Reply mi ha segnalato un interessante documento di ABILab a cui ha collaborato, intitolato "Linee Guida sulla digital forensics nel settore bancario italiano".

Il titolo è forse riduttivo, visto che la linea guida potrebbe essere applicabile a qualsiasi realtà. E' però evidente che si parte dal presupposto che le dimensioni debbano essere medio-grandi.

Il concetto chiave e importante di queste linee guida prende il nome di "digital forensics preventiva". Questa richiede di: identificare i possibili reati da trattare, identificare i criteri organizzativi e tecnologici e legali per individuarli tempestivamente e per raccogliere correttamente le prove da utilizzare eventualmente in sede legale.

Il concetto è importante e originale perché quasi tutti gli articoli sulla computer forensics partono dal presupposto di trovarsi in un'indagine quasi da telefilm (anche se la realtà è meno spettacolare) e non contemplano le necessità di un'impresa di tutelarsi anche in ottica preventiva a fronte di frodi o altre attività illecite che possono coinvolgere i propri sistemi informatici.

Si richiede quindi un certo sforzo di analisi preventiva dei possibili reati, dei propri sistemi informatici e dei piani di azione. Sforzo che in alcune realtà (come quelle bancarie) è sempre più necessario.

Le linee guida sono anche accompagnate da ottime analisi sull'uso delle prove nel processo penale e nel processo civile.

****

10- Rapporto Clusit 2012 sulla sicurezza ICT in Italia

Al Security Summit del 20-22 marzo 2012 a Milano è stato presentato il Rapporto Clusit 2012 sulla sicurezza ICT in Italia.

Qualche considerazione "sparsa":
- il titolo conferma il forte orientamento alla sicurezza ICT; nell'illustrazione degli incidenti registrati nel 2011 sono comunque sottolineati i numerosi casi in cui le tecniche di attacco si sono basate soprattutto sul social engineering
- il rapporto illustra quasi unicamente gli incidenti di cyber-crime, nella sua accezione più ampia; una sezione molto interessante è quella sugli incidenti registrati a livello internazionale: gli attacchi alla Sony, alla HBGary, ai certificati SSL
- i casi per me più emblematici sono quelli "Operation Nitro" ed "Operation Night Dragon": sono stati individuate attività di spionaggio in corso da lungo tempo, che dimostrano ancora una volta che uno dei problemi della sicurezza non è "cosa si individua", ma "cosa non si individua"
- molto interessante è il confronto tra le "Aree di maggior interesse" per i vendor e per gli "users": oltre ad risultati facilmente prevedibili (la "Compliance" è ugualmente importante per vendor e user, "standard e metodologie", ahimé, sono più importanti per i vendor che per gli user), mi ha colpito il risultato del Cloud Computing: per i vendor ha importanza pari a 3,5 su 5, mentre per gli user ha importanza 1,5 su 5.
- un dato dimostra come queste ricerche vadano sempre prese con cautela: gli user dichiarano che il parametro "economicità" è il meno importante nella selezione dei vendor, quando sappiamo bene che questo non corrisponde alla realtà
- altrettanto importanti sono le figure professionali richieste: i vendor puntano soprattutto su figure tecniche, mentre gli user puntano in egual misura su figure tecniche e gestionali

Complimenti agli autori, anche per gli interessanti articoli di approfondimento.

Per richiedere il rapporto, vi invito a leggere la pagina web:
https://www.securitysummit.it/page/rapporto_clusit

****

11- Social Media e sicurezza in azienda

Protiviti ha pubblicato un interessante documento intitolato "Social Media e sicurezza in azienda: verso un nuovo approccio".

Forse l'approccio non è così nuovo, ma è importante capire su cosa si basa: i social media, oggi, non possono essere ignorati dalle imprese, ma questi introducono nuovi fattori di vulnerabilità e di rischio che devono essere trattati. La tesi del documento è quindi che "cresce pertanto l‟esigenza di dotarsi di un modello di governo dell„utilizzo dei Social Media, che consenta di trarne i maggiori benefici, ma anche di minimizzare gli impatti negativi, soprattutto perché non sempre direttamente identificabili".

I rischi vengono suddivisi in due famiglie: "Rischi derivanti dalla partecipazione consapevole dell'azienda in ambito Social Media" e "Rischi derivanti dalla presenza non gestita da parte dell'azienda in ambito Social Media".

