****
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 o disiscriversi o scrivendo a cesaregallotti@cesaregallotti.it o seguendo le istruzioni riportate nella pagina http://www.cesaregallotti.it/newsletter.htm. L'informativa sul trattamento dei dati personali è alla pagina http://www.cesaregallotti.it/newsletter.htm.

****
Indice

01- Sicurezza delle informazioni: Attacchi (Microsoft, top-25, carte di pagamento, Security surveys)
02- Tecnologia: privacy, sicurezza e forensics su Windows
03- Tecnologia: Sistemi operativi (I 20 peggiori, Fosdem 2010)
04- Standardizzazione (ISO/IEC 27003, considerazioni)
05- Best practices: ITILv3.5
06- Best practices: Business Continuity
07- Normativa: Privacy e Responsabilità Amministrativa (231/2001)
08- Normativa: Dematerializzazione (Nuovo CAD, OMAT 2010, Codice ambientale, Delibera CNIPA, Moneta Elettronica)
09- Normativa: Responsabilità degli ISP (Sentenza di Google e Dlgs 70/2003)
10- Decisione UE contro "monitoraggio" da parte USA
11- Computer Forensics
12- Project Management
13- Presentazioni

****
01- Sicurezza delle informazioni: Attacchi (Microsoft, top-25, carte di pagamento, Security surveys)

Problemi di un patch Microsoft

Da SANS NewsBites Vol. 12 Num. 18: Microsoft pubblicherà una nuova versione dell'aggiornamento di sicurezza MS10-015 per Windows e Office perché la precedente ha causato dei crash.
Questo per segnalare che il "patching immediato" ha i suoi rischi e non sempre è la scelta migliore.
http://news.zdnet.co.uk/security/0,1000000189,40070580,00.htm
http://www.computerworld.com/s/article/9166158/Microsoft_plans_to_patch_8_Windows_Office_bugs_next_week
http://www.microsoft.com/technet/security/Bulletin/MS10-mar.mspx

I 25 errori di programmazione più gravi

Su SANS NewsBites Vol. 12 Num. 14 c'è la notizia sulla nuova edizione del SANS Top 25 Most Dangerous Programming Errors. Forse questa elencazione dei top-25 fa molto made-in-USA, ma il documento è certamente degno di attenzione, anche perché ogni vulnerabilità è accompagnata da linee guida per prevenirla.
http://www.sans.org/top25-programming-errors/

Carte di pagamento

Su Cryptogram di febbraio 2010 si trovano due interessanti interventi su attacchi alle carte di pagamento:
- lettori di carte man-in-the-middle per ATM http://www.krebsonsecurity.com/2010/01/would-you-have-spotted-the-fraud/
- un'analisi delle "misure di sicurezza" messe a disposizione dagli issuers
http://www.cl.cam.ac.uk/~rja14/Papers/fc10vbvsecurecode.pdf
(la discussione su questo paper è su http://www.lightbluetouchpaper.org/2010/01/26/how-online-card-security-fails/)

A me, intanto, Mastercard fa pagare gli SMS di avviso di avvenuta transazione a prezzo pieno (ma loro avranno sicuramente condizioni più favorevoli) e per attivare il servizio è necessario telefonare ad un numero 199 a pagamento.
Inoltre, il mese scorso mi ha bloccato la carta per "verifica" al terzo acquisto consecutivo via web, senza avvisarmi in alcun modo (gli acquisti riguardavano 2 biglietti di aereo e un albergo...). Complimenti alla sicurezza!

Security surveys

A inizio anno, le "solite" ricerche sulla sicurezza
- Ernst and Young:
http://www.ey.com/Publication/vwLUAssets/Global_Information_Security_Survey_2009/$FILE/EY_Global_Information_Security_Survey_2009.pdf
- Symantec: http://www.symantec.com/about/news/release/article.jsp?prid=20100221_01
- IBM: http://www-935.ibm.com/services/us/iss/xforce/

****
02- Tecnologia: privacy, sicurezza e forensics su Windows

Da Forensic Focus newsletter del febbraio 2010: Microsoft ha prodotto un documento ad uso riservato nel quale si dettagliano quali dati conserva su tutti gli utenti dei propri servizi e prodotti.

Il documento, è stato inizialmente pubblicato su http://cryptomeorg.siteprotect.net, ma è stato bloccato. Ora l'ho trovato qui
http://www.wired.com/images_blogs/threatlevel/2010/02/microsoft-online-services-global-criminal-compliance-handbook.pdf

Il documento e la storia sono tutti e due ben inquietanti perché dimostrano come la privacy non sia sempre garantita con i produttori di software e i fornitori di servizi IT.

