Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – NOVEMBRE 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- "Sicurezza delle informazioni" su carta

Vi segnalo, sempre a mo' di pubblicità, che ora è possibile acquistare il libro "Sicurezza delle informazioni", di cui sono autore, anche in formato cartaceo su www.lulu.com.

L'ho messo a 15 Euro (a cui aggiungere i costi di spedizione di circa 8 Euro). Il libro è acquistabile solo on-line:
- http://www.lulu.com/shop/cesare-gallotti/sicurezza-delle-informazioni-valutazione-del-rischio-i-sistemi-di-gestione-per-la-sicurezza-delle-informazioni-la-norma-isoiec-270012013/paperback/product-21861741.html

****

02- Standardizzazione: Stato delle norme ISO/IEC 270xx

Venerdì 24 ottobre si è concluso a Santa Fe (Messico) il 49mo meeting dell'SC 27 dell'ISO/IEC JTC 1. Purtroppo, causa cancellazione del volo, non ho potuto partecipare. A rappresentare l'Italia c'erano solo Fabio Guasconi (Presidente SC 27 italiano) e Andrea Caccia.

Provo comunque, sulla base del documento finale "WG 1 Recommendations, Resolutions and Acclamations", ad indicare lo stato di avanzamento delle norme in discussione:
- ISO/IEC 27000 (Panoramica e vocabolario); il documento è stato proposto per il passaggio in DIS;
- ISO/IEC 27003 (Guida alla ISO/IEC 27001); il documento è stato proposto per il passaggio in CD;
- ISO/IEC 27004 (Monitoraggi, misurazioni, analisi e valutazioni); il documento è stata proposta per il passaggio in CD;
- ISO/IEC 27005 (Gestione del rischio); rimane in stato di WD;
- ISO/IEC 27006 (Requisiti per gli organismi di certificazione rispetto alla ISO/IEC 27001); è stata proposta per il passaggio in DIS;
- ISO/IEC 27007 (Linee guida per gli audit dei sistema di gestione per la sicurezza delle informazioni); rimane in stato di WD;
- ISO/IEC 27008 (Linee guida per gli audit dei controlli di sicurezza delle informazioni); rimane in stato di WD;
- ISO/IEC 27009 (Requisiti per l'applicazione della ISO/IEC 27001 in settori specifici); rimarrà in stato CD;
- ISO/IEC 27010 (Sicurezza nelle comunicazioni tra settori e organizzazioni); il documento è stato proposto per il passaggio in DIS;
- ISO/IEC 27011 (controlli di sicurezza per il settore delle telecomunicazioni); rimarrà in stato CD;
- ISO/IEC 27013 (relazioni tra ISO/IEC 27001 e ISO/IEC 20000-1); è stata proposta per il passaggio in DIS;
- ISO/IEC 27017 (controlli di sicurezza per il cloud computing); è stata proposta per il passaggio in DIS;
- ISO/IEC 27021 (Competenze per i professionisti dei sistemi di gestione per la sicurezza delle informazioni); rimane in stato di WD;
- ISO/IEC 27023 (Mappa dei requisiti delle versioni del 2005 e del 2013 delle ISO/IEC 27001 e ISO/IEC 27002).

E' opportuno ricordare che i documenti attraversano diversi stadi prima della pubblicazione: WG (Working draft), CD (Committee Draft), DIS (Draft), FDIS (Final Draft).

Altre discussioni hanno riguardato:
- il futuro riesame della ISO/IEC 27019 (controlli di sicurezza per il settore energia);
- la redazione di un " Cloud Adapted Risk Management Framework";
- la redazione di un documento relativo alla "Information Security Library";

Essendo io assente, il povero Fabio Guasconi ha dovuto difendere da solo i miei numerosi commenti sulla ISO/IEC 27003 e non ho potuto aiutarlo sulle sue proposte per altre norme. Con queste poche righe, rendo merito alla sua capacità di portare avanti le istanze italiane.

Molta discussione si è fatta sulla ISO/IEC 27006 su due punti. Il primo riguarda la durata degli audit: attualmente le giornate previste per le organizzazioni piccole o molto piccole sono, a parere di alcuni, troppo numerose (per le aziende di 5 persone si richiede un minimo non derogabile di 4 giornate). Il secondo riguarda la necessità o meno di prevedere esplicitamente negli audit la verifica di come sono attuati i controlli di sicurezza previsti dall'Appendice A della ISO/IEC 27001. Come Italia, siamo ovviamente favorevoli a verificare i controlli di sicurezza, ma in un numero di giornate ragionevoli (purtroppo, troppi auditor si accontentano di verificare solo i documenti o di fare interviste ai top

manager, senza verifiche sul campo). La nostra posizione è quindi difficile perché richiede di bilanciare due esigenze diverse (tempi e costi degli audit ragionevoli e adeguato livello di profondità).