Infine, viene proposto un modello di intervento, certamente banale nella sua formulazione teorica, ma sicuramente complesso nella sua applicazione. Vale la pena ricordarne le fasi più significative:
1- Individuazione degli obiettivi e finalità dei Social Media nel contesto della realtà aziendale
2- Valutazione dei profili di rischio di sicurezza
3- Gestione della sicurezza delle informazioni
4- Individuazione delle responsabilità
5- Gestione dei flussi comunicativi e decisionali
6- Tutela dell'immagine aziendale, tramite la definizione di un processo di monitoraggio
7- Valutazione periodica dell‟efficacia e dell‟efficienza delle misure di sicurezza
8- Predisposizione di policy e di procedure
9- Formazione e informazione interna

Il documento (Newsletter numero 37 del Marzo 2012) dovrebbe essere disponibile sul sito di Protiviti:
- http://www.protiviti.it/it-IT/Pagine/Newsletter-di-Protiviti-Italia.aspx

****
12- Malware per Mac

Non è bello da dirsi, ma la leggenda che i Mac sono immuni da malware sembra falsa.

Altri avevano detto che il malware per Windows è molto numeroso per il semplice fatto che il suo installato è abbondantemente superiore a qualsiasi altro sistema operativo. Mac sta evidentemente prendendo quote di mercato e/o le piattaforme di sviluppo per Mac sono più accessibili.

Il link da SANS Newsbyte del 17 aprile 2012:
http://www.usatoday.com/tech/news/story/2012-04-16/apple-mac-java/54317794/1

****
13- Plug computing

Segnalo la pagina web di Marco Mattiucci dedicata al Plug Computing.

Lo ammetto: non credo di avere mai visto un plug computer ("sono generalmente server con funzionalità limitate e mirate che operano soprattutto fornendo servizi in rete; spesso si tratta di box direttamente collegati all'alimentazione elettrica; i servizi più comuni che realizzano sono: NAS, CloudPlugging, Security, Encryption e non sono esclusi servizi di routing e VoIP"), ma da oggi in poi, se qualcuno me ne farà vedere uno, non farò la faccia sorpresa... e poi mi farò spiegare meglio come funziona.
http://www.marcomattiucci.it/plugcomputer.php

****

14- Assessment e critiche

The IT Skeptic scrive un articolo molto critico sugli assessment sulla maturità dei processi ITIL. In particolare, fornisce 4 ragioni per dire che sono "un'inutile perdita di soldi":
1- i consulenti che fanno gli assessment non prendono in carico gli obiettivi del cliente (in altre parole, segnalano delle mancanze che forse non lo sono)
2- molti assessment non forniscono indicazioni su come rimediare (livello di gravità, priorità da dare all'azione correttiva)
3- una valutazione del livello di maturità è inutile, mentre è utile una valutazione rispetto ai rischi e agli obiettivi dell'organizzazione
4- ITIL non è uno strumento per valutare la maturità dei processi

I primi 3 punti sono facilmente applicabili a tutti gli altri schemi; il quarto è ovviamente istanziabile solo una parte di essi.

Sottoscrivo tutto, anche se ciò non farà piacere a qualche mio lettore.

Una parte del mio lavoro è dedicata a fare audit e assessment e quindi non posso dichiarare (così come non lo fa IT Skeptic) che gli assessment sono in generale inutili. Dichiaro che gli assessment sulla maturità dei processi non mi convincono, che gli assessment senza una conseguente prioritizzazione delle azioni correttive non forniscono indicazioni utili ai clienti e che gli assessment basati su check list per condurli e grafici troppo semplicistici per presentarne i risultati sembrano professionali ma non lo sono.

Il post di IT Skeptic (commentato non sempre in modo condivisibile): http://www.itskeptic.org/uselessness-itil-process-maturity-assessment

La segnalazione l'ho avuta da ITSM News:http://www.itsmportal.com/news/process-maturity-assessments-prove-it-it-service-providers-suck

****
15- Agenda Digitale

Dalla newsletter del Clusit segnalo il documento ufficiale della Cabina di Regia dell'Agenda Gigitale con tutti i dettagli dell'attività di Governo varato dal Governo Monti e dai ministri Profumo e Passera.

Si parla della costituzione di un CERT, di attivazione di sistemi di allerta per i cittadini, progetti per la sicurezza dei pagamenti e dell'identità digitale, nonché di nuovi CED.

La presentazione: http://www.slideshare.net/micheleficara/agenda-digitale-ecco-il-documento-ufficiale-della-cabina-di-regia