****
IT SERVICE MANAGEMENT NEWS – MARZO 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.

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- Nuovo CAD - Relazione convegno 3 marzo Politecnico Milano

Giovedì 3 marzo si è tenuto un appuntamento al Politecnico di Milano sulle novità introdotte dal Dlgs 235 del 2010 al Codice dell'Amministrazione Digitale.

Hanno partecipato Giovanni Manca, Pierluigi Perri e Stefano Zanero. Incontro molto interessante e molto tecnico.

Alcuni elementi emersi sono elencati di seguito.

- Tipologie di firme informatiche: ce ne sono 4. Probabilmente almeno una è di troppo (quella "digitale", perché si sovrappone a quella "elettronica qualificata", a sua volta un caso particolare della "elettronica avanzata", a sua volta caso particolare della "elettronica"... sigh...)

- Firma grafometrica (ossia la firma su una sorta di tavoletta): una delle tecnologie del futuro potrà essere proprio questa, introdotta all'articolo 25 comma 2 del CAD.
Bisognerà però poi capire come il tutto si intersecherà con la privacy, visto che la firma grafometrica è anche una caratteristica biometrica

- Certificazione dei prodotti: il DPCM del 10 febbraio 2010 proroga ulteriormente la possibilità dei certificatori di firma elettronica di autodichiarare il livello di sicurezza dei propri dispositivi per l'apposizione di firme elettroniche con procedure automatiche.

Nel corso del dibattito si è ribadito che (i) è comunque auspicabile che tali prodotti (hardware o appliance come smart card, lettori e HSM) siano certificati ISO/IEC 15408 (Common Criteria) rispetto a precisi Protection Profiles e (ii) gli installatori stiano attenti a questo aspetto, di modo che non si avrà un detrimento del sistema (tra l'altro, su questo punto, il DPCM del 30 marzo 2009 è ancora in vigore per le altre casistiche)

- Firma remota e firma massiva: argomenti molto delicati, trattati (tra le righe, per la verità) dall'articolo 35 ai commi 2, 3 e 5. Dovranno comunque essere emesse delle regole tecniche (Articolo 71)

- Conservatori accreditati: si è discusso di questa nuova interessante figura riportata dall'articolo 44-bis; i requisiti di sicurezza richiesti non sembrano semplici da soddisfare per tutte quelle aziende di media dimensione che potrebbero essere interessate a questo tema.
Si è anche accennato al rischio di avere modalità di accreditamento che non garantiscono un buon livello di sicurezza (Manca ha fatto il paragone con le certificazioni ISO 9001 e ISO/IEC 27001 aggiungendo una frase che io riporto così "non tutti i certificatori sono bravi come il DNV"... io mi sono sentito onorato di questo riconoscimento anche se molto indiretto)

- Business Continuity: l'articolo 50-bis dice che "le pubbliche amministrazioni predispongono i piani di emergenza in grado di assicurare la continuita' delle operazioni indispensabili per il servizio e il ritorno alla normale operatività".
Manca ha ironizzato sul fatto che anche gli asili nido dovranno avere il loro BCP.

Io ho fatto notare che questa normativa rischia di riportarci indietro: l'argomento viene affrontato in una normativa di tipo IT e si rischia che ritorni diffusa l'equazione Business Continuity = Continuità dei sistemi IT; proprio quando finalmente questo errore era meno diffuso (insieme a Business Continuity = Continuità in caso di disastri)

- Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni: l'articolo 51 prevede che vengano emesse delle regole tecniche su questi temi. Vedremo come saranno.

- Copie di documenti: molto parlare si è fatto degli articoli 22 (Copie informatiche di documenti analogici), 23 (Copie analogiche di documenti informatici), 23-bis (Duplicati e copie informatiche di documenti informatici).
Gli articoli non sono un esempio da seguire in termini di chiarezza e di coerenza con la tecnologia attuale.