La notizia completa è su http://www.theregister.co.uk/2010/02/25/cryptome_dmca_takedown/

Navigando su cryptomeorg, si trovano interessanti documenti di Computer Forensics su Windows (dette, forse non correttamente, "guide per spiare").

Mattia Epifani, da parte sua, ha pubblicato sul suo sito una breve guida introduttiva all'analisi forense del sistema operativo Windows 7.
http://www.digital-forensics.it/index.php?page=introduzione-all-analisi-forense-di-windows-7

****
03- Tecnologia: Sistemi operativi (I 20 peggiori, Fosdem 2010)

I 10 peggiori sistemi operativi

Da Computerworld Italia del 14 dicembre 2009 ho trovato un divertente (?) articolo sui 10 peggiori sistemi operativi della storia.

L'articolo in italiano di CWI
http://www.cwi.it/notizia/17723/2009-05-05/I-dieci-peggiori-sistemi-operativi-dal-lontano-1964-ai-

giorni-nostri.html

L'articolo in inglese originale
http://www.pcworld.com/article/162866/the_10_worst_operating_systems_of_all_time.html

Fosdem 2010

A questo proposito, sulla Newsletter HSC di marzo 2010 vi è una relazione sul convegno Fosdem 2010 (http://fosdem.org/2010/). In quella occasione, Andrew Tanenbaum ha presentato la nuova versione del sistema operativo Minix 3. Tanenbaum rimane un mito per tutti coloro che hanno studiato i sistemi operativi e trovo che i suoi studi e le sue scelte su "cosa deve fare un sistema operativo", sebbene di livello piuttosto tecnico, sono molto interessanti.
http://fosdem.org/2010/schedule/events/867
Per i tecnici, vale la pena guardare anche gli altri interventi.

****

04- Standardizzazione (ISO/IEC 27003, considerazioni)

ISO/IEC 27003:2010

Il 1 febbraio 2010 è stata pubblicata una nuova norma della famiglia 27000: la ISO/IEC 27003:2010 dal titolo "Information security management system implementation guidance".

La lettura presenta alcuni spunti di interesse. Però ricodo che si tratta di un documento ISO: mai sufficientemente dettagliato con esempi per chi vuole imparare la materia e troppo elementare negli spunti pratici per chi la conosce già.

Un'ulteriore critica: il documento, malgrado il titolo, si occupa solo della fase di plan del ISMS (l'ultimo capitolo ha titolo "Designing the ISMS") e tralascia completamente le imporantissime fasi di do, check e act.

Forse è una conferma della cattiva abitudine di alcuni manager e consulenti di produrre tanti bei piani per poi realizzarli poco o male, senza fornire supporto agli utenti e senza occuparsi troppo di comprendere anche le esigenze di efficienza, usabilità e operatività dell'ISMS.

Trovo conferma di tale cattiva abitudine (non di tutti, ovviamente!) quando spiego nei corsi e nelle presentazioni che i consulenti e i manager dovrebbero scrivere meno documenti per avere il tempo di supportare attivamente la realizzazione di quanto scritto: vedo molte teste che si agitano confermando quanto il problema sia sentito.

Sulla realizzazione di standard

Lo so: critico spesso le norme ISO. Giustamente qualcuno mi ha detto che dovrei partecipare ai gruppi di lavoro, piuttosto che fare il grillo parlante.

E' opportuno sapere che, in Italia, l'interlocutore della ISO sulle norme della famiglia ISO/IEC 27000 è la UNINFO. Per partecipare a ciascun gruppo di lavoro, la quota di iscrizione è di circa 1.200 Euro. A questo, per chi volesse partecipare alle riunioni plenarie semestrali della ISO in diversi Paesi del mondo (o anche semplicemente alle riunioni interne all'UNINFO), è necessario aggiungere tutte le spese di trasferta.

Se questo spiega il perché non abbia (ancora) partecipato attivamente alla discussione sulle norme, è opportuno segnalare che l'UNINFO ha creato una speciale modalità di iscrizione, a cui ho aderito, di 350 Euro per coloro che volessero partecipare ai lavori sulla sola famiglia ISO 27001 (il GdL che se ne occupa, alle tariffe sopra indicate, ha in carico anche altre pubblicazioni).

Se da una parte ringrazio l'UNINFO per aver emendato le modalità di iscrizione, ritengo che qualche riflessione in materia andrebbe fatta, ma non so in quale sede, sul fatto che chi lavora

(volontariamente) alle norme deve pagare cifre a mio parere molto elevate.

****

05- Best practices: ITILv3.5

OGC ha pubblicato gli obiettivi per l'aggiornamento di ITIL (da ITSM News - February 24, 2010)
http://www.best-management-practice.com/gempdf/Scope_and_Development_Plan_ITIL_V3_Update.pdf

****

06- Best practices: Business Continuity

Da Franco Ferrari (DNV Italia): il Manchester Business Continuity Forum mette a disposizione interessanti documenti sulla Business Continuity.

