****
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.

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 famiglia ISO/IEC 27000
02- Standardizzazione: altre norme (ISO 22301, ISO 26000, ISO 29990)
03- Novità legali: DPR 178/2010 su Privacy e diritto di opposizione
04- Novità legali: Codice Amministrazione Digitale e Dlgs 235/2010
05- Sentenze (Furto di files, Uso di software pirata, Uso email aziendale)
06- Cancellazione sicura dei files
07- Cloud Computing: BSI BIP 0117; NIST
09- Qualità dei dati e SLA
08- Documenti tecnici (NIST e virtualizzazione, Secure coding; PCI DSS)
10- Sicurezza: Il trasferimento dei rischi (parte 2)
11- Microsoft e Data Governance
12- Report sicurezza (CISCO, Dataloss DB)
13- Incidenti (Phishing, Vodafone Australia)
14- Business Continuity per disabili
15- Un cyber-esercito contro i pirati della rete
16- Norme armonizzate alle Direttive Europee
17- Futuri interventi di Cesare Gallotti (14 marzo)

****
01- Standardizzazione famiglia ISO/IEC 27000

Tra dicembre 2010 e gennaio 2011, sono state inviate agli esperti dell'Uninfo le bozze delle seguenti norme perché le commentassero:
- ISO/IEC 27000 (2o draft)
- ISO/IEC 27001 (4o draft)
- ISO/IEC 27002 (3o draft)
- TR ISO/IEC 27008 - "Guidelines for auditors on information security controls" (Draft)
- ISO/IEC 27010 - "Information security management for intersector and inter-organisational communications" (Committee draft)
- ISO/IEC 27013 - Relazioni tra 27001 e 20000 (3o draft)

- ISO/IEC 27014 - Governance of information security (Committee draft)
- ISO/IEC 27015 (2nd WD) -Guidelines for financial services
- ISO/IEC 27016 - Organizational economics (1o draft)
- ISO/IEC 27033-2 (FCD, revision of ISO/IEC 18028-2:2006) - Guidelines for the design of network security
- ISO/IEC 27033-3 - Reference networking scenarios -- Threats, design techniques and control issues (Final Draft)
- ISO/IEC 27033-4 (3rd WD; revision of ISO/IEC 18028-3:2005) -Securing communications between networks using security gateways
- ISO/IEC 27033-5 (WD) - Securing communications across networks using Virtual Private Networks (VPNs)
- ISO/IEC 27036-3 (Preliminary draft) - Guidelines for ICT supply chain security
- ISO/IEC 27038 (1st WD) - Specification for digital redaction

Inoltre, è stata approvata la FDIS della ISO/IEC FDIS 27031 (Guidelines for information and communication technology readiness for business continuity) e quindi dovrebbe essere pubblicata la versione definitiva sul sito dell'ISO (a pagamento...).

Nessuna nuova notizia sulla ISO/IEC 27037 (Guidelines for identification, collection, acquisition and preservation of digital evidence) che era arrivata al terzo Working Draft e che desta un certo interesse perché relativa alla computer forensics

****

02- Standardizzazione: altre norme (ISO 22301, ISO 26000, ISO 29990)

*** ISO 22301 per la Business Continuity ***

Il BSI ha comunicato con la "Risk and Business Continuity Management Newsletter" del 14 febbraio la possibilità di commentare la ISO 22301 "Continuity management systems – Requirements" attualmente allo stato di DIS (Draft of International Standard).

La ISO 22301 sarà uno standard certificabile, assimilabile alla BS 25999-2:2007, elaborato dallo stesso comitato tecnico che ha emesso la ISO/PAS 22399:2007 "Societal security - Guideline for incident preparedness and operational continuity management".

La struttura è la stessa della "nuova" ISO/IEC 27001. In altre parole, seguirà la cosiddetta Common Structure a cui via via si uniformeranno tutte le specifiche dei sistemi di gestione ISO. Ovviamente, questo vuole anche dire che la ISO 22301 non seguirà l'impostazione della attuale BS 25999-2.

