****
IT SERVICE MANAGEMENT NEWS – APRILE 2011
****

Newsletter mensile con novità in materia di sicurezza delle informazioni, IT Service Management, Qualità. E' possibile dare il proprio contributo e diffonderla a chiunque.

IT Service Management News è rilasciata sotto la Creative Commons Attribution 3.0 Unported License (http://creativecommons.org/licenses/by/3.0/deed.it). Bisogna attribuire il lavoro a Cesare Gallotti con link a http://www.cesaregallotti.it/Newsletter.html

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- Privacy: dei Titolari e dei Responsabili esterni

Su LinkedIn, nel gruppo del Clusit, è stata sollevata la questione di un'azienda che fa monitoraggio della rete e configurazione degli apparati ed è stata nominata Responsabile Esterno da un cliente. Inoltre, il cliente ha deciso di "nominare" gli amministratori di sistema del fornitore.

Ho rabbrividito e ho risposto così:

1- Nella "nuova" Legge Privacy (Dlgs 196) il Titolare è stato definito in modo sottilmente diverso dalla "vecchia" 675/96. In particolare, nella nuova definizione, al Titolare "competono, anche unitamente ad altro titolare, le decisioni...". E' stato aggiunto "anche unitamente ad altro titolare" (Articolo 1 lettera d della Legge 675/1996 e Articolo 4 lettera f del Dlgs 196/2003).

Io interpreto così: clienti e fornitori possono essere Titolari autonomi, una volta che si sono definite le finalità di ciascuno (nel caso in questione, "monitoraggio e configurazione della rete IT") e il profilo di sicurezza (dal semplice "rispetto della normativa privacy" ad una serie di procedure concordate tra le parti).

Andando avanti con il ragionamento: io quindi dovrei nominare Responsabile esterno la mia banca, il mio ISP e operatore mobile (Wind), mio gestore del telefono fisso e ADSL (Telecom), le Poste Italiane? Dovrei quindi chiedere loro i nominativi degli AdS? Dovrò fare loro delle verifiche (Articolo 29 comma 5 del Dlgs 196/2003)? A sua volta, il Responsabile esterno come
può interfacciarsi con i propri fornitori, visto che un responsabile non può nominare responsabili ma solo

incaricati?

Ancora: lo studio legale che ha dato quelle belle interpretazioni è stato nominato Responsabile Esterno? Permetterebbe al Titolare di fare "verifiche periodiche" presso i suoi uffici? Gli ha dato il nominativo dei propri AdS (alla fine anche lo studio legale avrà un server o dei pc)?

E' ovvio che è un modello che non sta in piedi. E purtroppo tutti si trascinano dietro le interpretazioni pre-2003 e continuano a nominare Responsabili esterni i fornitori.

Rimane solo una possibiltà perché il tutto regga: il fornitore è un Titolare autonomo, che tratterà i dati solo per eseguire il contratto (finalità) e con misure di sicurezza concordate con il cliente (dal "solo" rispetto della normativa a cose più complesse).

Infine: nel Dlgs 196/2003 (ultima verione da consultarsi su www.normattiva.it), non si nomina MAI il "Responsabile esterno".

2- Anche se il fornitore fosse stato nominato Responsabile, il Titolare non deve avere a disposizione i nominativi degli AdS. Questo lo diceva il Provvedimento del 28 novembre del 2008. Poi modificato opportunamente il 25 giugno del 2009. Ora dice "il titolare o il responsabile del trattamento devono conservare i nominativi". E' stato incluso il responsabile (con una bella "o" tra lui e il Titolare), che lo dovrà mantere disponibile in caso di accertamenti.

Ma ancora una volta, sembra che non sia prassi tenersi aggiornati.

3- Dopo il mio post su LinkedIn, Mauro Cicognini concorda con me e mi conferma che non sono solo a vederla così. Aggiunge che "l'unica complicazione è che naturalmente tutti i Titolari devono essere riportati nell'informativa".

Io dico che il Codice Privacy impone (articolo 13, comma 1, punto d) di riportare nell'informativa i titolari e i responsabili. Quindi la mia interpretazione non complicherebbe la cosa rispetto a chi nomina "responsabili esterni" e non "titolari esterni".

Il Dlgs dice che nell'informativa vanno riportati: "i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualita' di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi".

Proviamo a riscriverla, senza modificazioni di rilievo ma cercando di dare un'interpretazione: nell'informativa vanno riportati: "1- i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati, 2- i soggetti o le categorie di soggetti che possono venirne a conoscenza in qualita' di responsabili o incaricati, 3- l'ambito di diffusione dei dati medesimi".

