Cesare Gallotti

From: Cesare Gallotti [cesaregallotti@cesaregallotti.it]
Sent: Thursday, 17 December, 2009 23:37
To: 'Cesare Gallotti'
Subject: Newsletter del 17 dicembre 2009

****
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 secondo la licenza http://creativecommons.org/licenses/by-nc/2.5/it/.
E' possibile iscriversi, disiscriversi e modificare le proprie opzioni, oltre a vedere l'informativa sul trattamento dei dati personali, all'indirizzo http://www.cesaregallotti.it/newsletter.htm (per il momento, però, il tutto è ancora inattivo...)

****
Indice

****
01- Segnalazione di servizio e auguri

La newsletter ha cambiato Service Provider. Infatti, ho scelto di cambiare fornitore di mail e web hosting. Per questo motivo, come vedete, oggi è spedita in maniera "artigianale" e, a breve, cambieranno le modalità per iscriversi e disiscriversi. Nel caso vogliate conoscerle, vi rimando alla pagina http://www.cesaregallotti.it\newsletter.htm.

Spero poi di garantire la continuità del servizio senza creare disagi (mail di prova, ritardi superiori alla media, eccetera).

Colgo l'occasione per augurare a tutti Buone Feste.

****
02- Privacy e Amministratori di Sistema

La notizia è una non notizia: il Garante non abbia concesso ulteriori proroghe sul Provvedimento sugli Amministratori di Sistema.

Il 10 dicembre ha inoltre pubblicato delle "precisazioni".
http://www.garanteprivacy.it/garante/doc.jsp?ID=1676654

Le "precisazioni", mi par di capire, esonerano dal Provvedimento alcuni profesionisti e le associazioni.

Molti dubbi rimangono ancora non soddisfatti, sia su come applicare effettivamente le misure (come considerare gli utenti "amministratori" dei propri client? come si dovrebbero svolgere le verifiche annuali? qual è il livello adeguato di sicurezza dei log in modo da garantirne l'integrità?), sia sulla loro utilità (a cosa servirebbe conservare i soli log di connessione e disconnessione degli amministratori? perché conservare i log per 6 mesi se le verifiche devono essere ogni 12?).

Intanto, il terrore del Garante ha fatto partire una buona quantità di progetti e i produttori di software hanno distribuito prodotti "conformi al Provvedimento", senza però poter dare garanzie in merito.

****

03- Legge 166/299 - Decreto Ronchi (comunicazioni indesiderate e Privacy)

Dalla Newsletter Giuridica di Filodiritto ricevo segnalazione della conversione in Legge 166/2009 del Decreto Ronchi. L'articolo 20-bis introduce una nuova normativa per le comunicazioni indesiderate via telefono, modificando il Codice Privacy e il Codice del Consumo.

Non credo di avere tutte le competenze per commentare questa notizia, ma mi pare di capire che ora le comunicazioni telefoniche commerciali non si baseranno più sul principio di opt-in (ossia, possono essere fatte solo a chi esplicita la propria volontà a riceverle), ma sull'opt-out (ossia, è necessario esplicitare la volontà di non poterle più ricevere). Certamente, in termini di diritto alla privacy, non sembra un passo avanti.

Sulla newsletter del 10 dicembre 2009 del Garante è anche presente questa notizia: "E' vietato effettuare telefonare commerciali usando sistemi che generano numerazioni casuali. Tanto più se gli abbonati vengono contattati con chiamate preregistrate.
Lo ha stabilito il Garante privacy intervenendo contro una azienda vinicola a seguito delle segnalazioni di numerosi cittadini che lamentavano la ricezione di telefonate indesiderate, in alcuni casi preregistrate."

Il Decreto Ronchi:
http://www.parlamento.it/parlam/leggi/09166l.htm

Le mie versioni consolidate:
- Codice Privacy: http://www.cesaregallotti.it/normativa/privacy/2003_Dlgs_196.htm
- Codice Consumo: http://www.cesaregallotti.it/normativa/e-commerce/2005_Dlgs_206_Codice_consumo.htm

****

04- Decreto Pisanu e rintracciabilità delle connessioni

Il decreto Pisanu sugli obblighi di autenticazione di coloro che si connettono alla rete (misure anti-terrorismo) scadrà a fine anno. Sono in corso dei dibattiti pro-contro la sua proroga.

