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: Monday, 16 March, 2009 17:56
To: Mailing list
Subject: [IT Service Management] Newsletter del 16 marzo 2009
Attachments: ATT00096.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

****
Indice

****
1- Privacy: Proroga per gli amministratori di sistema
(Da Franco Ferrari del DNV)

Il Garante, con Provvedimento del 12 febbraio 2009, ha prorogato i termini per l'adozione delle misure che riguardano gli "amministratori di sistema". Le regole erano state fissate dal Garante con il provvedimento del 27 novembre 2008.

Due considerazioni:
1- se per adempimenti "semplici", come il DPS e le misure minime, abbiamo assistito a continue proroghe fino a raggiungere i 3 anni, cosa dobbiamo prevedere per queste misure decisamente più complesse?
2- per gli utenti "normali" si richiede l'aggiornamento dell'antivirus annuale o semestrale (quando le best practices e la tecnologia spingono verso aggiornamenti almeno quotidiani), per gli amministratori di sistema si richiede che i log sugli accessi siano "inalterabili" (quando, per molti sistemi, l'adozione di questa misura richiede aggiornamenti tecnici non banali): è possibile chiedere al Garante di individuare un livello di sicurezza omogeneo a cui fare riferimento?

Il Provvedimento di proroga
http://www.garanteprivacy.it/garante/doc.jsp?ID=1591970

Il Provvedimento del 27 novembre sugli Amministratori di Sistema
http://www.garanteprivacy.it/garante/doc.jsp?ID=1577499

****
2- Conversione in Legge del DL "Anti-crisi" (PEC e archiviazione ottica)

Il DL 185/2008, con le novità in materia di Posta Elettronica Certificata e archiviazione ottica, è stato convertito in Legge.

Sono stati corretti alcuni errori, con impatto sulla privacy, in merito alla PEC ed è stato modificato il codice civile introducendo un concetto esteso di Documentazione informatica.

Il testo della Legge:
http://www.parlamento.it/parlam/leggi/elelenum.htm

Il mio consolidamento del DPR 68/2005 (PEC) e DLgs 82/2005 (Amministrazione digitale):
http://www.cesaregallotti.it/normativa/Gestione_documentale/2005_DPR_68_regolamento_posta_certificata.htm
e
http://www.cesaregallotti.it/normativa/Gestione_documentale/2005_Dlgs_82_Codice_amministrazione_digitale.htm

****

3- Statistiche sulla sicurezza

Vi segnalo diversi studi con statistiche sulla sicurezza

- Computer Security Institute (fino al 2006 nota come "CSI/FBI survey"):
http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf

- Ernst & Young
http://www.ey.com/Global/assets.nsf/International/TSRS_Global_Information_Security_Survey_2008/$file/TSRS_Global_Information_Security_Survey_2008.pdf

- Price Waterhous Coopers
http://www.pwc.com/extweb/insights.nsf/docid/0E50FD887E3DC70F852574DB005DE509/$File/Safeguarding_the_new_currency.pdf

****

4- Sicurezza: documenti tecnici

Il NIST ha pubblicato la bozza della Special Publication 800-46 Revision 1, dedicata alla sicurezza in materia di telelavoro e accesso remoto. Le guide del NIST sono sempre le mie preferite.
http://csrc.nist.gov/publications/PubsDrafts.html#800-46-rev1

Un consorzio USA ha emesso una lista di 20 controlli di sicurezza fondamentali, correlati agli attacchi che contrastano.
http://www.sans.org/cag/

****

5- I lavori per la nuova ISO/IEC 27001

Sono inziati i lavori per la nuova ISO/IEC 27001.

A livello italiano, sono stati raccolti i primi commenti (tra cui i miei) e saranno successivamente discussi.