Il prossimo meeeting sarà a inizio maggio 2015 a Kuching, in Malesia (isola di Borneo).

****

03- Standardizzazione: UNI EN ISO 22301:2014

Franco Ferrari di DNV GL mi informa che il giorno 11-09-2014 è stata pubblicata la UNI EN ISO 22031:2014.
- http://store.uni.com/magento-1.4.0.1/index.php/uni-en-iso-22301-2014.html

Si tratta della versione ufficiale in lingua inglese della norma europea EN ISO 22301 (edizione luglio 2014), che a sua volta è il recepimento della ISO 22301:2012.

Nulla cambia tra le diverse versioni, a parte, ovviamente, che la UNI è in italiano e non in inglese.

****

04- Standardizzazione e certificazione: ISO Survey 2013

E' stata pubblicata la ISO Survey del 2013, relativa alla diffusione nel mondo dei certificati ISO 9001 (qualità), ISO 14001 (ambiente), ISO 50001 (energia), ISO/IEC 27001 (sicurezza delle informazioni), ISO 22000 (sicurezza alimentare), ISO/TS 16949 (qualità nel settore Automotive) e ISO 13485 (qualità dei dispositivi medici):
- http://www.iso.org/iso/home/standards/certification/iso-survey.htm

Dalla pagina dell'ISO è possibile scaricare l'executive summary e i dati di dettaglio. Vedo anche che l'Italia ha "ben" 901 certificati ISO/IEC 27001 e si colloca al quinto posto (dopo Giappone, India, UK e Cina).

La notizia me l'ha fornita la newsletter del DNV GL:
- http://www.dnvba.com/it/information-resources/news/Pages/iso-survey-2013.aspx

****

05- Cosa vuol dire "Certificazione ISO/IEC 27001"?

Questo articolo, segnalatomi dal gruppo "Certified Information Systems Auditor" di LinkedIn avrei voluto scriverlo io, per quanto è chiaro, completo e sintetico:
- https://parkersolutionsgroup.wordpress.com/2014/10/15/what-does-iso-27001-certification-really-mean/

Visto che è bello trovare difetti: io avrei scritto ISO/IEC 27001 (corretto) al posto di ISO 27001 (scorretto).

****

06- Novità legali: DM 115 del 2014 e certificazione per Istituti di vigilanza privati

Secondo il nuovo decreto n.115/2014, gli istituti di vigilanza privati, per poter operare, devono obbligatoriamente ottenere il certificato di conformità dei propri servizi, impianti e professionisti secondo le norme UNI 10891 (istituti di vigilanza privata), UNI 50518 (centri di monitoraggio) e 10459 (professionista della security) e da parte di un organismo di certificazione accreditato da un Ente designato, quale Accredia in Italia.

Il decreto ministeriale prevede un passaggio immediato per le nuove licenze e nuovi istituti e una transizione di 36 mesi per chi è già certificato per le disposizioni del precedente decreto 269 del 2010.

Ricordo che la vigilanza e la sicurezza fisica sono controlli importanti per assicurare la sicurezza alle informazioni.

Quanto sopra scritto, tranne l'ultima riga, l'ho copiato dalla pagina del sito di DNV GL:
- http://www.dnvba.com/it/information-resources/news/Pages/Servizi_Vigilanza_Privati.aspx

****

07- Nuove linee guida Confidustria per 231

Dalla newsletter di Protiviti segnalo che Confindustria ha pubblicato le nuove Linee Guida per la costruzione dei "Modelli 231".

Il link è decisamente molto lungo (grazie a Nicola Valenza di Objectway per avermelo dato):
- http://www.confindustria.it/wps/portal/IT/AreeTematiche/Diritto-d-impresa/Documenti/Dettaglio-doc-diritto-impresa/4eaa0336-f353-4bc8-aa05-35dfda228a50/4eaa0336-f353-4bc8-aa05-35dfda228a50/!ut/p/a0/04_Sj9CPykssy0xPLMnMz0vMAfGjzOJ9PT1MDD0NjLz83UxNDBxNgpwCfYzdLCzDTPQLsh0VAVhK9gI!/

Le linee guida sono divise in due parti: una generale con i requisiti e una parte speciale, dedicata all'approfondimento dei reati e ad un metodo di analisi.