Il Clusit ha aperto una discussione su
http://blog.clusit.it/sicuramente/2009/12/wi-fi-lanonimato-il-decreto-pisanu.html

Duole dire che si trovano solo argomenti "contro". A me piacerebbe sapere se la misura, in questi 4 anni, è stata utile almeno una volta.

Non vorrei si scopra l'inutilità della misura, ma poi continuare a volerla tenere attiva perché "è giusto così". Troppo spesso mi sono imbattuto in responsabili della sicurezza che si rifiutavano di ammettere l'inutilità di alcune misure nel proprio contesto (deposito della Carta di Identità per accedere ad alcune sedi, richiesta di consegna di un foglio di uscita, registrazione dei laptop all'ingresso, siti di Disaster Recovery con capacità uguale al sito primario, richieste di cambiare le password ogni 30 giorni, eccetera), anche a fronte di evidenze sul loro eccessivo costo e cattiva gestione. Le imprese private pagano di tasca propria i loro eccessi di zelo, in questo caso pagherebbero i cittadini (in termini di riduzione del diritto di accesso alla rete, costi burocratici e di adeguamento tecnico per i gestori). E questo non sarebbe giusto.

Per chi volesse prima leggersi il testo vigente:
- Decreto Pisanu http://www.cesaregallotti.it/normativa/ISP_TLC/2005_dl_144_pisanu.htm
- Decreto "tecnico" http://www.cesaregallotti.it/normativa/ISP_TLC/2005-08-16-dm-pisanu.htm

Intanto, in UK, la misura è stata utile per sanzionare un pub inglese perché un avventore ha utilizzato la sua wi-fi per scaricare software protetto da copyright (da SANS NewsBites Vol. 11 Num. 94). Ma il decreto Pisanu non avrebbe questo scopo...
http://news.zdnet.co.uk/communications/0,1000000085,39909136,00.htm?tag=mncol;txt

****

05- Pubblicazione standard (Risk Management, ISO27k, ISO20k, ISO9k)

-- Risk Management --

Da Franco Ferrari (DNV) ricevo notizia che sono state pubblicate:
- ISO 31000 "Risk Management - Principles and guidelines"
- ISO/IEC 31010:2009 "Risk management – Risk assessment techniques"
- ISO GUIDE 73:2009 "Risk Management - Vocabulary"

La 31000 e la 73 non sono allineate al 100% alle ISO/IEC 27000:2009 e ISO/IEC 27001:2005, né sono particolarmente innovative, pertanto non sono fondamentali per coloro non coinvolti in discussioni teoriche. Sulla 31010 non mi pronuncio ancora (96 pagine uscite in novembre... abbiate pazienza).

Ovviamente, la loro utilità è incontestabile nella omogeneizzazione dei vocabolari utilizzati da altri standard.

-- Information Security --

E' stata appena appena pubblicata (7 dicembre) la
- ISO/IEC 27004:2009 "Information technology -- Security techniques -- Information security management -- Measurement".
Di più non ne so molto. I draft che ho avuto modo di osservare non mi avevano molto convinto, ma forse le cose sono migliorate.

Infine, con moltissimo ritardo, vi segnalo la pubblicazione della
- ISO/IEC 21827:2008 (Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®)).
Il SSE-CCM è un modello molto interessante. E' possibile scaricare la versione 3.0 del 2003 da http://www.sse-cmm.org/model/model.asp
Il link alla 21827 l'ho trovato sulla guida AIEA "Information Security Management System - Un valore aggiunto per le aziende", di cui raccomando la lettura perché presenta spunti di riflessione non triti e ritriti.

-- IT Service Management --

A ottobre è stata emessa la
- ISO/IEC TR 20000-3:2009 "Information technology -- Service management -- Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1"
La guida sarà probabilmente utilizzata come riferimento per gli Organismi di Certificazione (o Accredited Bodies) per accettare o meno le proposte di certificazione.