Per leggere il draft e commentarlo:
http://click.bsi-global-email.com/?ju=fe2a15717662037b771679&ls=fded127776660c7a77127373&m=fef91270746c03&l=fe94167372620c7c75&s=fe2e17707264007d7d1374&jb=ffcf14&t=

*** ISO 26000:2010 -- Guida alla responsabilità sociale ***

Il 28 ottobre, la ISO ha pubblicato la ISO 26000:2010 "Guidance on social responsibility". Dal mese di novembre è anche disponibile la versione italiana ufficiale della UNI.

Questa linea guida era molto attesa, anche in virtù del successo dell'iniziativa SA 8000 del SAI. In molti pensavano che la 26000 avrebbe messo sotto il cappello ISO un'iniziativa che potremmo definire "locale", esattamente come la BS 7799 poi diventata ISO/IEC 27001, la BS 15000 diventata ISO/IEC 20000 o i Common Criteria diventati ISO/IEC 15408.

Al momento, questa iniziativa non deve essere confusa con quella della SAI per almeno due motivi. Il primo è che la ISO 26000 esplicitamente esclude il proprio utilizzo per condurre audit, assessment o certificazioni mentre la SA 8000 è uno standard certificabile; il secondo è che la ISO 26000 ha l'ambizione di coprire tutti i temi della responsabilità sociale, mentre la SA 8000 è focalizzata alle condizioni di lavoro.

La lettura è interessante e si basa sui 7 principi della responsabilità sociale (accountability, trasparenza, comportamento etico, rispetto degli interessi degli stakeholder, rispetto del principio di legalità, rispetto delle norme internazionali di comportamento, rispetto dei diritti umani) e sui 7 temi fondamentali della responsabilità sociale (governance, diritti umani, rapporti e condizioni di lavoro, ambiente, corrette prassi gestionali, aspetti specifici relativi ai consumatori, coinvolgimento e sviluppo della comunità).

Nei temi "rapporti e condizioni di lavoro", "corrette prassi gestionali" (inerenti alla lotta alla corruzione, concorrenza leale, rispetto dei diritti di proprietà) e "consumatori" (che include il corretto trattamento dei dati personali) si trovano molti aspetti di sicurezza delle informazioni e di qualità.

Per come è scritto, il documento si scosta da altre norme ISO perché fornisce un'ampia biografia di documenti extra-ISO e un elenco di iniziative sulla responsabilità sociale (tra cui la già citata SAI e SA 8000). Inoltre, nei capitoli sono presenti diversi box di approfondimento.

Ringrazio Paola Generali di GetSolution per la segnalazione.

*** ISO 29990:2010 sulla formazione non scolastica ***

La ISO ha pubblicato con data 1 settembre 2010 la norma ISO 29990:2010 "Learning services for non-formal education and training — Basic requirements for service providers" (notizia trovata su CertiNews di dicembre 2010).

Provo a tradurre "non-formal education" con "formazione non scolastica e non universitaria". La norma riguarda quindi anche la formazione professionale e la formazione con qualifica o certificato finale.

Si tratta di una norma di "requisiti" e quindi certificabile.

La prima parte, al capitolo 3, definisce i requisiti che un ente di formazione (Learning Service Provider) deve rispettare quando determina le necessità di formazione, progetta ed eroga la formazione. Per capire meglio la completezza e pertinenza dei requisiti bisognerà verificare come la norma sarà applicata. Una mia prima impressione è che alcune interpretazioni della ISO 9001 applicata alla formazione professionale siano più rigorose di questo standard.

La seconda parte, al capitolo 4, riporta i "soliti" requisiti di sistema di gestione basati sul ciclo di Deming e simili a quello di altre norme come la 9001, la 27001 e la 20000-1.

****

03- Novità legali: DPR 178/2010 su Privacy e diritto di opposizione

La Legge 166/2009 (Decreto Ronchi) stabiliva che l'uso dei numeri di telefono riportati sugli elenchi pubblici (es. Pagine Bianche) per pubblicità, vendita o ricerche di mercato è consentito nei confronti di chi non abbia esercitato il diritto di opposizione.

