Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS - APRILE 2013
****

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- Standardizzazione: Traduzioni norme ETSI su sicurezza nella conservazione dei dati

Franco Ruggieri ha segnalato che è stato pubblicato a febbraio il terzo documento della traduzione delle specifiche ETSI in oggetto.

Il set completo delle pentole in offerta UNINFO è quindi costituito da:
- UNI/TS 11465-1:2012 "Firme elettroniche ed infrastrutture (Electronic Signatures and Infrastructures - ESI) - Sicurezza nella Conservazione dei dati - Parte 1: Requisiti per la Realizzazione e la Gestione" - traduzione della ETSI TS 101 533-01
- UNI/TR 11465-2:2012 "Firme elettroniche ed infrastrutture (Electronic Signatures and Infrastructures - ESI) - Sicurezza nella Conservazione dei dati - Parte 2: Linee Guida per l'Ispettore" - traduzione dello ETSI TR 101 533-02;
- UNI/TS 11465-3:2013 "Firme elettroniche ed infrastrutture (Electronic Signatures and Infrastructures - ESI) - Sicurezza nella Conservazione dei dati - Complemento italiano a ETSI TS 101 533-1 e ETSI TR 101" - localizzazione in Italia delle specifiche di cui sopra.

Io ci ho modestamente collaborato e le ho trovate molto interessanti, anche perché si tratta di specializzazioni delle ISO/IEC 27001 e 27002.

Le potete trovare in inglese sul sito della ETSI (www.etsi.org) o in italiano su quello dell'UNI (www.uni.com).

****

02- Standardizzazione: ISO/IEC TR 27015

Franco Ferrari del DNV Italia mi informa della pubblicazione della ISO/IEC TR 27015 dal titolo "Information security management guidelines for financial services".

Si tratta, in poche parole, di un'estensione dei controlli di sicurezza già descritti nella ISO/IEC 27002 applicabile ai servizi informatici di tipo "finance", in particolare quelli delle banche, che possono coinvolgere ATM, POS e terminali self service.

Lo standard è relativamente breve (28 pagine) e i punti che più mi hanno interessato sono:
- estensione del controllo 6.2.2 (sicurezza con i clienti), con la necessità di formare i clienti dei servizi su alcune misure di sicurezza informatica;
- estensione del controllo 6.2.3 (sicurezza con i fornitori), con alcune misure di sicurezza da prevedere in occasione della stipula di accordi con i fornitori
- aggiunta del controllo 10.9.4 con titolo "Internet banking services", con alcune misure di sicurezza da prevedere nella progettazione di tali servizi.

****

03- Standardizzazione: I risk assessment della ISO 22301 e della ISO/IEC 27001

Stefano Ramacciotti mi ha segnalato il seguente post dal titolo "Can ISO 27001 risk assessment be used for ISO 22301":
- http://blog.iso27001standard.com/2013/03/11/can-iso-27001-risk-assessment-be-used-for-iso-22301/

Ricordo che la ISO/IEC 27001 è la norma dedicata ai sistemi di gestione per la sicurezza delle informazioni (ISMS) e la ISO 22301 ai sistemi di gestione per la continuità operativa (BCMS).

L'articolo è un poco confuso. Segnalo le cose decisamente condivisibili:
- i risk assessment descritti dalle attuali versioni delle ISO/IEC 27001, ISO/IEC 27005 e ISO 22301 sono allineati con i requisiti della ISO 31000 "Gestione del rischio - Principi e linee guida";
- il BCM si occupa delle attività e dei processi, mentre un ISMS (SGSI) si occupa della sicurezza delle informazioni e, quindi, i rispettivi risk assessment sono necessariamente diversi;
- il collegamento tra BCM e ISMS è il parametro di disponibilità delle informazioni.

Tra le cose negative segnalo:
- l'articolo fa riferimento agli asset dicendo che dovrebbero essere identificati nel dettaglio (interpretazione non più condivisa, tanto che la futura 27001 parlerà solo di "information asset"),
- apprezza la descrizione dettagliata del risk assessment della 27001 (ritenuta oggi non più pertinente per uno standard di requisiti)
- confonde la genericità dei requisiti della 22301 con la possibilità di avere un risk assessment non approfondito
- vorrebbe un allegato alla 22301 simile all'allegato A della 27001, mentre il suo compito è demandato alla ISO 22313 che fornisce una linea guida per le misure da considerare per un BCM.

Detto questo, è comunque bene ricordare che le differenze tra i due approcci sono dovute alle loro diverse finalità: nel ISMS, il risk assessment ha la finalità di indicare le priorità di trattamento delle vulnerabilità relative alle informazioni; nel BCMS, il risk assessment ha la finalità di strumento sul quale basare le strategie di ripristino dei processi e delle attività.

