Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – FEBBRAIO 2014

****

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 dis-iscriversi
- 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- Ragazzi in rete

I ragazzi, come recentemente si è letto sulle prime pagine dei giornali, si suicidano a causa del cyberbullismo:
- http://www.corriere.it/cronache/14_febbraio_12/cerca-aiuto-online-ma-insultano-suicida-14-anni-c48f9e5a-93a8-11e3-84f1-d7c36ce692b4.shtml

Queste notizie non possono non turbarci.

Stefano Ramacciotti, Coordinatore GdL Educazione alla Sicurezza Informatica per (ISC)2 Italy Chapter, ha inviato ai soci di (ISC)2 dei link interessanti.

EU Kids Online, un'indagine effettuata a partire dal 2009 su incarico della Commissione Europea in 25 paesi dell'Unione, con l'obiettivo di conoscere cosa fanno i ragazzi in rete e il livello di competenza nell'utilizzo delle TIC ha coinvolto 25.000 giovani dai 9 ai 16 anni e i genitori. Il report è disponibile al link: http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/PerspectivesReport.pdf

A guide for parents. Education and new media:
http://www.saferinternetday.org/c/document_library/get_file?uuid=15f5f3ac-e6bb-4760-b6b0-eb4ca46a9829&groupId=10136

The Web We Want:
http://www.saferinternet.org/c/document_library/get_file?uuid=10c06ff7-9263-4996-a7d3-116340b9fe6f&groupId=10137

Infine, se qualcuno dovesse avere notizia di materiale altrettanto valido in italiano, lo prego di farmela avere per diffonderla.

Aggiungo che Stefano e altri si stanno prodigando facendo interventi nelle scuole e in altri contesti. A loro va tutta la mia ammirazione.

****

02- Standardizzazione: ISO/IEC 27000:2012

E' stata pubblicata la ISO/IEC 27000:2012 dal titolo "Information security management systems — Overview and vocabulary". In poche parole, si tratta delle definizioni delle norme della famiglia ISO/IEC 27000.

La norma è disponibile gratuitamente dall'URL:
- http://standards.iso.org/ittf/PubliclyAvailableStandards/

E' anche disponibile la versione del 2009, ma, ovviamente, è superata.

****

03- Standardizzazione: UNI/PdR 6:2014 sulle infrastrutture critiche

Franco Ferrari di DNV GL Italia mi ha segnalato la pubblicazione, il 16 gennaio, della prassi di riferimento UNI/PdR 6:2014 dal titolo " Infrastrutture Critiche - Sistema di gestione della resilienza - Requisiti".

Comunicato ufficiale e documento completo in pdf si trovano sul sito di AIPSA e di UNI:
- http://www.uni.com/index.php?option=com_content&view=article&id=2596:sistema-di-gestione-della-resilienza-delle-infrastrutture-critiche-pubblicata-la-prassi-di-riferimento&catid=111&Itemid=546
- http://www.aipsa.it/in-evidenza/tavolo-unipdr-tutela-delle-infrastrutture-critiche-ratifica-e-pubblicazione-unipdr-62014/

****

04- Novità legali: Direttiva e-commerce

La Direttiva Europea 2011/83 sui sui diritti dei consumatori è stata recepita dal'Italia con Decreto Legislativo del 3 dicembre 2013. Purtroppo, questo D. Lgs. non è stato ancora pubblicato in Gazzetta Ufficiale.

Esso è importante perché modifica il Codice del Consumo (Decreto Legislativo 206/2005) soprattutto nelle parti relative ai contratti a distanza ossia, se vogliamo usare l'inglese, all'e-commerce.

Appena ne avrò la notizia, provvederò a segnalare i riferimenti esatti del Decreto. Per intanto, segnalo l'interessante articolo di Filodiritto, in cui sono sintetizzate le novità (piuttosto impegnative per i venditori):
- http://www.filodiritto.com/governo-recepimento-direttiva-e-commerce-maggiori-tutele-per-i-consumatori-che-acquistano-online/

Attenzione che, secondo le ultime notizie, le nuove disposizioni entreranno in vigore dal 13 giugno 2014.

****

05- Creative Commons 4.0

Le Creative Commons sono licenze per chi desidera condividere i propri lavori con "alcuni diritti riservati". Per saperne di più:
- http://www.creativecommons.it/

A novembre 2013 sono state aggiornate alla versione 4.0. Potete trovare le novità sia sul sito italiano appena citato, sia qui:
- http://creativecommons.org/Version4

Ahimè... dovrò cambiare blog, sito e newsletter...

****

06- Principi di sicurezza per l'ingegnerizzazione IT

Lo confesso: di fronte al controllo A.14.2.5 "Principi per l'ingegnerizzazione sicura dei sistemi" della ISO/IEC 27001:2013 sono rimasto perplesso perché non capivo in cosa differisse dal controllo A.14.1.1 " Analisi e specifica dei requisiti per la sicurezza delle informazioni".

Ho trovato la SP800-27, meraviglioso documento del NIST dal titolo "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)":
- http://csrc.nist.gov/publications/PubsSPs.html

Lo trovo molto interessante, anche se continuo a non capire quali possano essere le differenze tra "specificare i requisiti di sicurezza" e "applicare principi di ingegnerizzazione sicura". Non capisco neanche quali siano le differenze tra progettazione (design) e ingegnerizzare. Forse qualche lettore mi aiuterà...

