Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS –MARZO 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- Prossimi appuntamenti

Giovedì 20 marzo parlo al Security Summit di Milano, con Fabio Guasconi, di "Le nuove norme della famiglia 27000":
- https://www.securitysummit.it/milano-2014/

Il 5 giugno organizzo, come membro del Consiglio direttivo di DFA (www.perfezionisti.it), alla Statale di Milano, il DFA Open Day 2014 su questi due argomenti:
- OSINT e Investigazioni Digitali
- Security e Incident Response aziendale
Maggiori informazioni saranno date nei prossimi mesi.

****

02- Presentazione audit

Il 27 febbraio ho tenuto una lezione sugli audit presso la Facoltà di giurisprudenza dell'Università statale di Milano per il modulo "Le ispezioni e gli accertamenti del Garante: modalità di svolgimento, sanzioni comminate e strategie di difesa " del Corso di perfezionamento in privacy e data protection:
- http://www.cesaregallotti.it/Pdf/Pubblicazioni/2014-Audit.pdf

La pagina web da cui scaricarla:
- http://www.cesaregallotti.it/Pubblicazioni.html

****
03- Progettazione, ingegnerizzazione e sviluppo (ossia, "Parole")

A febbraio mi ero chiesto e avevo chiesto quali fossero le differenze tra progettazione (design) e ingegnerizzazione (engineering):
- http://blog.cesaregallotti.it/2014/02/principi-di-sicurezza-per.html

Premetto che, in effetti, non avevo dubbi tra progettazione e ingegnerizzazione, ma tra sviluppo (development) e ingegnerizzazione. Scrivendo mi sono confuso (era S. Valentino...), ma poi le risposte di Andrea Rui e Fabrizio Monteleone (DNV GL) mi hanno segnalato l'errore.

Fabrizio Monteleone mi ha anche ricordato che " la progettazione equivale a ideare un prodotto sulla base di requisiti; l'ingegnerizzazione significa cercare il miglior modo di realizzarlo (quali pezzi usare, possibilità di riutilizzare cose di un prodotto simile, futura manutenzione, ...) prima di poter rilasciare il progetto per la produzione". In poche parole: "l'ingegneria del software cerca di fornire le regole per il processo di produzione e quindi le regole di ingegnerizzazione sicura e le regole di sviluppo sicuro sono la stessa cosa".

Altri, a cui ho confidato il medesimo dubbio, la pensano più o meno allo stesso modo, ma usano il termine "sviluppo" solo per la realizzazione del software, ossia per la codifica. Usano il termine "ingegnerizzazione" per modellare sistemi, oggetti e database. Loro potrebbero ingegnerizzare senza sviluppare, ossia configurare dei sistemi senza sviluppare codice.

Per Andrea Rui (e anche per la ISO 9001, che differenzia "progettazione e sviluppo" e "realizzazione"), invece "lo sviluppo è quella fase che ti porta dalle specifiche al prototipo; l'ingegnerizzazione è quella fase che ti porta da questo al prodotto finale".

Rileggendo la NIST SP 800-27, vedo che i principi di ingegnerizzazione si applicano a tutte le fasi del ciclo di vita di un sistema: initiation, sviluppo o acquisizione, test e installazione, conduzione e manutenzione, eliminazione.

Riassumendo: per Fabrizio Monteleone prima si ha la progettazione, poi l'ingegnerizzazione e infine lo sviluppo; per Andrea Rui prima si ha la progettazione, poi lo sviluppo e infine l'ingegnerizzazione; per la NIST SP 800-27, l'ingegnerizzazione comprende la progettazione e lo sviluppo.

Questo dimostra ancora una volta come in informatica sia opportuno condividere per bene i termini con i propri interlocutori, perché ciascuno potrebbe utilizzarli in modi diversi. Per esperienza, quando chiedo spiegazioni sull'uso di certi termini, mi guardano come se fossi uno sciocco, quando sono invece loro che non hanno idea di cosa succede al di fuori del loro piccolo mondo. Citando Andrea Rui: "sui termini

occorre spesso fare delle mappature tra i diversi significati attribuiti da enti diversi e dai diversi contesti d'uso (insomma, occorre introdurre i namespaces!)".

Per concludere, cito ancora Andrea Rui che mi ha ribadito dei concetti fondamentali, a prescindere dalla terminologia utilizzata: "trattandosi di fasi distinte, a cui lavorano figure e persone diverse attraverso attività diverse, occorre che per ciascuna siano analizzati i rischi e definite le appropriate misure di sicurezza da adottare; inizialmente occorre identificare i requisiti di sicurezza legati alle caratteristiche e funzionalità; per quanto riguarda la realizzazione, occorre identificare a priori tutti i requisiti di sicurezza che il processo di realizzazione (analisi, sviluppo, ecc.) deve avere per assicurare che il processo di gestione del ciclo di vita del prodotto non limiti o riduca la sicurezza progettata".