Sebbene i metodi di risk assessment utilizzati per un ISMS o per un BCM sono diversi a causa delle diverse finalità, è comunque bene studiarli entrambi, senza dimenticarne altri (per esempio quelli utilizzati per la sicurezza delle persone o nei settori dell'automotive, dei dispositivi medicali o del chimico) per poter individuare quello più adeguato alle proprie esigenze. Ho visto aziende che hanno utilizzato un buon mix tra il classico metodo di risk assessment relativo alla sicurezza delle informazioni e la FMECA utilizzata in ambito automotive.

Ultima riflessione: è bene studiare i metodi utilizzati nel campo di pertinenza, ma è anche bene farlo in modo critico. Ho visto molti danni dovuti all'uso del CRAMM (il metodo di risk assessment per la sicurezza

della informazioni "originario") o di suoi derivati, visto che sono difficili da mantenere e non sempre i risultati ottenuti sono pertinenti.

****

04- Se non lo misuri non lo conosci?

Finalmente ho scoperto da dove viene il detto "se non lo misuri, non puoi gestirlo". Qualcuno penserà che ci sono arrivato tardi...

L'origine è Lord Kelvin, che nel lontano 1893 disse "Se puoi misurare ciò di cui parli e puoi esprimerlo con un numero, allora conosci qualcosa del tuo soggetto; ma se non puoi misurarlo, allora la tua conoscenza è scarsa e insoddisfacente".

Lord Kelvin è noto per essere stato un grande fisico (fisico matematico e ingegnere). A mio modesto parere, le scienze sociali (e la conduzione di un'azienda è in gran parte collegata alle scienze sociali) non dovrebbero confondersi con la matematica e la fisica. Misurare qualcosa è importante, ma la conoscenza di un'impresa viene dal monitoraggio.

Non devo essere l'unico a pensarlo, visto che la stessa ISO 9001 chiede di "monitorare e, dove possibile, misurare".

****

05- Novità legali: DPCM 24 gennaio 2013 sulla protezione cibernetica

E' stato pubblicato il DPCM 24 gennaio 2013 dal titolo "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale". E' facilmente reperibile su www.normattiva.it.

L'ho letto con l'attenzione che merita. Non ho però trovato quello che speravo di trovare, ossia un CERT italiano.

Apparentemente, se ho capito correttamente, questo compito sarà affidato al "Nucleo per la sicurezza cibernetica", ma non mi è chiaro se si occuperà quasi esclusivamente della PA o anche di altri settori.

Il testo specifica che tale nucleo "promuove procedure di condivisione delle informazioni, anche con gli operatori privati interessati, ai fini della diffusione di allarmi relativi ad eventi cibernetici e per la gestione delle crisi". Non mi è chiaro se sarà disponibile un sito web utilizzabile da ciascun privato per formazione e informazione.

Gli operatori di telecomunicazioni dovranno anche comunicare al Nucleo le violazioni della sicurezza, oltre che adottare misure di sicurezza cibernetica che dovrebbero essere state pubblicate da tempo a cura del Ministero dello sviluppo economico. A me non risultano disponibili, ma se mi dovessi sbagliare, sarò grato a chi mi correggerà.

In definitiva, non credo ci rimanga altro che aspettare pazientemente per vedere come questo DPCM sarà attuato e coglierne tutti gli aspetti positivi.

Ringrazio per la segnalazione Pasquale Stirparo e Daniela Quetti di DFA e Enzo Ascione di Intesa Sanpaolo.

****

06- Novità legali: Modifiche ai requisiti di accessibilità nella PA

La Legge 221 del 2012 ha convertito, con modificazioni, il DL 179 del 2012, dal titolo "Ulteriori misure urgenti per la crescita del Paese", che riporta alcune modifiche alla Legge 4 del 2004 (Legge Stanca sull'accessibilità) e al Dlgs 82 del 2005 (Codice dell'amministrazione digitale o CAD).

Ricordo che la normativa sull'accessibilità è quella che richiede che i servizi IT siano progettati in modo da essere utilizzabili dai disabili.

Rilevante è l'estensione di applicabilità della Legge sull'accessibilità a "tutti i soggetti che usufruiscono di contributi pubblici o agevolazioni per l'erogazione dei propri servizi tramite sistemi informativi o internet".

Altro elemento rilevante è l'inserimento del tema dell'accessibilità nella formazione che deve essere erogata al personale della Pubblica Amministrazione.

Maggiori dettagli nella Circolare 61/2013 del 29 marzo 2013 dell'AgID:
- http://www.digitpa.gov.it/fruibilita-del-dato/accessibilita.

