[IT Service Management News]
Newsletter del 15 luglio 2010

****
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
- scrivendo a cesaregallotti@cesaregallotti.it
- seguendo le istruzioni riportate nella pagina http://www.cesaregallotti.it/newsletter.htm.
Sulla stessa pagina è possibile consultare l'informativa sul trattamento dei dati personali.

****
Indice

****
1- Novità privacy (videosorveglianza; spamming)

Videosorveglianza

Dalla newsletter di Filodiritto trovo la notizia di una sentenza importante della Cassazione: "Utilizzabili le videoriprese del lavoratore che ruba".

Mi pare una sentenza che getta nuove interpretazioni in merito ai rapporti tra Privacy, Statuto dei Lavoratori e controlli "a distanza". Mi auguro che qualcuno dei miei 11 lettori ci segnali qualche articolo di approfondimento.

Questo l'articolo della newsletter di Filodiritto:

<<
Sulla utilizzabilità a fini penali delle videoriprese effettuate con telecamera installata all'interno di un bar dal datore di lavoro per dimostrare il furto effettuato dalla cassiera, la Cassazione ha stabilito che "gli articoli 4 e 38 dello Statuto dei lavoratori implicano l'accordo sindacale a fini di riservatezza dei lavoratori nello svolgimento dell'attività lavorativa, ma non implicano il divieto dei cd. controlli difensivi del patrimonio aziendale da azioni delittuosi da chiunque provenienti. Pertanto in tal caso non si ravvisa inutilizzabilità ai sensi dell'articolo 191 Codice Procedura Penale di prove di reato acquisite mediante riprese filmate, ancorché sia perciò imputato un lavoratore subordinato".

La Cassazione ha ricordato che è stata riconosciuta la legittimità in sede civile dei cosiddetti "controlli difensivi": "Ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a

distanza dell'attività dei lavoratori previsto dall'art. 4 L. n. 300 del 1970, è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dell'ambito di applicazione della norma sopra citata i controlli diretti ad accertare condotte illecite del lavoratore" (Cass. sez. L n. 4746/02, Securpol srl / Pizzutelli M., CED rv. 553469, e v. n. 15892/07, Piluso / Eni spa, che appunto esclude il controllo che abbia per fine proprio le concrete modalità lavorative). In sintesi, la finalità di controllo a difesa del patrimonio aziendale non è da ritenersi sacrificata dalle norme dello Statuto dei lavoratori".
>>

E invece qui ho trovato il testo della sentenza:
http://ziczac.it/a/leggi/014261a250704ef37ab70a3f19538f82/

Spamming

Da Newsletter Garante privacy del 24 giugno 2010, si trova la notizia "Fax e mail promozionali: illeciti senza consenso - Il Garante ribadisce le regole contro lo spamming"

Di seguito, il copia-incolla dell'articolo. Ma colgo l'occasione per fare l'ennesima critica alle comunicazioni del GPDDPP: perché non ha messo i riferimenti dei Provvedimenti segnalati per renderne più facile la ricerca ai lettori?

<<
Continua la battaglia del Garante privacy contro lo spamming.
L'Autorità, a seguito di segnalazioni di imprese, enti e singoli cittadini, ha vietato l'ulteriore trattamento di dati personali a quattro società che inviavano pubblicità tramite fax o e-mail senza aver acquisito il consenso preventivo e specifico dei destinatari.
Tre di esse spedivano sistematicamente fax promozionali credendo di poter disporre liberamente dei dati, estratti da elenchi categorici (Pagine Gialle, Pagine Utili, ecc.) o pubblici (ad es. banche dati delle Camere di commercio, albi professionali, ecc.).
Nel quarto caso, un messaggio via mail era stato inviato da una società che aveva rintracciato il recapito del destinatario sul web. La società che aveva effettuato lo
spamming, si era considerata libera di poter disporre dei dati di un'altra azienda che si era registrata su un sito fieristico.
Con quattro distinti provvedimenti il Garante ha riaffermato il principio che, a prescindere da dove vengano estratti i recapiti, chiunque invii messaggi promozionali mediante sistemi automatizzati (fax, e-mail, sms, mms), è sempre obbligato a raccogliere preventivamente il consenso specifico ed informato dei destinatari.
Il mancato rispetto del divieto, ha ricordato il Garante, comporta le sanzioni amministrative e penali previste dal Codice privacy. Per il risarcimento di eventuali profili di danno le vittime dello spam possono comunque far valere i propri diritti in sede civile.
La battaglia del Garante contro i fax indesiderati incontra tuttavia serissimi ostacoli nella differenza tra le legislazioni degli Stati europei. Diversi sono infatti i Paesi, come ad esempio la Gran Bretagna e la Francia , nei quali la disciplina sulla protezione dei dati personali non garantisce le persone giuridiche e che pertanto impedisce all'Autorità omologa a quella italiana di poter contrastare l'invio di fax senza consenso diretto a ditte, enti o società. Si tratta di un fenomeno che preoccupa l'Autorità italiana perché ne limita la capacità di intervento e dimostra che l'armonizzazione tra le legislazione in materia di protezione dati è ancora incompiuta.
>>

****

2- Standardizzazione (ISO PAS 22399; ISO/IEC 20000-5)

Business Continuity: ISO PAS 22399

L'ISO ha emesso il documento dal titolo "Societal security — Guideline for incident preparedness and operational continuity management".

Si tratta di linee guida (ossia non certificabili), in qualche modo sovrapponibili alla BS 25999-1 ("Business continuity management – Part 1: Code of practice").