****

6- Sulle certificazioni PCI e non solo

La Heartland, società di servizi di pagamento che ha subito un attacco informatico con compromissione dei dati delle carte di credito gestite, ha dichiarato che era certificata secondo le specifiche PCI e per questo motivo cercherà di difendersi da ogni tipo di azione legale in cui dovesse essere coinvolta.
(da SANS NewsBites Vol. 11 Num. 16)

Questa vicenda ci ricorda che "essere certificati" (PCI DSS, ISO/IEC 27001 e quant'altro) non vuol dire "essere sicuri". Ma ci ricorda anche che una certificazione può comunque essere utile per dimostrare che "si è fatto il possibile" e per non essere accusati per noncuranza o inadempienza.

Per leggere l'articolo (con ulteriori considerazioni in merito ai recenti attacchi subiti da varie società di servizi):
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9128658&source=rss_topic17

Il sito degli standard PCI
https://www.pcisecuritystandards.org/

****

7- Usabilità

Pare che in Australia, nel Queensland, la polizia stia arrestando sempre meno persone perché il personale fa fatica a lavorare con il nuovo sistema informatico di registrazione degli arresti.
http://www.news.com.au/couriermail/story/0,23739,24723327-952,00.html
(da Crypto-gram del 15 febbraio 2009)

Il problema dell'usabilità è purtroppo sottovalutato dagli sviluppatori (per mancanza di tempo, perché non formati in merito, perché poco interessati all'argomento "poco tecnico") e, ahimé, dai committenti (per non competenza o per volontà di fare economia)

Ho visto (e subìto) troppi software che avrebbero fatto anche il caffè... se si fosse capito come dirglielo. Quindi, capisco i poliziotti australiani.

Purtroppo, le best practices più diffuse (tra cui ITIL) mette poco l'accento su questo aspetto fondamentale. Fa piccola eccezione la sola ISO/IEC 9126/2007 che lo mette tra gli aspetti da valutare in un software. Nell'ITILv4, quando e se verrà, sarebbe bello se gli si desse maggior rilievo nel Service Design.

****

8- I rischi dei Social network

Dal Corriere della Sera di qualche giorno fa, leggo che, in Inghilterra, l'azienda Ivell ha licenziato una ragazza perché aveva scritto su Facebook che il suo lavoro "è noioso".

Il Corriere richiama anche il caso di alcuni impiegati di Marks & Spencer che, sempre su Facebook, definiscono "idioti" i clienti e sono quindi licenziati; di dipendenti (anche loro licenziati) della British Airways che definiscono "puzzolenti e fastidiosi" i passeggeri della compagnia, di altri dipendenti della Virgin che invece accusano i passeggeri di essere degli "zotici".

Lascio a sociologi e analisti le riflessioni sull'eccesso di permalosità dei responsabili dell'Ivell e sull'eticità dimostrata dai protagonisti di queste vicende.

Mi soffermo su due aspetti.

1- i licenziati di cui sopra hanno diffuso i loro pensieri, quasi sicuramente ben sapendo che non sarebbero stati graditi dalle proprie aziende. Eppure... l'hanno fatto, senza considerare gli impatti che questa azione avrebbe avuto sulla loro azienda e sul proprio lavoro. Quando si parla di sensibilizzazione del personale, è bene pensare anche a questo tipo di destinatari, non solo a quelli che eccedono nello spirito di servizio, come la maggioranza di quelli descritti da Mitnick nel suo "L'arte dell'inganno".

2- i licenziati hanno pubblicato i propri pensieri senza riflettere che qualche giornalista o qualche loro capo avrebbe potuto leggerli. Sicuramente non hanno pensato a questi rischi. Mi sono permesso di collegare questo episodio agli "omissis del caso Calipari" e al "documento Word con le revisioni attive e pubblicato dalla 3Com", oltre ai casi che mi sono capitati della "procedura così ben protetta che non ho potuto fare il 'cerca'" e di un certificato che non posso pubblicare sul mio sito perché protetto da password (a che mi serve un certificato se non lo posso far leggere agli altri?). Li collego tutti al fatto che la tecnologia può essere bella e utile, ma deve essere utilizzata con prudenza... molta prudenza.