Su questo tema si discusse assai perché rappresentava una marcia indietro del diritto alla

privacy in favore delle aziende pubblicitarie. In particolare, si vedeva (a ragione, come sappiamo bene) la vittoria di certe pratiche commerciali maleducate e irrispettose della vita privata di ciascuno: prima del Decreto Ronchi era vietato fare chiamate di marketing diretto salvo diversa indicazione dell'interessato (opt-in), mentre ora si possono fare chiamate di marketing diretto salvo diversa indicazione dell'interessato (opt-out).

Ad ogni modo, il Decreto Ronchi (del 25 settembre 2009) dava 6 mesi per istituire il registro dei cittadini che esercitano il diritto di opposizione. Il 7 settembre 2010 (con soli 6 mesi di ritardo) è stato quindi emanato il DPR 178/2010 che regola il registro pubblico degli abbonati che si oppongono all'utilizzo del proprio numero telefonico per vendite o promozioni commerciali. Anche se non enunciate nel titolo, le stesse modalità valgono per chi effettua ricerche di mercato.

Si può scaricare il DPR (GU n. 256 del 2-11-2010) da:
- http://gazzette.comune.jesi.an.it/2010/256/1.htm
- www.normattiva.it

Il registro, gestito dalla Fondazione Ugo Bordoni, è disponibile su http://www.registrodelleopposizioni.it/.

Note polemiche:
- in pieno disaccordo con il Dlgs 196/2003 (che richiede consensi distinti per finalità distinte), non viene lasciata la possibilità di opporsi al marketing diretto e/o alle ricerche di mercato: o tutto o niente!
- sul sito del Garante non viene detto nulla
- sulle newsletter del Garante non mi sembra di aver letto nulla in merito

Ringrazio Ivo Trotti di TNS per la segnalazione.

****

04- Novità legali: Codice Amministrazione Digitale e Dlgs 235/2010

Dal 25 gennaio è in vigore il Dlgs 235 del 2010 che ha pesantemente modificato il Codice dell'Amministrazione Digitale (CAD) Dlgs 82 del 2005.

Questo Codice è particolarmente importante perché è il punto di riferimento per la definizione di "documento informatico" e per stabilirne la validità anche dal punto di vista legale.

Il 5 e 6 aprile a Milano è prevista l'edizione del 2011 di Omat. Spero che lì saranno discusse opportunamente le modifiche apportate e il loro impatto.

Per intanto, segnalo l'articolo di Filodiritto che mi ha portato alla notizia:
http://www.filodiritto.com/index.php?azione=visualizza&iddoc=2178

Segnalo anche questo articolo:
http://www.filodiritto.com/index.php?azione=visualizza&iddoc=2190

Per leggere il Dlgs 235 del 2010 e la versione consolidata del CAD, consiglio di utilizzare www.normattiva.it.

****

05- Sentenze (Furto di files, Uso di software pirata; Uso email aziendale)

*** Rubare files non è reato (parte 2) ***

A inizio gennaio avevo segnalato la notizia sulla sentenza della Corte di Cassazione sui reati configurabili in materia di sottrazione di file sul luogo di lavoro.
http://blog.cesaregallotti.it/2011/01/rubare-files-non-e-reato.html

Luca De Grazia propone un'analisi più esaustiva della vicenda:
http://lucadegrazia.postilla.it/2011/01/25/copiare-un-documento-su-un-server-aziendale-non-e-un-furto-poiche-non-vi-e-spossessamento-o-distruzione/

*** Diritto d'autore: assoluzione per uso di software pirata ***

Attilio Rampazzo ci segnala la seguente notizia: La Corte di Appello di Trento ha assolto due architetti della Valsugana che utilizzavano nei loro uffici programmi informatici privi di licenza. Per i giudici non è reato perché si trattava di liberi professionisti e non di imprenditori.

La vicenda riguarda l'applicazione dell'articolo 171-bis della Legge 633 del 1941 che riguarda "scopi commerciali o imprenditoriali". Altro discorso deduco sia stato fatto in merito all'applicazione del 174-ter che non ha restrizioni.

