****
IT SERVICE MANAGEMENT NEWS - LUGLIO 2012
****

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

****
Editoriale

Breve editoriale per segnalarvi che il prossimo appuntamento con la newsletter è per il 15 settembre: ad agosto sarò in vacanza e anche le notizie faranno altrettanto. Auguro buone ferie a tutti voi; se non doveste essere tra quanti in agosto si accalcano nei luoghi di villeggiatura o turistici del mondo, i miei auguri rimangono validi per quando visiterete quei luoghi in momenti meno affollati.

Vi ricordo che confido sempre nei vostri contributi sul blog o a questo indirizzo per rendere questa newsletter sempre più interessante.

Cesare

****

01- Novità legali: Cassazione su videosorveglianza

La Cassazione Penale, con Sentenza 22611 del 11 giugno 2012, ha stabilito che la videosorveglianza presso i luoghi di lavoro è legittima se il lavoratore ha prestato il proprio consenso.

La Cassazione ha basato la propria decisione considerando che lo Statuto dei lavoratori tutela verso forme "subdole di sorveglianza". A mio modesto parere, ha dimenticato che lo Statuto dei lavoratori tutela anche verso forme palesi ma eccessive di sorveglianza, richiedendo pertanto che siano autorizzate da organismi di categoria e non dai singoli lavoratori, i cui rapporti di forza con il datore di lavoro sono necessariamente squilibrati.

Questo non per fare polemica sindacale, ma per segnalare come questa interpretazione della Cassazione vada presa con le dovute cautele perché secondo me prima o poi ne emetteranno una contraria.

La notizia:
- http://www.filodiritto.com/index.php?azione=archivionews&idnotizia=3810

****
02- Classificazione incidenti

Su @ISACA Volume 14 del 3 luglio 2012 è riportata un'interessante classificazione degli incidenti di sicurezza (così, anche coloro che vogliono distinguere tra "incidenti" e "incidenti di sicurezza" possono sentirsi soddisfatti):
-
http://isaca.informz.net/z/cjUucD9taT0yNDcxNjk2JnA9MSZ1PTEwMjAwOTQ5NDUmbGk9MTIyOTU2NTk/index.html

Per i pigri, le categorie sono le seguenti:
- Accesso non autorizzato
- Denial of Service
- Malware
- Uso improprio
- Scansioni - Tentativi di accesso non autorizzato

Viene riportato un'ulteriore classificazione: "Investigazione", per i casi non ancora diagnosticati.

****
03- Anonimizzare i documenti

Pasquale Stirparo della DFA ha segnalato un link ad una sentenza pubblicata dopo "anonimizzazione":
- http://www.oppic.it/index2.php?option=com_docman&task=doc_view&gid=467&Itemid=60

E' da vedere per imparare cosa non fare.

Se non lo trovate più in rete, ve lo inoltro.

****

04- Esami di maturità e sicurezza

Sandro Sanna mi segnala questa ANSA dal titolo "Miur, hacker? 3 anni per decriptare chiave - Nessuna preoccupazione su ipotesi di eventuali assalti di pirati informatici" e si chiede: "sembra il lancio di una sfida... no?".
- http://www.ansa.it/web/notizie/maturita2012/news/2012/06/18/Miur-hacker-3-anni-decriptare-chiave-_7057957.html

Condivido il dubbio, anche se questa mattina (20 giugno) alla radio hanno detto che è andato tutto bene.

Mi sono fatto altre due domande:
- dicono che "la chiave è di 25 caratteri e può essere decifrata in 3 anni"; come è stato calcolato il tempo di tre anni?
- dopo anni di studi e di ricerche su come gestire lo scambio delle chiavi, il MIUR la scambia rendendola disponibile sul proprio sito web, al TG1 e su Televideo; nel futuro saranno adottate altre tecniche più conformi allo stato dell'arte in materia, con uso di algoritmi crittografici asimmetrici?

Mi sono anche dato le due risposte:
- non sanno come è stato calcolato il tempo dei 3 anni; l'intervistato o l'intervistatore si saranno confusi (la risposta è pervenuta grazie allo stesso Sandro Sanna che dopo aver saputo del mio dubbio è riuscito a girarlo a una persona del MIUR)
- non realizzeranno alcun meccanismo di scambio di chiavi pubbliche di cifratura: considerando l'elevato numero di destinatari e il fatto che le informazioni diventano pubbliche all'apertura delle "buste", questo metodo è il più efficace ed efficiente.

****
05- Il mercato delle vulnerabilità

Segnalo questo articolo della newsletter Crypto-gram di Bruce Scheneir dal titolo "The Vulnerabilities Market and the Future of Security":
- https://www.schneier.com/blog/archives/2012/06/the_vulnerabili.html

In poche parole, Bruce Schneier segnala la crescita del mercato delle vulnerabilità: diverse organizzazioni, incluse quelle governative, si stanno attrezzando per comprare vulnerabilità non ancora note e corrette per poi utilizzarle in segreto.

Questo ha due gravi conseguenze: la prima è che, ora, chi trova vulnerabilità non è più incentivato a segnalarle al produttore del software affinché le corregga e renda Internet più sicura; la seconda è che ci potrebbero essere sviluppatori invogliati a creare vulnerabilità nei software che producono rendendo Internet ancora più insicura.

****
06- LinkdIn non ha né CIO né CISO

Andrea Rui mi ha segnalato, questo articolo dal titolo "LinkedIn Has Neither CIO nor CISO".

L'articolo è successivo al furto delle password di molti utenti del social network avvenuto a inizio giugno 2012 (ecco il mio post in proposito: http://blog.cesaregallotti.it/2012/06/furto-delle-password-da-linkedin.html).

L'articolista è scandalizzato dal fatto che LinkedIn non abbia un Chief information officer né un Chief information security officer. Io invece non critico questa impostazione: meglio attribuire direttamente la responsabilità alla direzione, piuttosto che avere un pupazzo con il titolo altisonante di CIO, CISO, "capo xxx", "manager yyy", con la sola funzione di dire qualcosa sulla sicurezza e fare da capo espiatorio in caso di incidente.

L'articolo:
- http://www.govinfosecurity.com/blogs/linkedin-has-neither-cio-nor-ciso-p-1289?goback=.gna_60173