Aggiungo il link alla pagina pertinente della DigitPA: http://www.digitpa.gov.it/firma-digitale

Aggiungo il link al testo vigente del CAD:
http://www.digitpa.gov.it/sites/default/files/CAD_lgs_235_2010.pdf

Nota mia finale.
Non ho avuto il coraggio di fare la domanda: "a fronte di questa normativa, che valore hanno le e-mail? e i log dei sistemi?".
Fornisco la mia risposta: vale il comma 1-bis dell'articolo 20: "L'idoneita' del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualita', sicurezza, integrita' ed immodificabilita', fermo restando quanto disposto dall'articolo 21."
Mi auguro di ricevere (e pubblicherò) ulteriori pareri.

Ho posto la domanda a Giovanni Manca via mail e mi ha risposto: "La sua valutazione è corretta!".
Faccio notare che la risposta di Manca è arrivata via Mail, quindi, fino a prova contraria, ritenetela informale.

****

02- Ancora sul CAD (Codice Amministrazione Digitale)

Segnalo un ulteriore articolo da Filodiritto:"La firma digitale ora si fa con le dita";
http://www.filodiritto.com/index.php?azione=visualizza&iddoc=2190

Segnalo anche il sito per iscriversi a Omat 2011 a Milano (5-6 aprile): www.omat360.it/mi11
Dal "progetto 2011" non sembra che il CAD sarà argomento di discussione, ma bisognerà verificare quando sarà disponibile il programma definitivo. La parte forse più interessante è il 6 mattina.

****

03- Presentazioni itSMF al Security Summit

Sono disponibili le presentazioni tenute al Security Summit il 14 marzo 2011 durante la sessione dedicata all'itSMF. Una è mia.

Il link alla home dell'itSMF per la notizia:
http://www.itsmf.it/index.php

Il link con le tre presentazioni:
http://www.itsmf.it/index.php?method=section&action=zoom&id=2265

Il mese prossimo conto di dare ulteriori dettagli sul Security Summit.

****

04- Errata corrige: DPR 178/2010 su Privacy e diritto di opposizione

Il mese scorso, trattando di DPR 178/2010 su Privacy e diritto di opposizione, avevo scritto che l'argomento non era trattato sul sito del Garante Privacy:
http://blog.cesaregallotti.it/2011/02/dpr-1782010-privacy-e-diritto-di.html

Massimo Cottafavi (Spike Reply) mi ha contraddetto, segnalandomi due link dal sito stesso:
- http://www.garanteprivacy.it/garante/doc.jsp?ID=1785597
- http://www.garanteprivacy.it/garante/doc.jsp?ID=1784528

Colpito e affondato!

****

05- Contenzioso penale sul lavoro e privacy

Finalmente, una notizia su un'azienda che agisce correttamente quando conduce indagini su un lavoratore.

In poche parole, l'azienda ha "solo" preso in consegna il pc aziendale per poi metterlo a disposizione dell'autorità giudiziaria.

Ribadisco un concetto importante in modo molto sintetico, parafrasando il "don't do it at home": è giusto e corretto imparare le tecniche di digital forensics, ma non usatele a casa (o nell'azienda) vostra! Prendete esempio da questo caso: congelate e chiamate chi di dovere.

La notizia sul sito del Garante: http://www.garanteprivacy.it/garante/doc.jsp?ID=1792844#3

****

04- L'analisi del rischio operativo: il caso DB Consorzio

Segnalo questo interessante articolo di Enrico Toso di Deutsche Bank:
http://www.zerounoweb.it/index.php?option=com_content&task=view&id=4464&Itemid=0

Alcuni spunti che ritengo utile segnalare:
- il reimpiego di contributi provenienti da precedenti analisi (tema molto complesso, perché svilito dai tanti che pensano di avere "LA soluzione" adatta per tutti i contesti e di essere molto più bravi di quelli che li hanno preceduti; qui si parla invece di "elemento vincente")
- il pericolo di una versione eccessivamente analitica ma poco mantenibile e quello di una descrizione generica ma inutile allo scopo (il tema della mantenibilità dell'analisi è cruciale)
- la "verifica di fondatezza perché il modello possa essere considerato attendibile e sostenibile in sede di contraddittorio o di verifica interna o esterna, o perché lo stesso abbia un valore esimente in sede di giudizio".

****
05- NIST IR 7298, Glossary of Key Information Security Terms

Il NIST ha pubblicato il proprio glossario dei termini della sicurezza.