****

04- Legale: Libertà di link

Segnalo questo articolo di Filodiritto dal titolo "Corte di Giustizia: libero link in libera rete, purché verso contenuti liberamente disponibili nel sito linkato":
- http://www.filodiritto.com/corte-di-giustizia-libero-link-in-libera-rete-purche-verso-contenuti-liberamente-disponibili-nel-sito-linkato

In sintesi: "Un sito internet può contenere al suo interno diversi link con cui rinvia a opere protette dal diritto d'autore, liberamente accessibili in altri siti, senza il consenso dei titolari del diritto".

Meno male: sono anni che lo faccio sul blog e sulla newsletter e non mi era mai sorto il dubbio di commettere reato. Infatti non lo facevo, ma ora ne ho la conferma al 100%.

****

05- Standard: ISO/IEC 27000:2014 (errata corrige)

Avevo precedentemente annunciato la pubblicazione della ISO/IEC 27000:2012, ma volevo annunciare la pubblicazione della versione del 2014. Grazie a Franco Ruggieri e Fabio Guasconi per avermi avvisato per primi.

Mi scuso con tutti e confermo che la norma si può trovare a questo link:
- http://standards.iso.org/ittf/PubliclyAvailableStandards/

****

06- Standard: Standard ETSI per accessibilità

Da UNINFO ricevo la notizia della pubblicazione di alcuni nuovi standard ETSI relativi all'accessibilità dei prodotti ICT. Il comunicato stampa, con link alla pagina dove trovare gli standard:
- http://www.cencenelec.eu/News/Press_Releases/Pages/PR-2014-03.aspx

In particolare è stato pubblicato lo standard EN 301 549 dal titolo "Accessibility requirements suitable for public procurement of ICT products and services in Europe". Lo standard riporta molti requisiti tecnici per rendere accessibili gli strumenti ICT a tutti.

****

07- Minacce e attacchi: Malware The Mask

Da Crypto-Gram rilancio la notizia dell'individuazione di un nuovo malware APT detto The Mask:
- http://www.wired.com/threatlevel/2014/02/mask/

Sembra che questo malware sia usato da 7 anni per spiare agenzie governative soprattutto in Marocco e Brasile.

****
08- Minacce e attacchi: ATM e dispositivi medici

Sul SANS NewsBites del 18 febbraio ci sono due notizie a mio parere collegate.

La prima riguarda gli ATM (ossia i Bancomat): in un Paese ignoto, dei malfattori sono riusciti a manomettere gli ATM e, inserendo una chiave USB, ottenere i soldi:
- http://www.darkreading.com/attacks-breaches/criminals-control-cash-out-banks-atm-mac/240166070

La seconda i dispositivi medici negli ospedali: il US Department of Health and Human Services (HHS) Office of Inspector General (OIG) ha deciso di effettuare degli audit presso gli ospedali per verificare se i loro dispositivi sono configurati per garantire un adeguato livello di sicurezza ai dati dei pazienti:
- http://www.govinfosecurity.com/oig-to-review-medical-device-security-a-6490

Cosa hanno in comune queste due notizie? Traduco liberamente e modifico un poco il commento di Murray, editor del SANS NewsBites: "un tempo questi dispositivi erano solidi, presso dei locali controllati, utilizzavano del software proprietario ad hoc, con reti e protocolli ad hoc, condotti e gestiti dall'ente stesso. Oggi questi dispositivi sono come degli elettrodomestici, siti in locali non sempre controllati, con software solitamente installato su Windows, su reti e protocolli pubblici, condotti e gestiti da terze parti. Questo ha fatto aumentare le possibilità di attacco e le vulnerabilità; le notizie sugli attacchi possono essere drammatiche, ma non sorprendenti".

Qui, a mio parere, è sottintesa un'altra conclusione: "sono cambiate le architetture dei dispositivi e i loro interfacciamenti, ma produttori, installatori, manutentori e utilizzatori continuano a progettarli, installarli, mantenerli e usarli come se ciò non fosse mai successo".

_____
Cesare Gallotti
Ripa Ticinese 75
20143 Milano (Italia)
Tel: +39.02.58.10.04.21
Mobile: +39.349.669.77.23
Web: http://www.cesaregallotti.it
Blog: http://blog.cesaregallotti.it
Mail: cesaregallotti@cesaregallotti.it
PEC: cesaregallotti@mailcert.it