Articoli simili che ho trovato in rete:
- Commento di Costabile:
http://www.marcodimartino.it/documenti/pdf/Costabile_Software_senza_licenza_in_azienda.pdf
- http://www.reteingegneri.it/notizie/economia-e-fisco/sentenza-su-software-senza-licenza.html
- Sentenza della Cassazione 1: http://www.studiolegalelaw.net/consulenza-legale/15772
- Sentenza della Cassazione 2: http://www.penale.it/giuris/cass_015.htm

Due miei quasi ironici commenti:
1- come libero professionista, prendo nota
2- non si può più dire che i professionisti ("quelli della partita IVA") sono "imprenditori di se stessi"

A parte ciò, la materia pare decisamente complessa e forse troppo discussa perché si possano dedurre i comportamenti completamente corretti (a "prova di Legge"). Tranne pagare tutte le licenze di tutti i software utilizzati...
http://www.ilgazzettino.it/articolo.php?id=134678&sez=NORDEST

*** Uso dell'email aziendale per comunicare con l'avvocato ***

Il mese scorso avevo riportato dei comportamenti attenti sull'uso di Facebook
http://blog.cesaregallotti.it/2011/01/realta-e-virtualita-qualcuno-capisce-le.html

Questa volta riporto la notizia appresa dal SANS NewsBites Vol. 13 Num. 6: un'impiegata ha usato l'email aziendale per concordare con il proprio avvocato come condurre una causa ostile all'azienda stessa e le mail sono state accettate come prova in tribunale della malafede dell'impiegata (non valendo, a questo punto, il segreto avvocato-assistito):
http://www.wired.com/threatlevel/2011/01/email-attorney-client-privilege/

Bisogna avere una bella fantasia per usare la mail aziendale per complottare contro l'azienda stessa...

****

06- Cancellazione sicura dei files

Dalla newsletter DFA, segnalo il link ad un articolo sulla cancellazione sicura dei files pubblicato dal SANS:
http://computer-forensics.sans.org/blog/2011/01/25/digital-forensics-erasing-drives-quick-easy

Anche questo articolo conferma che: UN passaggio di sovrascrittura è sufficiente.

Aggiungo: chi dice che i passaggi devono essere 35 o 37 o qualcosa del genere, fa riferimento a studi degli anni '60 o '70, quando gli hard disk erano ben diversi.

Dal link sopra riportato è possibile rintracciare un altro articolo più corposo (con software freeware)
http://cmrr.ucsd.edu/people/Hughes/DataSanitizationTutorial.pdf

****

07- Cloud Computing: BSI BIP 0117; NIST

Nel novembre del 2010, il BSI ha pubblicato il documento "BIP 0117 - Cloud Computing. A Practical Introduction to the Legal Issues". Non uno standard, non una linea guida: un libro pubblicato da un editore che pubblica anche standard. Per questo non deve essere considerato come "utile per le certificazioni ISO o BS".

E' noto che il cloud computing è un argomento forse abusato (lo stesso documento cita Larry Ellison, CEO della Oracle, molto critico in merito perché, dice, si sta parlando di cose note da tempo con altri nomi). Ho comunque trovato interessante questo libro perché richiama e mette in ordine un insieme di argomenti da tenere presente quando si stipula un contratto con un outsourcer (cloud o non cloud, italiano o europeo o extraeuropeo).

I titoli di alcuni capitoli rendono l'idea: Security, Data protection (la nostra "privacy"), Software licensing, Customer data, Service change and service levels, Contracting and liability.

Come difetto, devo segnalare che il libro è incentrato sulla legislazione UK.

Il link al BSI Shop (con Overview ufficiale)
http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030215581

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

Il NIST ha inoltre pubblicato il draft della SP-800-144 "Guidelines on Security and Privacy in Public Cloud Computing". E' una lettura più tecnica della precedente, presenta all'inizio le diverse definizioni di cloud computing e ha il pregio di essere gratuita.
http://csrc.nist.gov/publications/PubsDrafts.html#800-144

****

08- Documenti tecnici (NIST e virtualizzazione, Secure coding; PCI DSS)

*** Guida NIST - Virtualizzazione ***

Il NIST ha pubblicato la SP 800-125 dal titolo "Guide to Security for Full Virtualization Technologies".
http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf

La guida è al solito di facile lettura ed espone in ordine: una dissertazione sulle tecniche di virtualizzazione, un'analisi delle minacce applicabili al contesto e le misure raccomandate.

