[IT Service Management News] Newsletter del 16 maggio 2010

****
IT SERVICE MANAGEMENT NEWS
****

Newsletter mensile con novità in materia di sicurezza delle informazioni, IT Service Management, Qualità.

E' possibile iscriversi o disiscriversi o scrivendo a cesaregallotti@cesaregallotti.it o seguendo le istruzioni riportate nella pagina http://www.cesaregallotti.it/newsletter.htm. Sulla stessa pagina è possibile consultare l'informativa sul trattamento dei dati personali.

****
Indice

****
01- Novità legali: Privacy e videosorveglianza
di Angelo Chiarot (Impronta Digitale srl)

Nell'aprile 2010, l'Autorità per la protezione dei dati personali ha definito il Provvedimento in materia di videosorveglianza pubblicato nella Gazzetta Ufficiale n. 99 del 29 aprile 2010, in sostituzione al precedente provvedimento del 29 aprile 2004.

Il Garante dei dati personali ha ritenuto necessario intervenire poiché:
- l'incremento massiccio dei sistemi di videosorveglianza quale forma di difesa passiva, controllo e deterrenza di fenomeni criminosi e vandalici, ha visto pervenire all'Autorità ingenti quantità di quesiti, segnalazioni, reclami e richieste di verifica;
- tra i numerosi interventi legislativi in materia, l'attribuzione a sindaci e comuni di specifiche competenze in materia di sicurezza urbana hanno incentivato l'utilizzo di telecamere.

In estrema sintesi, il Provvedimento puntualizza tempi, metodi e strumenti di conservazione delle informazioni e informative da rendersi agli interessati, secondo le finalità di acquisizione, con un distinguo di maggior rilievo tra i soggetti che impiegano la videosorveglianza, siano essi pubblici o privati.

Inoltre, dato il grado di evoluzione degli strumenti di acquisizione ed elaborazione di immagini, fisse o in movimento, in particolar modo per quelli con funzionalità di riconoscimento biometrico (in particolare i c.d. sistemi intelligenti), il Garante dispone che debbano essere da lui preventivamente sottoposti a verifica.

A mio avviso era indispensabile una maggiore diversificazione delle misure che facessero riferimento ai diversi soggetti con specifiche finalità di controllo (ad es. banche, ospedali, soggetti privati, eco-piazzole, ecc.). Tuttavia, al momento sono forse ancora troppo interpretabili e poco nitide le distinzioni tra la videosorveglianza per finalità di sicurezza urbana, con obbligo di informativa, e quelle di tutela della sicurezza pubblica, prevenzione o accertamento di reati e tutela delle persone e delle proprietà, prive invece degli obblighi di informativa e di consenso.

A tal proposito ricordo che in Italia, ai primi posti nel mondo per numerosità, sono installati circa 130.000 dispositivi per l'acquisizione di immagini.

Il Provvedimento è consultabile all'indirizzo:
http://www.garanteprivacy.it/garante/doc.jsp?ID=1712680
<http://www.garanteprivacy.it/garante/doc.jsp?ID=1712680>

****

02- Standard: ISO/IEC 19770

Franco Ferrari (DNV Italia) mi ha segnalato la recente pubblicazione della ISO/IEC 19770-2:2009 "Information technology - Software asset management - Part 2: Software identification tag".

Le norme della serie 19770 sono dedicate al software asset management, ossia ad un processo assimilabile al "Configuration Management" di ITIL e ISO/IEC 20000.

La parte 1 del 2006 descrive il processo di Software Asset Management e può anche essere usata per dichiarazioni di conformità. La ritengo interessante, anche se di non facile completa applicabilità.

La parte 2, citando la parte 1, "fornisce le specifiche per i dati di software asset management, realizzati dai produttori di software e di tool per l'IT Service Management". In altre parole, mentre la parte 1 riguarda processi e attività organizzative, la parte 2 è molto tecnica e si vedrà nel tempo se verrà effettivamente recepita dai produttori di software.

****

03- A proposito di change management e sicurezza

Il 21 aprile, il SANS NewsBites ha segnalato che "un recente aggiornamento dell'antivirus McAfee, a causa di un falso positivo, blocca i sistemi con Windows XP SP3".

Purtroppo sento ancora responsabili IT convinti che "certi change" non richiedono test preventivi...

Articolo "divulgativo": http://krebsonsecurity.com/2010/04/mcafee-false-detection-locks-up-windows-xp/ <http://krebsonsecurity.com/2010/04/mcafee-false-detection-locks-up-windows-xp/>
Articoli più tecnici:
http://isc.sans.edu/diary.html?storyid=8671 <http://isc.sans.edu/diary.html?storyid=8671>
http://isc.sans.edu/diary.html?storyid=8656 <http://isc.sans.edu/diary.html?storyid=8656>

****

04- ROSI o Return Of Security Investment

Dagli atti del Security Summit di Milano, ho trovato interessante la presentazione sul ROSI (Return of Security Investments).

Per me, il ROSI inteso come "analisi quantitativa dei costi e benefici in termini strettamente economici delle misure di sicurezza" è un'illusione: infatti, è possibile calcolare quasi precisamente i costi di introduzione di una misura di sicurezza, ma non i benefici, dato che non è possibile sapere correttamente i danni che può portare un attacco riuscito, perché se sono difficilmente calcolabili i danni diretti e indiretti, è impossibile calcolare quelli consequenziali (i danni all'immagini, tanto per intenderci).

Il lavoro scaricabile da http://rosi.clusit.it/pages/Homepage.html <http://rosi.clusit.it/pages/Homepage.html> prende atto di questi limiti e presenta il ROSI da un punto di vista esplicitamente qualitativo.

Il lavoro mi lascia un poco perplesso, visto che propone un percorso che parte dalle "possibili misure da implementare" per calcolarne i benefici, inverso a quello tradizionale del risk management, che parte dai "possibili rischi" per arrivare a trovare le misure più appropiate.

Ad ogni modo, il lavoro è interessante, ed è accompagnato da tabelle degne di attenzione e da link da approfondire.

Due critiche: sembra che ogni membro del Gruppo di lavoro ha voluto inserire riferimenti alla propria società, rendendo un po' pesanti o confusi alcuni passaggi, inoltre non c'è la data di pubblicazione.

Sengalo anche i seguenti link collegati:
- https://www.clusif.asso.fr/fr/production/ouvrages/pdf/RoSI.pdf
<https://www.clusif.asso.fr/fr/production/ouvrages/pdf/RoSI.pdf>
- http://www.securityforum.org/ <http://www.securityforum.org/>

_____
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