"ISO PAS" vuol dire che il Comitato Tecnico che l'ha emessa (il TC 233 "Societal Security") l'ha approvata con un numero di voti compreso tra il 50% e il 66% (se è tra il 66% e il 75% diventa un ISO TR, se supera il 75% è un International Standard). Ciò non ne diminuisce la futura portata, soprattutto se verranno emessi i requisiti per la certificazione (ISO 22301).

Rimango, come al solito, scettico nei confronti di quasi tutte le linee guida emesse dall'ISO: troppo generiche per essere veramente utili.

ISO/IEC TR 20000-5

E' stata pubblicata il 1 maggio 2010 la ISO/IEC TR 20000-5 dal titolo "Exemplar implementation plan for ISO/IEC 20000-1".

Anche a questa sono applicabili i miei soliti commenti sulle linee guida della ISO. Su questa, però, ho però ulteriori dubbi: è inutile per chi conosce bene la norma perché è già al corrente di come pianificare gli interventi presso un IT Service Provider che intende conformarsi alla ISO/IEC 20000-1; è inutile per chi conosce poco la norma perché non è avendo queste poche indicazioni che può pensare di far partire un progetto di messa in conformità alla ISO/IEC 20000-1.

La parte interessante di questo documento è questa riflessione: l'implementazione di un ITSMS può esere condotta in 3 fasi: nella prima si implementano i requisiti "di sistema" (capitoli 3 e 4 dello standard) e i processi di SLM, Service Reporting, Budgeting & Accounting, Information Security, BRM, IM, Configuration e Change; nella seconda i processi di SACM, Capacity, Supplier, Problem e Release; nella terza il processo di pianificazione e implementazione dei nuovi servizi.

Tutte queste cose saltano all'occhio a chiunque cominci ad elaborare un piano di azione per un'azienda che intenda implementare un ITSMS (esperienza personale!)

****

3- Certificazione dei software rispetto a ITIL

Sulla ITSM Newsletter trovo la notizia che APM Group, l'ente di accreditamento ufficiale per le certificazioni software rispetto a ITIL, ha pubblicato i criteri da soddisfare per essere riconosciuti in tal senso.
http://www.itil-officialsite.com/SoftwareScheme/ITILSoftwareScheme.asp

ITSkeptic dice la sua su
http://www.itskeptic.org/itil-product-compliance-criteria-are-no-longer-sec

Io dico la mia: lo schema non è convincente perché si basa, tra l'altro, sul numero di clienti che hanno comprato la soluzione. Inoltre: le aziende devono prima imparare a capire cosa vogliono e come valutare rispetto alle proprie esigenze i prodotti. Requisiti generali come questi non possono sostituire l'analisi da parte del potenziale utilizzatore, che deve comprendere innanzitutto di cosa ha bisogno per i PROPRI processi.

Purtroppo lo so che quasi tutti prima decidono cosa comprare e poi valutano se gli serve veramente (insomma, come se fossero in giro per shopping il sabato pomeriggio... con i soldi dell'azienda e gli impicci degli utenti).

****

4- Dare in outsourcing l'application management: qualche rischio

Vado dai clienti e faccio notare che dovrebbero controllare meglio i propri sviluppatori. Insomma, non fidarsi proprio al 100%. Auguro a tutti che non succeda mai nulla.

Intanto, da SANS NewsBites trovo l'altro caso estremo (sviluppatori criminali): in Spagna sono stati arrestati 3 sviluppatori perché nel codice hanno installato delle "logic bomb" che avrebbero mandato in crash il prodotto dopo qualche tempo e costretto il cliente a chiedere (e pagare...) della manutenzione straordinaria.
http://www.theregister.co.uk/2010/06/25/spanish_logic_bomb_probe/

Ripeto, questo è un caso estremo, così come è estremo fidarsi al 100% degli sviluppatori.

Riporto anche la segnalazione di SANS Newsbyte di uno storico articolo in materia:
http://cm.bell-labs.com/who/ken/trust.html

****

5- Rischi IT

Interessante articolo sull'Isaca Journal intitolato "IT Risk Analysis—The Missing “A”".

In poche parole, l'articolo ricorda che i rischi IT (e non solo, direi) possono essere categorizzati in rischi di disponibilità (availability) accesso, accuratezza e agilità (le quattro “A’s”). Normalmente ci si focalizza solo sulle prime 3.

L'articolo spiega un aspetto molto importante della nostra percezione del Risk Management: solitamente ci focalizziamo nella sua efficacia (fare le cose giuste), molto raramente nella sua efficienza (fare le cose nel modo giusto): pensiamo a compilare moduli, a stabilire diversi livelli di autorizzazione, a imporre diversi livelli di controllo senza mai porci il problema della semplicità di tali processi.

Bisogna riflettere sul fatto che, alla fine, un processo inefficiente diventa inefficace. Esempi banali di cui sono stato testimone: se bisogna cambiare la password di 10 caratteri ogni 15 giorni, inesorabilmente qualcuno comincia a scriverla su un post-it; se bisogna mettere troppi dettagli su un modulo, inesorabilmente qualcuno applica un copia/incolla selvaggio; se bisogna tenere chiuse troppe porte, inesorabilmente qualcuno utilizza un estintore per lasciare aperte quelle che è più comodo e non rischioso tenere aperte.

L'articolo presenta esempi meno banali dei miei.

http://www.isaca.org/Journal/Past-Issues/2010/Volume-3/Pages/IT-Risk-Analysis-The-Missing-A.aspx

****

6- I sette errori di comunicazione

Sembrano banali, ma non lo sono nella pratica: quante volte ho sentito manager mentire, pensare di avere a che fare con stupidi, omettere cose troppo evidenti per poter essere omesse.

In questo articolo che ce ne sono altre 4:
http://blogs.hbr.org/hmu/2009/03/seven-communication-mistakes-m.html