****
IT SERVICE MANAGEMENT NEWS - Ottobre 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- Idea fallita (un convegno che non ci sarà)
02- Videosorveglianza, standard ISO e Garante Privacy
03- Posta Elettronica Certificata -- Scadenza e professionisti
04- Dispositivi mobili aziendal-personali
05- Divieto di concorrenza
06- Le sanzioni disciplinari nel rapporto di lavoro. Cenni introduttivi
07- Vulnerabilità SCADA
08- Pagina normativa "informatica"
09- Mio prossimo intervento sulle norme ISO/IEC 270xx

****
01- Idea fallita (un convegno che non ci sarà)

Ci ho provato, ma ho avuto poche adesioni: il "convegno come l'avrei voluto fare io" non ci sarà.

Sono molto dispiaciuto, ma me ne farò una ragione.

Per recuperare, il 10 novembre terrò un intervento alla Statale di Milano (vedere in fondo).

****
02- Videosorveglianza, standard ISO e Garante Privacy

Il 14 luglio il Garante Privacy ha emesso un provvedimento che permette alla società DNP Photomask Europe S.p.A. di conservare alcune immagini videoregistrate per 90 giorni, contrariamente al Provvedimento Generale del 8 aprile 2010 che impone un limite di 24 ore, a meno di eccezioni che possono portare fino al limite massimo di 7 giorni.

- http://www.garanteprivacy.it/garante/doc.jsp?ID=1836335

Cos'è successo? In altre occasioni il Garante ha chiesto di limitare il tempo di conservazione, qui addirittura permette di estenderlo fino a 13 volte il limite massimo ed eccezionale.

Un potenziale cliente (Infineon, tedesco) della società DNP ha richiesto alla DNP di adottare delle misure di sicurezza, tra cui la conservazione per 90 giorni delle immagini, in conformità alle loro procedure, "conformi alla ISO/IEC 17799 e alla ISO/IEC 15408".

Per i pignoli: il Provvedimento dice che la Infineon "opera rispettando i criteri dettati dal protocollo EAL5+ (ISO15408, ISO17799)", non che sono certificati (anche se un prodotto della Infineon è effettivamente certificato EAL5+)

Quindi, al punto 3 del Provvedimento, il Garante (Relatore: Fortunato) elogia gli standard internazionali dicendo alcune cose corrette e osservando che queste norme fissano "stringenti criteri" da prendere per buoni. Il tutto si conclude con: "si ammette la conservazione delle immagini per 90 giorni".

Ecco cosa c'è di sbagliato:
- il Provvedimento è del 14 luglio 2011; ormai da 6 (sei) anni, la ISO/IEC 17799 si chiama ISO/IEC 27002 (peccato veniale, ma allora sentiamoci autorizzati di citare la Legge 675 del 1996)
- le norme citate sono ISO/IEC non ISO (altro peccato veniale)
- la ISO/IEC 27002 (o 17799) non c'entra nulla con il "protocollo EAL5+"
- nessuna delle due norme citate fissa "stringenti criteri"; l'unico "stringente criterio" è che (semplifico) le misure di sicurezza devono essere commisurate al rischio analizzato dall'impresa; non si parla di "videosorveglianza", "90 giorni", "TVCC" o altre cose del genere (ho trovato solo un "suitable intruder detection systems")
- la ISO/IEC 27002 non fornisce "stringenti criteri" per sua natura (è una linea guida, da adattare caso per caso)

Alla luce di tutto ciò, provo a tradurre quello che è successo: la Infineon ha fatto le sue analisi del rischio (secondo un metodo e con risultati non riportati dal Provvedimento) e ha stabilito che il tempo giusto per conservare le immagini per lei e i suoi fornitori è di 90 giorni, lo richiede alla DNP, la quale DNP lo richiede al Garante, che dice "OK". Sintetizzo ancora: il Garante ha detto "se mi dite che avete fatto un'analisi dei rischi (che non vorrò vedere) che vi dice di conservare le immagini per 90 giorni, io approvo".