Sempre notizia di questi giorni è la prevista modifica all'Allegato A del Decreto Ministeriale 8 luglio 2005 (Ministro per l'Innovazione e le tecnologie) sui "requisiti tecnici di accessibilità delle applicazioni basate su tecnologie internet" (l'Allegato si trova alla medesima pagina web sopra indicata).

E infine, l'ETSI ha appena pubblicato una bozza dello standard europeo EN 301 549 dal titolo "Accessibility requirements for public procurement of ICT products and services in Europe". Sarebbe bello se venisse adottato dalla pubblica amministrazione e dalle aziende private.

****

07- Novità legali: Siti web e dati societari

La notizia è vecchia e nota ed ero convinto di averla già pubblicata. Non trovandola tra i miei articoli, la scrivo.

Sui siti web (spazi elettronici destinati alla comunicazione collegati ad una rete telematica ad accesso pubblico) delle società soggette all'obbligo dell'iscrizione nel registro delle imprese (s.p.a., s.r.l. e s.a.p.a.), devono essere riportati:
- sede legale;
- ufficio del registro delle imprese presso il quale la società è iscritta;
- il numero d'iscrizione (ossia il codice fiscale, che potrebbe coincidere con la Partita IVA; sono diversi, per esempio, nel caso in cui una società abbia trasferito il proprio domicilio da una provincia ad un'altra);
- capitale della società (somma effettivamente versata);
- se il socio è unico.

Questo in virtù dell'articolo 2250 del Codice Civile, così come modificato dall'articolo 42 della Legge 88 del 2009.

Ringrazio Roberto Bonalumi per alcune correzioni all'articolo originario e la mia commercialista Sara Gardella per la consulenza sul numero di iscrizione al registro delle imprese.

****

08- Misure di sicurezza: Segregazione delle responsabilità

Segnalo un bell'articolo sull'ISACA Journal del dicembre 2012 dal titolo "What Every IT Auditor Should Know About Proper Segregation of Incompatible IT Activities".

Per ovvi motivi di diritto d'autore, non mi addentro nel contenuto, ma riferisco i titoli, già di per se stessi utili anche se sintetici:
- IT vs. utenti (business)
- database administrator vs. resto dell'IT
- sviluppo applicazioni vs. DBA e vs. conduzione dei sistemi (questa però è nota!)
- sviluppo nuove applicazioni vs. manutenzione delle applicazioni
- sicurezza delle informazioni vs. resto dell'IT (anche questa è nota)

Un commento all'articolo ricorda la necessità di separare la sicurezza delle informazioni dall'IT, ma questo è un tema molto caldo e non facilmente risolvibile.

****

09- Atti del Security Summit 2013 a Milano

Segnalo la pubblicazione degli atti del Security Summit 2013 di Milano:
- http://milano2013.securitysummit.it/page/atti.

Come al solito, in mezzo a qualche presentazione un po' troppo commerciale, negli atti si trovano parecchi utili spunti di riflessione.

****

10- Minacce e attacchi: Rapporto Clusit 2013

Il Clusit ha pubblicato il Rapporto 2013 sulla sicurezza ICT in Italia. Esso può essere richiesto dal sito del Clusit:
- https://www.securitysummit.it/page/rapporto_clusit.

Come sempre, riporta notizie interessanti. Segnalo in particolare la prima sezione dal titolo "Panoramica degli eventi di cyber-crime e incidenti informatici più significativi del 2012 e tendenze per il 2013".

****

11- Minacce e attacchi: Spamhaus e la carica degli spammer

La notizia è stata molto diffusa e riguarda la Spamhaus, una società dedicata a servizi di antispamming, oggetto di un attacco DDoS dopo aver inserito in blacklist un grande provider olandese.

Non c'è commento da fare, tranne la preoccupazione di vedere Internet potenzialmente oggetto di attacchi di enormi dimensioni:
- http://www.corriere.it/tecnologia/13_marzo_27/sicurezza-informatica-in-atto-il-piu-grande-attacco-hacker-della-storia_8d0c0142-96f8-11e2-b7d6-c608a71e3eb8.shtml
- http://www.theregister.co.uk/2013/03/27/spamhaus_ddos_megaflood/

****

12- Data Centres Energy Efficiency - EU Code of Conduct on Data Centres

Non sono un esperto di green IT o di altri argomenti correlati, però questa iniziativa del JRC segnalatami da un mio lettore mi pare interessante:
- http://iet.jrc.ec.europa.eu/energyefficiency/ict-codes-conduct/data-centres-energy-efficiency

La trovo interessante perché differenzia bene le attività di ciascuna parte interessata ad un data center, dal proprietario all'utilizzatore. Inoltre, mi è sembrato un documento facilmente leggibile, a parte la scelta di usare dei codici-colore non immediati (soprattutto per i daltonici).