E' una forzatura? Certo. Ma anche nominare degli esterni come "Responsabili" che poi a loro volta nomineranno dei "Responsabili" è una forzatura. Oppure nominare degli esterni come "Responsabili" e non fargli mai le verifiche periodiche è una forzatura (alla banca, per esempio). Oppure scrivere nome e cognome di alcuni responsabili o co-titolari nell'informativa e non inviarla ad ogni aggiornamento è una forzatura.

Forzare per forzare, scelgo di forzare utilizzando un modello coerente, in linea con ogni prassi gestionale di processi e di sicurezza, in linea con quanto previsto nel resto dell'Europa (dove la Direttiva 95/46/CE è ovviamente applicata). E scelgo di non aggrapparmi ad un modello fuori da ogni logica e neanche "a prova di contestazione".

Ci sarebbe da riflettere mestamente su tanti (troppi) professionisti che seguono come buoi il primo che dice una fesseria: la custodia delle password in busta chiusa per migliaia di persone da moltiplicare per decine di sistemi, il DPS come cosa complessissima che ha richiesto anni di proroghe, richieste di consenso inutili ancora in circolazione, eccetera.

La smetto qui. Ma se ci sono controdeduzioni da proporre, sarò contento di pubblicarle (e di rispondere e di pubblicare le risposte e così via; fino a che nel botta-risposta ci saranno cose intelligenti).

****

02- Italiani, brava gente?

Ieri 14 aprile, alla sessione di studio dell'AIEA a Milano, Tamara Devalle e Tiziana Boffi di Protiviti hanno presentato i risultati di una ricerca sull'organizzazione IT nelle aziende italiane. Il quadro non è certo confortante.

Al termine della presentazione, un partecipante ha detto il solito luogo comune: "molti problemi sono propri di noi italiani".

Ho dovuto intervenire facendo notare che non è vero. Le mie esperienze all'estero o con multi-nazionali e le notizie e articoli da tutto il mondo dimostrano che le difficoltà dell'IT sono comuni.

Il problema del luogo comune "l'IT va male in Italia perché gli italiani non seguono le procedure, non sono educati, eccetera" è che poi diventa una giustificazione per i manager che non sanno convincere e spiegare e inserire una cultura aziendale adeguata, per i consulenti e i vari responsabili che scrivono procedure illeggibili e contorte, per i vertici aziendali che operano cambi organizzativi solo sugli organigrammi e mai sui processi e sui loro riporti che pensano solo a raggiungere gli obiettivi della propria area e mai a capire e risolvere i problemi di interrelazione con le altre aree (e il povero IT che è trasversale se la passa male...).

Concludo pregando tutti di ribellarvi a chiunque dica "siamo noi italiani che siamo fatti così": è una comoda e sbagliata giustificazione. Se vogliamo migliorare (non l'Italia, ma la piccola realtà che ci circonda), non c'è nulla di peggio di nascondersi dietro i luoghi comuni.

La presentazione di Protiviti dovrebbe essere pubblicata su http://www.aiea.it/html/anno_2011.html.

****

03- Standardizzazione: ISO/IEC 27031 e BS 25777

Faccio seguito al post del 26 novembre 2010 che annunciava (e commentava) la prossima uscita della ISO/IEC 27031 "Guidelines for information and communication technology readiness for business continuity"
http://blog.cesaregallotti.it/2010/11/fdis-isoiec-27031.html

Il 1 marzo è stata pubblicata la versione finale ed è disponibile dal sito della ISO.

Il BSI segnala poi che questa norma sostituisce la BS 25777.

****

04- Standardizzazione: ISO/IEC 25010 sui modelli di qualità del software

Il 1 marzo 2011 è stata pubblicata la ISO/IEC 25010 "Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models".

Lo standard definisce due modelli qualità del software: il primo "quality in use" si compone di 5 caratteristiche (efficacia, efficienza, soddisfazione, assenza di rischi e copertura) ed è relativa alle sue interazioni quando utilizzato in uno specifico contesto; il secondo "product quality" riguarda le proprietà del software e del sistema informatico e si compone in 8 caratteristiche (adeguatezza fuznionale, efficienza delle prestazioni, compatibilità, usabilità, affidabilità, sicurezza, mantenibilità e portabilità.

Questo standard sostituisce la ISO/IEC 9126-1:2001 e fa parte della serie ISO/IEC 250xx dedicata alla qualità del software. Alcuni standard della serie sono già stati pubblicati, altri non ancora.