Pagina "MBCF Publications, Resources and Templates"
http://www.manchester.gov.uk/info/100002/business/2540/business_continuity_management/10

Business Impact Analysis Template
http://www.manchester.gov.uk/site/scripts/download_info.php?fileID=5589

****

07- Normativa: Privacy e Responsabilità Amministrativa (231/2001)

Sulla newsletter di Filodiritto del 1 marzo 2010 vi è la segnalazione dell'intervento del Garante Privacy in riferimento alla disciplina portata dal Decreto Legislativo 231/2001 in materia di responsabilità da reato degli enti.
http://www.filodiritto.com/index.php?azione=visualizza&iddoc=1763&newsfrom=2334

Sempre su Filodiritto, a proposito di 231:
- articolo del Dott. Faustino Petrillo su "Organismo di Vigilanza e Corporate Governance"
http://www.filodiritto.com/index.php?azione=visualizza&iddoc=1723
- articolo dell'Avvocato Maurizio Areno sulla sentenza di assoluzione dell'ente per responsabilità ex 231
http://www.filodiritto.com/index.php?azione=visualizza&iddoc=1698

****

08- Normativa: Dematerializzazione (Nuovo CAD, OMAT 2010, Codice ambientale, Delibera CNIPA, Moneta Elettronica)

Il nuovo Codice dell'Amministrazione Digitale (CAD)

Il Dlgs 82/2005 (Codice dell'Amministrazione Digitale) dovrebbe essere in fase di revisione da parte del Governo
http://www.governo.it/GovernoInforma/Dossier/codice_amministrazione_digitale/

Le intenzioni sono più che condivisibili. Come al solito, bisognerà vedere nella pratica cosa succederà, visto che questo dispositivo di legge non ha solo impatti sulla Pubblica Amministrazione, ma su tutte le imprese.

Su questo tema, ci sarebbe da riflettere anche sul livello culturale di quello che io chiamerei "cittadino mediamente tecnologizzato": accetta sì i documenti via mail, ma purché siano scansioni di documenti firmati e timbrati, senza pensare che (a quel punto) timbro e firma possono essere considerati ridondanti. Per non parlare poi delle altre centinaia di esempi di burocrazia "vecchio stampo" che si incastra in modi imprevedibili con le nuove tecnologie.

OMAT 2010

Segnalo OMAT 2010 a Milano
http://milano2010.omat360.it/

Codice ambientale

Il regolamento di attuazione del Decreto Legislativo 152/06 (Codice ambientale) ha istituito il «sistema di controllo della tracciabilità dei rifiuti» (SISTRI), sistema di monitoraggio informatico diretto a sostituire il regime cartaceo.
http://www.filodiritto.com/index.php?azione=visualizza&iddoc=1752&newsfrom=2318

Delibera CNIPA sul riconoscimento del documento informatico

Grazie ad un articolo di Luca De Grazia su postilla.it (http://lucadegrazia.postilla.it/2009/12/09/riconoscimento-e-verifica-del-documento-informatico/) mi accorgo con ritardo della pubblicazione delle nuove regole di riconoscimento e verifica del documento informatico del CNIPA (ora DigitPA).

La Delibera del Cnipa è la 45 del 21 maggio 2009, pubblicata sulla Gazzetta Ufficiale 282 del 3 dicembre 2009.

La Delibera abroga le precedenti AIPA numero 24 e CNIPA numero 4 e 34.

Se non faccio male i conti, inoltre, rimangono ancora parzialmente in vigore, fino al 30 agosto 2010, le Delibere del CNIPA 4 e 34 (il calcolo è fatto sulla base dell'articolo 29 della Delibera).

Sul web si trova una versione html della Delibera:
http://www.isfol.it/Normativa/Dettaglio_Normative/index.scm?id=18594

Decreto legislativo Moneta Elettronica

Entrerà in vigore il 1 marzo 2010 il Decreto Legislativo 11/2010 che recepisce la Direttiva comunitaria 2007/64 sui requisiti dei servizi di pagamento nel mercato interno. In particolare, il Dlgs regolamenterà gli strumenti di pagamento di "moneta elettronica"
http://www.camera.it/parlam/leggi/deleghe/10011dl.htm

****

09- Normativa: Responsabilità degli ISP (Sentenza di Google e Dlgs 70/2003)

Come non riflettere sulla sentenza che incrimina Google perché un utente ha caricato su un servizio "tipo-Youtube" un filmato discutibile, che Google ha provveduto a cancellare non appena ricevuta notizia?