Trovate ulteriori dettagli sui casi di licenziamento:
http://www.mirror.co.uk/news/top-stories/2009/01/11/exclusive-marks-spencer-staff-ridicule-customers-on-facebook-115875-21033664/

****

9- Cassazione e furto di identità
(da Filodiritto del 23 febbraio 2009)

Vi segnalo questa interessante notizia (che copio integralmente), perché sarà interessante valutarne gli impatti nel futuro:

"Un soggetto agisce nei confronti di alcuni istituti di credito per i danni patiti a causa dell'apertura di conti correnti muniti di convenzione assegni a favore di un terzo che, a tal fine, aveva presentato come documento di identità la patente di guida di cui il primo aveva denunciato lo smarrimento due anni innanzi. La vittima del furto d'identità ricorre in Cassazione avverso la sentenza con la quale la Corte d'appello ha assolto gli istituti di credito citati, compensando le spese di giudizio.

La Cassazione ha rigettato innanzitutto la tesi del ricorrente rilevando che "Va disatteso il richiamo all'articolo 2050 Codice Civile non potendosi l'attività bancaria considerare attività pericolosa, di per sé od in relazione alla natura dei mezzi adoperati, nei termini di cui alla citata norma, come si è venuta storicamente formando e come viene normalmente interpretata. L'attività bancaria può indubbiamente sollecitare (più di altre) iniziative e comportamenti illeciti da parte di terzi, anche pericolosi per l'incolumità altrui. Né si può escludere che in futuro - con il moltiplicarsi del numero e della potenzialità dannosa degli illeciti - possano essere elaborate regole peculiari e più ampie di imputazione della responsabilità, a tutela degli utenti dei servizi bancari. Ad oggi, l'esercizio dell'attività bancaria si considera mera occasione dell'esposizione a pericolo del patrimonio od anche dell'incolumità fisica della clientela; non invece la causa prima ed originaria dei corrispondenti rischi".

Tuttavia, secondo la Cassazione "la motivazione della Corte di appello appare illogica e contraddittoria sotto svariati profili". In particolare, secondo la Cassazione, "In primo luogo perché richiama la non esigibilità di controlli particolarmente sofisticati da parte della banca, mentre nella specie si trattava di verificare se fossero stati effettuati i controlli minimi indispensabili al fine di identificare il cliente, cioè la verifica della corrispondenza della fotografia riportata sul documento alla persona del richiedente il servizio. In secondo luogo perché incorre in una vera e propria petizione di principio, quando afferma che la foto era da presumere somigliante perché il falso non è stato riconosciuto, dando così per dimostrato il fatto che l'impiegato allo sportello avesse controllato il documento e la fotografia, circostanza che era invece da dimostrare. Il fatto che il documento non fosse stato in alcun modo falsificato o alterato induce a presumere che lo scambio di identità fosse immediatamente riconoscibile (come è stato in effetti riconosciuto da altro operatore economico, a breve distanza di tempo)".

In conclusione la Cassazione ha rilevato che "Risultando in fatto dimostrati il furto di identità e l'utilizzazione da parte del reo di un documento altrui in nulla alterato o modificato, la riconoscibilità dell'abuso era da ritenere in re ipsa, e da presumere fino a prova contraria. Era a carico della banca, quindi, e non del danneggiato, l'onere di fornire la prova della scusabilità del suo errore (per la somiglianza fra le due persone o per altra causa), contrariamente a quanto ha affermato la Corte di appello".

(Corte di Cassazione - Sezione Terza Civile, Sentenza 11 febbraio 2009, n.3350: Apertura di conto correnti con convenzione assegni - Furto d'identità - Valutazione dell'errore della banca - Onere della prova dell'errore scusabile - Risarcimento danni a favore del soggetto danneggiato)."

****

10- Errata Corrige

La volta scorsa avevo indicato che Max Cottafavi lavora per "Spike Replay", quando invece il nome dell'azienda ha una "a" in meno e si chiama "Spike Reply"; mi scuso con lui e con i suoi numerosi colleghi ;-)

_____
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