****

07- US Government's Cybersecurity-Framework

Preannunciato dal SANS NewsBites, è stato pubblicato il US Government's Cybersecurity Framework e lo si trova a questa pagina:
- http://www.nist.gov/cyberframework/

Ho cercato di capire di cosa si tratta. Riducendo al massimo, mi pare dica: fate un risk assessment e stabilite quali funzioni di sicurezza applicare. Mi ricorda un po' troppo la ISO/IEC 27001, anche per la presenza di 100 titoli di misure di sicurezza.

Per ciascun titolo sono riportati i documenti dove la funzione è meglio descritta (CCS CSC, COBIT 5, ISA 62443-2-1:2009, ISA 62443-3-3:2013, ISO/IEC 27001:2013 e NIST SP 800-53 Rev. 4). Ma allora che serve avere un nuovo elenco di misure (o controlli, o funzioni) di sicurezza se poi bisogna leggerne i dettagli altrove?

Un po' interessante è la suddivisione delle misure in 5 famiglie: identificazione, protezione, rilevazione, risposta e ripristino.

Un altro aspetto interessante è la possibilità di stabilire il livello (Tiers) di attuazione del framework, sulla base di valutazioni del processo di risk managment, integrazione del programma di risk management e di partecipazione di entità esterne. La descrizione dei livelli è ridotta poche righe e mi pare un po' poco.

Se qualcuno vuole segnalare posizioni diverse è il benvenuto.

****

08- NIST SP 800-53 rev 4.1 "Security and Privacy Controls..."

Il NIST ha annuciato la pubblicazione della rev 4.1 della Special Publication 800-53 dal titolo "Security and Privacy Controls for Federal Information Systems and Organizations".

Si tratta di un bel malloppone di 460 pagine; le prime 157 sono di introduzione, mentre le restanti riportano il catalogo di misure di sicurezza.

Interessante è la messa a disposizione di un file xml delle 4.124 misure di sicurezza, che può quindi essere utilizzato per check list o altro. Certamente, 4.124 misure sono tante!

Il link:
- http://csrc.nist.gov/publications/PubsSPs.html#800-53

****

09- Minacce e attacchi: Un errore di battitura ed ecco il malware!

Dal SANS NewsBytes segnalo questa notizia sugli errori di programmazione:
- http://www.bbc.co.uk/news/technology-26016802

In breve: sui siti del National Health Service del UK alcuni link rimandavano a siti pubblicitari o infestati da malware perché il programmatore aveva scritto Googleaspis al posto di Googleapis. Mi chiedo come abbiano fatto i test, ma questo caso rimane molto utile per ricordare come la programmazione sia un lavoro molto delicato.

****

10- Minacce e attacchi: Phishing alla CNN

Questo caso mi sembra interessante da analizzare (dal SANS NewsBites):
- http://www.darkreading.com/attacks-breaches/report-phishing-attacks-enabled-sea-to-c/240165675

In sintesi:
- le spie siriane (SEA) hanno inviato messaggi di phishing ben fatti al personale CNN;
- una persona di CNN ha creduto al messaggio e si è connessa con la propria user-id e password ad un sito fasullo;
- quelli della SEA hanno quindi usato il suo account per inviare tweet e post sul blog della CNN;
- la SEA ha usato il suo account anche per inviare altri messaggi di phishing; 5 nuove persone ci hanno creduto e hanno fornito le proprie credenziali al sito fasullo della SEA.

****

11- Le 25 peggiori password del 2013

Da gruppo Italian Security Professional di LinkedIn rilancio la notizia della pubblicazione del rapporto "Worst Passwords of 2013".

Il rapporto originale è qui, con una brevissima descrizione del metodo utilizzato:
- http://splashdata.com/press/worstpasswords2013.htm

La traduzione in italiano, con una comparazione dettagliata della lista del 2012 con quella del 2013:
- http://www.techeconomy.it/2014/01/22/le-peggiori-password-del-2013-e-come-scegliere-quella-giusta/

****

12- 5 metodi per costruire una cultura di sicurezza

Segnalo questo interessante articolo dal titolo "5 Solid Ways to Build Security Culture in Your Organization (That You Probably Never Heard Of)":
- http://infosecisland.com/blogview/23577-5-Solid-Ways-to-Build-Security-Culture-in-Your-Organization-That-You-Probably-Never-Heard-Of.html

I metodi sono i seguenti:
- insegnare alle persone a non dire NO,
- lasciar perdere i messaggi paranoici e sulle minacce,
- perseguire la felicità,
- discoraggiare la socializzazione,
- incoraggiare le camminate.

Come si vede dai titoli, sono argomenti nuovi e non abusati. Vale la pena approfondirli, anche per discuterne.

****

13- E-book "Grazie mr. Snowden"

Giusto giusto il mese scorso avevo detto che non mi sono occupato di Snowden, NSA, PRISM e compagnia.

Continuerò a non farlo, ma Sandro Sanna mi ha segnalato questo e-book gratuito indirizzato a chi avesse perso qualche puntata della saga:
- http://messaggeroveneto.gelocal.it/cronaca/2014/01/17/news/grazie-mr-snowden-scarica-gratis-l-e-book-di-fabio-chiusi-1.8486390