Io direi che l'articolo di Cammarata esponga ottimamente le perplessità in merito:
http://www.mcreporter.info/sistema/google.htm

La sentenza (che richiama anche altre sentenze made in USA) è stata discussa in tutto il mondo (da SANS NewsBites Vol. 12 Num. 16):
http://www.nytimes.com/2010/02/25/technology/companies/25google.html?ref=technology
http://news.bbc.co.uk/2/hi/technology/8533695.stm
http://www.technewsdaily.com/italian-conviction-of-employees-threatens-entire-internet-100224-0245/
http://www.informationweek.com/news/hardware/utility_ondemand/showArticle.jhtml?articleID=223100601

Altre recenti sentenze sullo stesso tema sono passate un poco inosservate:
1- il Tribunale di Roma si pronuncia in sede cautelare sulla richiesta di RTI per la rimozione e l'inibitoria nei confronti di You Tube alla diffusione in rete di contenuti riproducenti sequenze di immagini relative al programma Grande Fratello. Pur senza voler affermare un obbligo di

sorveglianza generale del provider rispetto al contenuto dei dati trasmessi conformemente al disposto dell'art.17 D.Lgs 70/2003 direttiva sul commercio elettronico ("il prestatore non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza"), non appare nemmeno ragionevole sostenere l'assoluta estraneità alla commissione dell'illecito, posto che le reclamanti hanno continuato la trasmissione del Grande Fratello nei loro siti internet, organizzando la gestione dei contenuti video anche a fini pubblicitari [...]. Non si tratta quindi di pretendere dal provider un'attività preventiva di controllo e di accertamento di ciascun singolo frammento caricato dagli utenti ma di rimuovere materiale illecitamente trasmesso, dopo aver avuto conoscenza dall'avente diritto a mezzo di diffide della sua presenza in rete con conseguente denunciata lesione di diritti esclusivi, e ciò senza dover attendere apposito ordine, come pretenderebbe di fare la reclamata You Tube, da parte dell'autorità giudiziaria.
(Tribunale Civile di Roma - Sezione specializzata in materia di proprietà industriale ed intellettuale, Ordinanza 11 febbraio 2010).
- la Cassazione (49437/2009 -- http://www.filodiritto.com/index.php?azione=archivionews&idnotizia=2231) ha recentemente stabilito che "l'articolo 17 del Decreto Legislativo 70/2003 esclude sì un generale obbligo di sorveglianza nel senso che il provider non è tenuto a verificare che i dati che trasmette concretino un'attività illecita, segnatamente in violazione del diritto d'autore, ma – congiuntamente all'obbligo di denunciare l'attività illecita, ove il prestatore del servizio ne sia comunque venuto a conoscenza, e di fornire le informazioni dirette all'identificazione dell'autore dell'attività illecita – contempla che l'autorità giudiziaria possa richiedere al prestatore di tali servizi di impedire l'accesso al contenuto illecito (art.17, comma 3)".

****

10- Decisione UE contro "monitoraggio" da parte USA

Il Parlamento dell'Unione Europea, inoltre, ha bocciato la richiesta degli USA di poter accedere alle transazioni bancarie dei cittadini UE. Finalmente una notizia politica che mi mette di buon umore. Anche se il fatto che gli USA vogliano svolgere mansioni di polizia anche all'estero mi inquieta
http://www.theregister.co.uk/2010/02/11/europe_rejects_data_share/

****

11- Computer Forensics

Si trovano in linea le slides dell'intervento dell'Avv. Marcello Bergonzi Perrone presso l'Università di Milano su "Investigazioni digitali nel diritto di famiglia"
http://www.facebook.com/l/c4c60;forensics.typepad.com/files/intervento-avv.-marcello-bergonzi-perrone.pdf

La relazione dell'avvocato Bergonzi Perrone è inclusa in una serie di incontri del corso di perfezionamento post-laurea in Computer Forensics organizzato dall'Università Statale di Milano. Tutte le slides finora prodotte si trovano su
http://www.facebook.com/l/c4c60;forensics.typepad.com/computer_forensics/materiali-2010.html

(grazie a Giovanni Ziccardi per la segnalazione e la messa a disposizione del materiale)

****

12- Project Management

Da ITSM News - February 24, 2010 vi segnalo l'interesante articolo sul project management
http://www.cioupdate.com/insights/article.php/3866441/Reinventing-IT-Project-Management---Peter-Drucker-Style.htm

****

13- Presentazioni

Il 17 febbraio e il 3 marzo ho presentato per le sessioni di studio di Milano e Roma dell'AIEA alcune riflessioni su come si conducono i risk assessment e su VERA, la metodologia molto

semplice
http://www.cesaregallotti.it/art_pres/20100303-Presentazione%20AIEA-Roma.pdf