-- ISO 9001 e ISO 9004 --

Da NQA Italia ricevo notizia di modifica della ISO 9001: l'Appendice A "Corrispondenza tra la ISO 9001:2008 e la ISO 14001:2004", dove sono state corrette alcune corrispondenze tra i punti della UNI EN ISO 9001:2008 ed i punti della UNI EN ISO 14001:2004.

Per quanto riguarda la ISO 9004:2009, ne raccomando la lettura; soprattutto perché l'appendice A propone un interessante modello di maturità.

****
06- ITIL (v3.x e Guida per autostoppisti)

-- ITIL v3.x --

Come già annunciato, il TSO ha dato mandato per una revisione di ITIL
http://www.best-management-practice.com/gempdf/ITIL_Mandate_for_Change_0909.pdf

La volontà è quella di creare una versione 3.1 (o 3.x). E le cose vanno avanti (Da ITSM Neswletter):
http://www.sourcewire.com/releases/rel_display.php?relid=52376

-- Guida a ITIL per autostoppisti --

Dalla ITSM Newsletter vi segnalo la The Hitchhiker's Guide to ITIL. Utile per:
- chi vuole cominciare a conoscere ITIL (le cose sono tutte corrette, anche se accompagnate da un po' di humor)
- chi conosce già ITIL (ci sono alcune riflessioni molto interessanti)
- chi deve presentare o insegnare ITIL (alcuni spunti possono essere utilizzati per rendere i corsi o le presentazioni più dinamiche e più efficaci).

L'articolo cita Terry Pratchett. E questo basta per dire che l'autore è sicuramente un grande.

Il tutto è in inglese e, al momento, sono state pubblicate solo le prime due puntate.
- http://islebeebach.blogspot.com/2009/10/hitchhikers-guide-to-itil-introduction.html
- http://islebeebach.blogspot.com/2009/11/hitchhikers-guide-to-itil-introduction.html

****

07- Materiale conferenza itSMF

Sono disponibili gli atti della conferenza itSMF ai soli soci.

http://www.itsmf.it/index.php?method=section&action=zoom&id=1180

****

08- Materiale tecnico (Hardening e PCI-DSS)

-- Hardening --

Da una segnalazione del SANS, ho "scoperto" che la NSA pubblica delle linee guida per l'hardening dei sistemi operativi.

Non è certo comoda da trovare, ma il link è
http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml

Sul menu a sinistra si trovano le tipologie di prodotti e poi si possono scaricare le guide.

Inutile dirvi che questo interesse della NSA per l'hardening ha già fatto nascere delle teorie complottiste
http://www.theregister.co.uk/2009/11/19/nsa_enhanced_windows7_security/

-- PCI-DSS --

Vi segnalo la pubblicazione di un nuovo Quaderno Clusit: "PCI-DSS: Payment Card Industry - Data Security Standard", scritto da Jean Paul Ballerini e Fabio Guasconi.

Il nuovo quaderno è disponibile all'indirizzo http://www.clusit.it/download/index.htm e la sua consultazione è riservata ai soci.

****

09- Computer Forensics

Mattia Epifani segnala la nascita di una rivista elettronica interamente dedicata alla Digital Forensics ed edita in UK. Registrandosi al sito si può scaricare gratuitamente il primo numero (L'abbonamento per i quattro numeri annuali del 2010 costa 54 sterline.)
http://www.digitalforensicsmagazine.com/

Il NIST, invece, segnala la pubblicazione della NIST IR 7617 dal titolo "Mobile Forensic Reference Materials: A Methodology and Reification"
http://csrc.nist.gov/publications/nistir/ir7617/nistir-7617.pdf

_____

Cesare Gallotti
Ripa Ticinese 75

20143 Milano (Italy)
Tel: +39.02.58.10.04.21
Mobile: +39.349.669.77.23
Web: http://www.cesaregallotti.it
Mail: cesaregallotti@cesaregallotti.it