Grazie a Franco Ferrari (DNV Italia) per la segnalazione.

****

05- Standardizzazione: ISO 28000 - Security in supply chain

Settimana scorsa, leggendo la newsletter dell'IRCA, ho trovato un articolo sulla ISO 28000:
http://www.irca.org/inform/issue29/TCummins.html?dm_i=4VM,DS56,HZSOT,151FL,1

Volevo quindi segnalarlo su questa newsletter con il titolo "ISO 28000 - Uno standard dimenticato". Ma giusto nell'ultima settimana ho avuto conferma che sta nascendo interesse per questa norma internazionale sulla sicurezza "fisica". La norma è quindi applicabile a chi opera nella logistica e nel magazzinaggio.

La sua prima versione fu emessa come ISO PAS nel 2005; la seconda e attuale versione è del 2007 come ISO IS.

Di interesse sono le seguenti parti:
- ISO 28000:2007 "Specification for security management systems for the supply chain"; è lo standard "certificabile" e ricorda molto la ISO/IEC 27001:2005;
- ISO 28001:2007 "Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance"; riporta anch'esso dei requisiti (malgrado il titolo con l'ossimoro "best practices" - "requirements"), ma l'introduzione non aiuta a comprendere la sua relazione con la 28000; il suo contenuto sembra però più una best practices per il risk assessment richiesto dalla ISO 28000;
- ISO 28004:2007 "Security management systems for the supply chain — Guidelines for the implementation of ISO 28000", riporta le best practices e cita solo la 28000 e non la 28001.

****

06- Novità legali: Servizi di vigilanza - Nuovo Decreto

Franco Ferrari (DNV Italia) mi ha segnalato l'importante entrata in vigore del Decreto 269 del 2010, o "decreto sulla capacità tecnica degli istituti di vigilanza".

Negli allegati sono riportati, tra gli altri, i requisiti di qualità che tali istituti devono soddisfare.

E' possibile consultare il Decreto in questione su www.normattiva.it.

****

07- Novità legali: Abolizione Decreto Pisanu sulle wi-fi libere (parte seconda)

A dicembre avevo segnalato l'abolizione del Decreto Pisanu che, per dirla in termini molto poplari, impediva l'apertura di wi-fi libere.
http://blog.cesaregallotti.it/2010/12/abolizione-decreto-pisanu-sulle-wi-fi.html

Navigando ho trovato sul sito di Pierluigi Perri una presentazione che mi permette ora di precisare ulteriormente la storia.

Il Decreto Pisanu NON è stato abolito, ma è stato prorogato fino al 31 dicembre 2011. Questo grazie al Decreto Legge 225 del 2010 convertito in Legge 10 del 2011 (per leggere il testo della norma, su www.normattiva.it bisogna cercare il DL 225 del 2010).

Il nuovo Decreto Legge 225, inoltre (e positivamente secondo molti), rimuove per gli esercizi pubblici che mettono a disposizione le wi-fi gli obblighi di monitoraggio delle operazioni degli utenti e di identificazione degli utenti.

E ancora, precedentemente la messa a disposizione di connettività in "un pubblico esercizio o un circolo privato di qualsiasi specie" doveva essere conseguente ad una licenza fornita dalla Questura. Ora, tale misura preventiva si applica solo agli esercizi per i quali la connettività è "l'attività principale".

Per leggere la presentazione di Pierluigi Perri:
http://pierluigiperri.com/2011/01/23/legge-pisanu-cerchiamo-di-fare-chiarezza/

PS: Pierluigi, come altri, essendo lettore di questa newsletter avrebbe potuto segnalarmi l'intervento; non lasciarmi fare il segugio del web ;-)

****

08- Attaccati (con successo) RSA e HBGary

Non si tratta di attacchi di poco conto perché hanno colpito in profondità aziende dove gli esperti di sicurezza sono ben preparati.

Il primo (notizia da Crpyo-Gram del 15 marzo) ha permesso a un gruppo di hacker (blackhat) di prelevare e pubblicare moltissime informazioni da HBGary, una società di informatica forense collaboratrice dell'FBI.

Tra le informazioni pubblicate, ve ne sono alcune compromettenti sulla stessa azienda.