Non credo fosse quello il suo intendimento. Purtroppo, avendo accettato di trattare un argomento senza conoscerlo e senza averlo studiato, questo è il risultato.

Ma c'è un ulteriore effetto negativo della storia: si dà alle norme ISO/IEC citate un valore inesatto, esattamente come lo si dà alla ISO 9001. Come la ISO 9001 non garantisce l'alta qualità dei prodotti o servizi offerti, così la 27002 e la 15408 non garantiscono l'alta sicurezza dei prodotti o servizi o dell'azienda in assoluto. Non la faccio lunga, ma ricordo che Windows NT fu certificato EAL3, e oggi molti sistemi operativi Windows sono certificati EAL 4+... questo intuitivamente vi fa capire che non basta sapere "certificato", bisogna andare un poco oltre.

E infatti, da tempo, insieme ad altri colleghi, cerco di far capire che queste affermazioni sono false (il Garante invece ha dimostrato di prenderle per buone, soprattutto l'ultima; sarà forse perché tutte quelle sigle e quei numeri l'hanno confuso?):
- io sono certificato ISO -> sono al sicuro
- il mio fornitore è ISO -> è sicuro anche secondo i miei standard, anche se non glieli ho detti
- ricerco un fornitore ISO -> non ho bisogno di dirgli i miei requisiti di sicurezza perché tanto lui è sicuro -> non ho neanche bisogno di capire cosa c'è scritto sul certificato
- compro un prodotto ISO o da un fornitore ISO -> il prodotto è sicuro
- il mio cliente, fornitore o partner è ISO -> tutto ciò che dice è buono e giusto

Mi limito a concludere dicendo che:
- il Garante ha sbagliato
- se ha sbagliato qui, quante altre volte è stato superficiale nei Provvedimenti?
- come è possibile che il Garante non conosca almeno approssimativamente gli standard internazionali sulla sicurezza delle informazioni?
- allora è vero che emette Provvedimenti con misure di sicurezza da realizzare senza una base condivisa dagli specialisti della materia!

- Il Provvedimento Generale sulla videosorveglianza del 8 aprile 2010: http://www.garanteprivacy.it/garante/doc.jsp?ID=1712680#3.4
- il sito ufficiale dei Common Criteria: http://www.commoncriteriaportal.org/

Mi fermo qui. Qualcuno mi dia i riferimenti di un avvocato in caso riceva una querela.

****

03- Posta Elettronica Certificata -- Scadenza e professionisti

Prendendo spunto da una pubblicità che mi è arrivata, ricordo che "La legge n.2 del 2009 impone a tutte le Aziende, entro il 29/11/2011, di comunicare al registro imprese della C.C.I.A.A. il proprio indirizzo di casella PEC - Posta Elettronica Certificata."

Io non sono un'impresa, ma a breve attiverò la PEC.

Ha i suoi limiti (tra gli altri, vi segnalo l'articolo di Andrea Monti su Interlex "Posta certificata: troppe questioni ancora aperte"), ma mi pare sia utile.

L'articolo di Andrea Monti: http://www.interlex.it/docdigit/amonti92.htm
Inoltre segnalo questo articolo di Filodiritto sulla PEC per i professionisti iscritti agli albi professionali: http://www.filodiritto.com/index.php?azione=visualizza&iddoc=2457
Infine, segnalo anche questo sulla condanna alla Regione Basilicata per "mancato uso di PEC": http://www.filodiritto.com/index.php?azione=visualizza&iddoc=2456

****

04- Dispositivi mobili aziendal-personali

Lo scorso dicembre segnalai il fatto che oggi sempre più smartphones e tablet personali (per non parlare del pc di casa) sono utilizzati per il lavoro, visto che sono spesso migliori della strumentazione fornita dall'azienda.http://blog.cesaregallotti.it/2010/12/lasciatemi-il-mio-pc.html

Ora scopro che questa modalità ha un nome: BYOD, Bring your own device.