Non tutte le definizioni sono condivisibili o in linea con altri riferimenti.

Vale però la pena averlo sotto mano:
http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf

****
06- NIST SP 800-39, Managing Information Security Risk

Il NIST ha pubblicato il proprio equivalente della ISO/IEC 27003.

L'ho trovato interessante da leggere, come quasi tutte le pubblicazioni del NIST, con molte idee e considerazioni utili; cito tra gli altri: le rfilessioni sulle diverse tollerabilità del rischio, la convivenza di diverse metodologie di risk assessment nella medesima organizzazione, i rapporti con le terze parti. Inoltre, è gratuito.

Il link: http://csrc.nist.gov/publications/PubsSPs.html#800-39

****
07- Proteggersi dal leakage

Dopo il caso di Wikileaks, qualcuno mi ha chiesto cosa si può fare per prevenire il coinvolgimento di un'azienda in eventi simili. Propongo di seguito alcune mie riflessioni. Ogni contributo per migliorarle sarà ben accetto (e opportunamente attribuito).

Le tecniche sono quelle di prevenzione dallo spionaggio industriale e si possono ridurre in due opzioni.

OPZIONE 1: pianificare una serie di interventi, tra i quali l'impostazione di un preciso processo di gestione delle credenziali e delle autorizzazioni (incluso un meccanismo basato sui ruoli), la revisione periodica e la riduzione delle autorizzazioni, la formazione, la chiusura delle connessioni a Internet, la limitazione dell'uso della posta elettronica al di fuori del perimetro dell'organizzazione (alcune aziende mettono a disposizione "funghi" per permettere l'uso illimitato dell'e-mail), il blocco delle porte USB, la restrizione delle attività di configurazione sui pc

Sono in commercio diversi prodotti per il controllo delle comunicazioni da/a un'organizzazione. Una molto breve ricerca su Internet mi ha portato a questi due (non li conosco, non li ho mai provati), ma sicuramente i grossi produttori e system integrator ne propongono altri:
- http://www.slideshare.net/mmilazzo/infomation-leakage-prevention-ita
- http://cleverconsultingsrl.createsend3.com/t/r/l/yujjfd/bmlklukr/j

Ognuno di questi interventi richiede un elevato sforzo da parte dell'organizzazione che intende attuarli. In alcuni casi, lo sforzo è economico, in tutti è di tipo culturale e organizzativo (provate a togliere la connessione Internet al personale e rischiate grandi malumori, se non opportunamente previsti e gestiti).

OPZIONE 2: non fare nulla. Ogni azione non chiuderà mai tutti i buchi; basti pensare che il dossier Mitrokin è stato costituito anche attraverso documenti copiati a mano.

Tra queste due opzioni, vi è il "livello adeguato", individuabile a seguito di risk assessment. Un risk assessment che si basi su due parametri specifici:
- quali informazioni sono gestite dall'azienda, quali danni può portare una loro diffusione al suo esterno, qual è la loro appetibilità, per chi sono appetibili
- quali sono gli "agenti di attacco": quali sono le loro motivazioni e i loro mezzi

****

08- Non solo Wikileaks (anche lo spionaggio industriale)

Dal sito del BSI, segnalo il breve articolo "Industrial espionage targets Renault electric car designs".

In breve: Renault, General Motors e Ford recentemente sono state vittime di casi di spionaggio industriale.

Mio commento: si parla tanto di Wikileaks in termini sociali o di impatti sulla politica. Ma lo spionaggio industriale è vecchio come il mondo. Solo alcuni mezzi di raccolta e diffusione delle informazioni sono cambiati e alcune motivazioni si sono aggiunte.

****

09- Rischi e sistemi virtuali

Sul Volume 1 del 2011 dell'Isaca Journal è apparso l'interessante articolo "Virtualization Benefits and Security Audit of Virtual IT Systems".

L'articolo presenta brevemente le tecnologie di virtualizzazione e infine presenta una check list di audit di 141 punti. Come è ovvio, le check list di audit possono anche essere usate come valido spunto per la pianificazione e la realizzazione.