Per specifiche più tecniche, legate al singolo prodotto di VM, è necessario fare riferimento al Security Configuration Checklists Program: http://checklists.nist.gov/

*** Secure coding ***

Sul Clusit Group su Linkedin viene segnalato questo articolo sull'utilità delle metodologie di programmazione sicura (OWASP soprattutto)
http://blogs.techrepublic.com.com/security/?p=4932&goback=%2Egde_54878_member_39150496

Difficile non essere d'accordo su due considerazioni (tra le altre):
1- ci sono troppi mediocri programmatori e rari bravi programmatori (come in tutte le professioni)
2- i programmatori lavorano male perché costretti a rispettare tempi molto ristretti

*** PCI DSS 2.0 ***

Recentemente ho segnalato la pubblicazione del Quaderno Clusit dal titolo "PCI-DSS: Payment Card Industry - Data Security Standard". Luca Lazza (di Novit) mi fa notare che avrei anche dovuto segnalare l'uscita della versione 2.0 del PCI-DSS, operativa dal 1 gennaio di quest'anno.
https://www.pcisecuritystandards.org/pdfs/summary_of_changes_highlights.pdf

Sia Luca che Fabio Guasconi (co-autore del quaderno Clusit) dicono che non cambia praticamente nulla: sono stati chiariti alcuni punti, introdotti alcuni requisiti riguardo alle nuove tecnologie (es. cloud computing e virtualizzazione dei server) e modificato il "ciclo di vita" delle specifiche PCI da 2 a 3 anni.

****

09- Qualità dei dati e SLA

Franco Ferrari (DNV Italia) segnala questo interessante articolo sulla qualità dei dati e gli SLAs. Fa riferimento ad un white paper di DataFlux, società acquisita da SAS, la cui lettura è sottoposta alla registrazione presso il loro sito. Quindi, non l'ho scaricato, ma direi che l'articolo è più che esaustivo
http://www.zerounoweb.it/index.php?option=com_content&task=view&id=4576&Itemid=126

A fronte di ciò, Tony Coletta, ha segnalato che in merito a questo argomento è stato pubblicata la ISO/IEC 25012:2008, dal titolo "Software engineering -- Software product Quality Requirements and Evaluation (SQuaRE) -- Data quality model". Lo standard è interessante e propone 15 dimensioni della qualità dei dati, a loro volta da considerare come "inerenti" ai dati o "dipendenti dal sistema". La norma è quindi collegata agli altri standard sulla qualità del software, in particolare la ISO/IEC 9126-1 "Information technology - Software product quality - Quality model" che sarà sostituita dalla ISO/IEC 25010 "System and software quality models"(ora allo stato di Final Draft).

Aggiungo: questi temi sono importanti quando si parla di qualità dei dati da proteggere o da utilizzare per l'erogazione di servizi e quando si parla di misurazioni dell'efficacia e efficienza (per esempio di un sistema di gestione per la sicurezza delle informazioni o di gestione dei servizi IT).

****

10- Sicurezza: Il trasferimento dei rischi (parte 2)

Il 5 novembre 2010 avevo segnalato la pubblicazione di un articolo Clusit sui rischi trasferibili al mercato assicurativo.

L'autore aveva promesso la futura pubblicazione di una vasta panoramica di sinistri realmente avvenuti e trattati dalle Assicurazioni. Tale seconda pubblicazione è ora disponibile su:
www.clusit.it/docs/rscalici_11-01-24.pdf

Devo dire che a me è parso più un elenco di attacchi, più che una descrizione utile a capire come gestire un contratto assicurativo. Certamente interessante per quanti apprezzano le "storie dell'orrore", ma continuo a non vedere una facile applicazione del "trasferimento del rischio alle assicurazioni".

****

11- Microsoft e Data Governance

Da un articolo dell'ISACA Journal Volume 6 del 2010, ho trovato un interessante link alla pagina della Microsoft dedicata alla Data Governance.