Un articolo "normale":
http://arstechnica.com/tech-policy/news/2011/02/anonymous-to-security-firm-working-with-fbi-youve-angered-the-hive.ars <http://arstechnica.com/tech-policy/news/2011/02/anonymous-to-security-firm-working-with-fbi-youve-angered-the-hive.ars>

Un articolo con commenti sulle notizie compromettenti della HBGary e sui confini tra "buoni" e "cattivi":
http://threatpost.com/en_us/blogs/rsa-2011-winning-war-losing-our-soul-022211
<http://threatpost.com/en_us/blogs/rsa-2011-winning-war-losing-our-soul-022211>

Il secondo (notizia ricavata dal SANS NewsBites del 18 marzo) ha colpito informazioni sui prodotti token SecurID dell'RSA. Il calcolo dice che circa 300 milioni di clienti (o token?) sono quindi potenzialmente meno sicuri.

L'articolo di Wired: http://www.wired.com/threatlevel/2011/03/rsa-hacked/
<http://www.wired.com/threatlevel/2011/03/rsa-hacked/>

Questi due attacchi, come già detto, sono stati portati ad aziende le cui competenze di sicurezza sono molto elevate.

Lo stesso gruppo di hacker (blackhat) ha anche colpito il sito web del nostro Governo (notizia dalla DFA Newsletter del 17 marzo). Poca roba, al confronto:
http://www.webmasterpoint.org/news/governoit-sito-attaccato-e-modificata-anche-la-homepage-limmagine-e-i-motivi_p38842.html <http://www.webmasterpoint.org/news/governoit-sito-attaccato-e-modificata-anche-la-homepage-limmagine-e-i-motivi_p38842.html>

****

09- Atti del Security Summit

Il 14-16 marzo 2011 si è tenuto a Milano il Security Summit. Sono disponibili le presentazioni dei relatori su https://www.securitysummit.it/page/atti_milano_2011

Io ho assistito (e ne raccomando le slides) a:
- La sicurezza dei pagamenti e delle carte di credito (PCI-DSS)
- La computer forensics e le investigazioni digitali tra approcci pratici e rigore scientifico: un'introduzione accademica
- Seminario a cura dell'Information Technology Service Management Forum Italia (itSMF)
- Seminario a cura dell'Information Technology Service Management Forum Italia (itSMF)

Buona lettura!

****

10- Prodotti per Data Leak Prevention

L'ISACA ha pubblicato un white paper sulla Data Leak Prevention: www.isaca.org/DLP.

Lettura certamente utile, anche se il titolo è fuorviante. Infatti, si occupa di prodotti di Data Leak Prevention (DLP solutions) e solo parzialmente di altri elementi (alcuni li ho riportati in http://blog.cesaregallotti.it/2011/03/proteggersi-dal-leakage.html)

****

11- Spionaggio: forse errata corrige

Avevo segnalato un articolo che citava dei casi di spionaggio industriale:
http://blog.cesaregallotti.it/2011/03/non-solo-wikileaks-anche-lo-spionaggio.html

Roberto Bonalumi mi invia un link ad un recente articolo del Corriere della Sera per cui sembra tutta una montatura:
http://archiviostorico.corriere.it/2011/marzo/13/Renault_spy_story_cinese_era_co_8_110313028.shtml

E un link al sito del 24 Ore:
Il commento di Roberto: "Se quanto riportato è vero, evidentemente è troppo facile ingannare il top management, e fargli prendere decisioni avventate su basi inesistenti [stranamente questo mi ricorda qualcosa che aveva a che fare con Iraq e armi di distruzione di massa...]. A questo proposito, penso che leggerò il libro di Varanini, anche se non farà che rafforzare la mia opinione generale sul livello dei manager in Italia..."

In Italia, i manager avrebbero fatto causa. Mi stupisce che in tutto ciò gli avvocati di Renault non abbiano notato la scarsità di prove prodotte dagli investigatori. O forse gli avvocati non erano proprio stati chiamati.

http://www.ilsole24ore.com/art/economia/2011-03-15/bastano-scuse-spionaggio-danni-134022.shtml

****

12- Errata corrige di errata corrige (sigh!)

Il 14 marzo avevo pubblicato un'errata corrige, ringraziando Max Cottafavi per la segnalazione:
http://blog.cesaregallotti.it/2011/03/errata-corrige-dpr-1782010-su-privacy-e.html

Il 16, Paolo Cupola mi ha fatto osservare che mi aveva fatto la medesima segnalazione qualche settimana prima, come commento al post "incriminato":
http://blog.cesaregallotti.it/2011/02/dpr-1782010-privacy-e-diritto-di.html#comments

Tutto ciò è successo perché non avevo configurato correttamente il blog.

Mi scuso con tutti (in fondo alla mail, sperando che in pochi ci arrivino)