Purtroppo l'articolo completo è disponibili ai soli soci ISACA. Il riassunto lo trovate qui:
http://www.isaca.org/Journal/Blog/Lists/Posts/Post.aspx?ID=45

Alternativa disponibile a tutti è la già citata SP-800-125 del NIST:
http://csrc.nist.gov/publications/PubsSPs.html

****

10- Proposta (negli USA) di certificare la sicurezza IT

Aldo Ceccarelli, sul gruppo Clusit di LinkedIn segnala questo articolo:
http://www.linkedin.com/news?viewArticle=&articleID=380816458&gid=54878&type=member&item=44385712&articleURL=http%3A%2F%2Frss%2Eslashdot%2Eorg%2F%7Er%2FSlashdot%2Fslashdot%2F%7E3%2FajQVyVJYd7k%2FIndustry-IT-Security-Certification-Proposed&urlhash=GNav&goback=%2Egde_54878_member_44385712

In breve: alla conferenza RSA è stato proposto di certificare (in modo simile alla revisione dei conti o alla SOX) la sicurezza informatica, al fine di dare maggiore fiducia nelle aziende.

Ovviamnete, se la cosa andrà avanti, sarà interessante vedere quale approccio prenderanno, visto che non sembra sarà seguito l'approccio ISO/IEC 27001.

****

11- Richiami di prodotto e contro il management

Un articolo sul sito del BSI dice che, nel 2010 in UK, i prodotti richiamati dalle case produttrici sono aumentati del 12% rispetto al 2009.

L'articolo ha titolo "Cutting Corners in quality compromising brands from Ferrari to Johnson and Johnson" e si trova a questa URL:
http://shop.bsigroup.com/en/Browse-By-Subject/Quality--Sampling/Product-recalls-in-2010-break-records/?id=185248&utm_source=QUALB-NA&utm_medium=et_mail&utm_content=546448&utm_campaign=QUALB-NA_2_March_2011&utm_term=article.

Non credo di poter sottoscrivere la tesi dell'articolo, per cui l'uso della ISO 9004 può aiutare a ridurre questi casi. Penso piuttosto che, in tempi di crisi, il management taglia i costi avendo come unici riferimenti un foglio Excel, il proprio stipendio e il proprio tenore di vita. Senza pensare a processi, tecniche e qualità.

Chiunque si sia occupato di processi di qualità avrà visto come troppo spesso i controlli sono fatti in modo anti-economico (per esempio, innumerevoli controlli a fine linea a scapito delle attività preventive), da personale non sempre motivato o completamente competente. Un bel taglio dei costi avrà eliminato anche questo senza pensare ad alternative.

In questo periodo sto leggendo "Contro il management" di Francesco Varanini.
Il commento sopra espresso prende spunto anche da questa lettura.

In molti abbiamo visto come in alcune aziende si taglia l'uso della carta, la formazione, gli strumenti di lavoro e alcuni rimborsi (del personale operativo, ovviamente), mentre non c'è alcun limite per alcune trasferte, alcuni benefit e certa formazione (soft skill manageriali...) e gli sprechi per mancanza di pianificare sono immensi. Varanini, però, mette tutto questo e anche molto di più in un buon libro.

Per scrivere questo post, ho "scoperto" che Varanini gestisce un blog:
http://www.controilmanagement.blogspot.com/

****

14- ISO/IEC 17021:2011

Una comunicazione dell'organismo di certificazione NQA dice che dal 1°febbraio 2011 è stata pubblicat a la revisione della norma internazionale ISO/IEC 17021:2011 "Conformity assessment -- Requirements for bodies providing audit and certification of management systems".

Questa norma fornisce requisiti a cui devono sottostare i soli organismi di certificazione (in altre parole, se non lavorate in un OdC, non vi interessa).

Secondo quanto riportato dalla comunicazione già citata, la ISO 17021:2011 contiene, praticamente invariati, i requisiti per la conduzione degli audit da parte degli Organismi di certificazione; fornisce invece ulteriori criteri per la competenza degli auditor.

IAF (International Accreditation Forum) e ISO (International Organization for Standardization) hanno fissato al 1°febbraio 2013 il termine ultimo per l 'implementazione della ISO/IEC 17021:2011 da parte degli Organismi di certificazione di sistemi di gestione.