Nulla di nuovo sotto il cielo. Ma almeno è gratuito ed è possibile visitare le tante pagine della Microsoft dedicate a questo argomento e non solo:
http://www.microsoft.com/datagovernance

****

12- Report sicurezza (CISCO, Dataloss DB)

*** Report CISCO ***

Dalla newsletter del Clusit, segnalo la pubblicazione del
- Cisco 2010 Annual Security Report
- Cisco 4Q10 Global Threat Report

Si trovano a questo indirizzo:
http://www.cisco.com/en/US/prod/vpndevc/annual_security_report.html

*** Dataloss DB ***

Agli appassionati di statistiche su incidenti e per i colleghi appassionati di "storie dell'orrore informatico", questo sito piacerà:
http://datalossdb.org/

Traduco la prima riga della presentazione: "DataLossDB è un progetto di ricerca che è l'obiettivo di documentare gli inciedenti con perdite di dati, conosciuti e segnalati, avvenuti a livello mondiale"

****

13- Incidenti (Phishing, Vodafone Australia)

*** Phishing anche per rivendere quote di CO2 ***

Simone Tomirotti segnala questa notizia: il phishing non colpisce solo gli utenti dei sistemi di home banking.

Dal Financial Times Deutschland del 3 febbraio 2010: Dopo un primo attacco alla fine del 2009, alcuni hacker professionisti hanno colpito alcune imprese in Europa, in Giappone e in Nuova Zelanda. I pirati hanno inviato false mail chiedendo alle vittime di registrarsi di nuovo sulla piattaforma di scambio per prevenire un attacco informatico. Con queste nuove password hanno inviato dei diritti di emissione su dei conti in Danimarca e Gran Bretagna e poi li hanno rivenduti. Il numero di imprese vittime di questa truffa è ancora sconosciuto, "ma le verifiche di più di una dozzina di imprese in Germania ha già rivelato nove truffe". Di conseguenza il registro delle emissioni di anidride carbonica è stato chiuso in 13 paesi. "Questo sistema di scambio, che dovrebbe essere lo strumento per proteggere il clima, rivela la sua fragilità", commenta il quotidiano.
http://www.presseurop.eu/it/content/news-brief-cover/182761-gli-hacker-rubano-i-diritti-di-emissione

Da Presseurop del 21 gennaio 2011: "I ladri di quote colpiscono ancora". Alcuni hacker hanno rubato e poi rivenduto quote di CO2 di diversi paesi europei, riporta Libération. "Niente porte forzate, niente casseforti fatte saltare in aria con la nitroglicerina. Soltanto sistemi informatici di registri nazionali alleggeriti dei diritti di emissione" delle più grandi imprese austriache, greche, ceche, polacche e estoni, che il 19 gennaio si sono rese conto della portata dell'attacco. Secondo la Commissione europea i cyber-ladri hanno prelevato permessi per circa 3 milioni di tonnellate di CO2 e un valore di 200 milioni di euro. "Il furto rischia di intaccare la credibilità del giovane mercato europeo delle emissioni", precisa Libération. Un mercato "creato dal nulla dall'Unione europea nel 2005 per limitare le emissioni di carbonio delle industrie". Dal 2007 il mercato è costantemente il bersaglio degli attacchi dei criminali informatici.
http://www.presseurop.eu/it/content/news-brief/471771-i-ladri-di-quote-colpiscono-ancora

*** Incidente in Vodafone Australia ***

Dal SANS NewsBites Vol. 13 Num. 4: Vodafone Australia ha licenziato un numero imprecisato di persone dopo il recente incidente di sicurezza che ha compromesso la riservatezza dei dati di almeno 4 milioni di clienti.

Sono state fatte accuse di vendita a criminali di accessi al database clienti.
http://www.zdnet.com.au/vodafone-sacks-staff-over-data-breach-339308574.htm
http://www.itnews.com.au/News/244672,vodafone-sacks-staff-over-alleged-security-breach.aspx

In Italia non è così facile licenziare il personale. Però, ci sono già stati diversi casi di cambiamenti di fornitori a seguito di incidenti. Di chi sia poi la colpa, è sempre difficile da stabilire. Però tutto ciò ci insegna ad essere prudenti.

****

14- Business Continuity per disabili

Dalla newsletter del DRI Italy, ho trovato un riferimento ad un report di un workshop sulla gestione delle emergenze per persone disabili.
http://publicaa.ansi.org/sites/apdl/Documents/News%20and%20Publications/Links%20Within%20Stories/

Ho trovato interessante la parte sulle "evacuazioni" e i due link alla guida della NFPA (http://www.nfpa.org/categoryList.asp?categoryID=824) e al sito dell'ADA (http://www.ada.gov/).