Segnalo quindi questo breve articolo pubblicato sul sito web dell'ISACA dal titolo "5 Information Risk Management and Security Tips When Adopting a BYOD Strategy for Mobile Devices": http://www.isaca.org/About-ISACA/-ISACA-Newsletter/Pages/at-ISACA-Volume-21-12-October-2011.aspx?utm_source=informz&utm_medium=email&utm_campaign=informz#2

****

05- Divieto di concorrenza

Da Filodiritto trovo questa sentenza della Cassazione sul divieto di concorrenza: la cessione del "solo" 40% delle quote societarie non implica il divieto di concorrenza previsto dall'articolo 2557 del Codice Civile.

La notizia, di per se, non riguarderebbe i temi di questo blog. Però ho capito il perché, in alcuni contratti, si impone la clausola di riservatezza per "almeno cinque anni" (per me dovrebbe valere per sempre, a meno che le informazioni non diventino pubbliche) dopo il termine del rapporto di lavoro per dipendenti) o del contratto per fornitori.

Infatti, l'articolo 2557 recita "Il patto di astenersi dalla concorrenza in limiti più ampi di quelli previsti dal comma precedente è valido, purché non impedisca ogni attività professionale dell'alienante. Esso non può eccedere la durata di cinque anni dal trasferimento."

L'articolo: http://www.filodiritto.com/index.php?azione=archivionews&idnotizia=3368
****

06- Le sanzioni disciplinari nel rapporto di lavoro. Cenni introduttivi

Segnalo questo interessante articolo di Filodiritto sulle sanzioni disciplinari nel rapporto di lavoro.

Come dice il titolo stesso dell'articolo, si tratta di una semplice introduzione. Penso comunque che sia necessaria:http://www.filodiritto.com/index.php?azione=visualizza&iddoc=2429

****

07- Vulnerabilità SCADA

La newsletter Sans NewsByte del 20 settembre segnala che "Un ricercatore italiano, Luigi Auriemma, ha pubblicato 13 vulnerabilità di alcuni prodotti SCADA (supervisory control and data acquisition). In marzo, Auriemma aveva già pubblicato altre 34 vulnerabilità."

La notizia su Computerworld:http://www.computerworld.com/s/article/9220099/Researcher_discloses_zero_day_flaws_in_SCADA_systems?taxonomyId=17

Per essere aggiornati in materia, segnalo il ICS-CERT, collegato al "Ministero della Sicurezza Interna" (Department of Homeland Security) degli USA: www.ics-cert.org.

L'ICS-CERT pubblica newsletter mensili e dei Vulnerability Report per gli ICS (o SCADA) che possono interessare i loro utilizzatori.

****

08- Pagina normativa "informatica"

Ho cambiato la pagina sulla normativa in materia informatica: http://www.cesaregallotti.it/Normativa.html

Ho infatti scelto di non allegare più una copia delle norme, ma di riinviare a siti come www.normattiva.it o quello del Garante Privacy (era impossibile tenere aggiornati i files).

Avrò fatto sicuramente molti errori: se li trovate, vi prego di segnalarmeli.

****

09- Mio prossimo intervento sulle norme ISO/IEC 270xx

La Digital Forensics Alumni ha organizzato per il 10 novembre 2011 (ore 16.30 - 18.30) un evento dal titolo "Considerazioni tecniche e giuridiche sulla ISO/IEC 27037 - guidelines for identification, collection, acquisition and preservation of digital evidence".

Io parteciperò raccontando delle norme della serie ISO/IEC 270xx (non più di 30 minuti), poi Alessandro Guarino dovrebbe parlare della ISO/IEC 27037 e infine ci sarà un dibattito con i legali.

Non dico molto di più perché i dettagli sono ancora da definire. Se mi vorrete scrivere tra un paio di settimane, dovrei fornirveli.