Tutta roba USA, ma sicuramente interessante anche per noi e per questo tema spesso sottovalutato quando si tratta di Business Continuity.

****

15- Un cyber-esercito contro i pirati della rete

Simone Tomirotti segnala questa notizia chiedendosi "cosa succederà in Italia in questo ambito?"

Estonia - Un cyber-esercito contro i pirati della rete: Preoccupata dagli attacchi informatici alle sue istituzioni, l'Estonia ha formato un'unità di cyber-soldati volontari, la Küberkaitseliit (Lega di cyber-difesa, KKL), con l'obiettivo di proteggere il paese da nuove minacce, scrive Rzeczpospolita. Primo cyber-esercito volontario del mondo, la KKL fa parte del gruppo paramilitare estone Lega di difesa totale, e nell'eventualità dello scoppio di una guerra verrebbe posta sotto l'autorità militare. Per adesso è formata da 80 specialisti e ingegneri informatici che si incontrano una volta alla settimana per sventare attacchi informatici simulati. Leader nella diffusione dell'accesso a internet, l'Estonia è stata "il primo paese al mondo a permettere il voto via web nelle elezioni parlamentari. Per questo motivo un altro cyber-attacco potrebbe paralizzare l'intera nazione", ha dichiarato al quotidiano polacco Vahur Made, dell'Accademia diplomatica estone.
http://www.presseurop.eu/it/content/news-brief-cover/461991-un-cyber-esercito-contro-i-pirati-della-rete

Dal gruppo su LinkedIn del Clusit, Aldo Ceccarelli segnala un'analoga notizia questa volta dagli USA:
http://punto-informatico.it/3067360/PI/News/cybersicurezza-nsa-costruisce-fortezze.aspx?goback=%2Egde_54878_member_40284642

E infine, su theregister (segnalato dalla Forensic Focus newsletter, January 2011), un articolo dal titolo "Cyberwar hype is obscuring real security threats": troppa attenzione alla cyberwar che è improbabile e toglie energie alla prevenzione di minacce più probabili.
http://www.theregister.co.uk/2011/01/17/cyberwar_hype_oecd_study/

****

16- Norme armonizzate alle Direttive Europee

Alcune Direttive Europee stabiliscono i requisiti di sicurezza per alcuni prodotti. In particolare, ricordo che per gli strumenti elettrici ed elettronici, possono essere applicabili: la Direttiva Bassa Tensione (2006/95/EC), la Direttiva sulla compatibilità elettromagnetica (2004/108/EC), la Direttiva sugli apparati radio e di telecomunicazione (1999/5/EC). Per soddisfare i requisiti tecnici delle Direttive applicabili, è preferibile fare riferimento alle norme tecniche cosiddette "armonizzate".

Fino a poco fa, il sito www.newapproach.org era un ottimo punto di riferimento per sapere quali norme tecniche sono collegate alle Direttive, ma ho scoperto che non è più aggiornato da tempo.

Il link attuale è questo: http://ec.europa.eu/enterprise/policies/european-standards/documents/harmonised-standards-legislation/list-references/index_en.htm.

****

17- Futuri interventi di Cesare Gallotti (14 marzo)

Il 14 marzo dovrei intervenire alla sessione del Security Summit di Milano dedicata a itSMF con un intervento dal titolo "Sistemi di gestione integrati: come la ISO/IEC 20000 può essere di supporto alla ISO/IEC 27001".

Sarà un'occasione anche per parlare dei lavori sulla ISO/IEC 27013.

Il programma sarà su http://www.securitysummit.it/. Al momento, però, la situazione non è definitiva perché l'evento doveva coprire le giornate del 15, 16 e 17 marzo, ma la nuova festività del 17 ha imposto lo slittamento delle giornate al 14, 15 e 16 marzo con la conseguente necessità di rivedere tutto il programma.

Che desideriate o meno sentire il mio intervento, raccomando comunque di partecipare al Security Summit (organizzato dal Clusit) perché sempre utile per chi si occupa di sicurezza delle informazioni e non solo.