****

08- Atti del Privacy Academy and CSA Congress 2014

Antonio Salis di Tiscali, che ringrazio, segnala gli atti del Privacy Academy and CSA Congress 2014:
- https://privacyassociation.org/conference/privacy-academy-2014/sessions/

Devo dire che le presentazioni sono numerose e interessanti. Quasi mai dicono "le solite cose" su privacy, cloud, sicurezza, audit, eccetera. Anzi...

****

09- I VA sono la sicurezza applicativa?

Negli ultimi tempi ho notato che a fronte della domanda "come assicurate la sicurezza delle applicazioni?" mi viene risposto: "facciamo dei vulnerability assessment, dei penetration test e delle code review". Peccato che queste pratiche siano realizzate a fine lavori (in rari casi, anche in fasi intermedie), mentre la sicurezza andrebbe considerata sin dall'inizio, quando si stabiliscono i requisiti funzionali, si progetta il software e la sua architettura e si scelgono gli strumenti di sviluppo e i compilatori; un poco dopo, ma sempre prima dei VA-PT-CR, si dovrebbero stabilire degli standard di codifica.

Perché quindi in molti riducono la sicurezza applicativa ai VA-PT-CR? Provo con delle deduzioni, ma è bene precisare che si applicano a coloro che veramente intendono assicurare un buon livello di sicurezza alle applicazioni; non è questa un riflessione sul perché molti non si interessano all'argomento.

In molti riducono la sicurezza applicativa ai VA-PT-CR perché:

1- i venditori dei servizi di VA-PT-CR sono molto più bravi dei venditori dei servizi di sicurezza a supporto dell'analisi, progettazione, sviluppo e realizzazione dei software;
2- quasi nessuno offre buoni servizi di sicurezza a supporto dell'analisi, progettazione, sviluppo e realizzazione dei software; i tecnici migliori e più preparati si dedicano a fare VA-PT-CR, anche per attitudine (è molto più divertente cercare di bucare un'applicazione che scrivere documenti o scrivere codice); questa non è una critica, ma una presa d'atto delle diverse attitudini di ciascuno;
3- in effetti, chi offre servizi di sicurezza a supporto dell'analisi, progettazione, sviluppo e realizzazione dei software o è un consulente con pochissima conoscenza tecnica dello sviluppo (e quindi si limita a dire "individuate i requisiti di sicurezza fin dalla fase di analisi" senza poi dare ulteriori consigli), oppure riduce il tutto all'OWASP Top 10 (che riguarda alcuni aspetti della progettazione e non dell'analisi e dello sviluppo);
4- gli sviluppatori sono orientati a realizzare funzionalità, non la sicurezza; quindi è ben lontano dalla loro mentalità affrontare questo argomento sin dall'inizio;
5- i libri che trattano di questi argomenti sono pochissimi, molto voluminosi e molto costosi; ottime scuse per evitare di affrontarli, sia per gli sviluppatori (che quindi preferiscono affidarsi ad esterni che, per il punto 1, vendono solo VA-PT-CR) sia per i consulenti (che vendono già altri servizi più "di moda" senza doversi impegnare in una nuova materia difficile e poco richiesta).

Per dimostrare ulteriormente il punto 2, si osservi l'andamento dei progetti OWASP (owasp.org): la testing guide è stata aggiornata nel 2007, 2008 e 2014. La development guide, invece, è stata scritta inizialmente nel 2002, aggiornata nel 2005 e poi basta, anche se da diverso tempo stanno lavorando ad una nuova versione.

****

10- Minacce e attacchi: Rapporto semestrale MELANI

Io continuo ad apprezzare il lavoro fatto da MELANI della Confederazione Svizzera, che ogni 6 mesi pubblica il suo rapporto sulla sicurezza delle informazioni e in questi giorni è uscito quello della prima metà 2014:
- http://www.melani.admin.ch/dienstleistungen/archiv/01588/index.html?lang=it

E' opportuno ricordare il lavoro fatto in Italia dal Clusit (gli svizzeri sono bravi, ma anche noi lo siamo):
- http://clusit.it/rapportoclusit/

****

11- Minacce e attacchi: Poddle e SSL

Il protocollo SSL 3.0 è obsoleto e vulnerabile, anche a causa della tecnica di attacco Poddle. Si consiglia di usare il TLS anche perché una soluzione non è stata ancora realizzata.

La notizia è di settembre e quindi non così nuova. Quello che trovo interessante è un'altra notizia (arrivata con il SANS NewsBites): Apple migrerà su TLS e questa sarà una forte spinta al cambiamento. Mi chiedo quanti siti e servizi web stiano per migrare e ho il timore che siano molto pochi.

Un articolo interessante, che riporta anche il link all'articolo che descrive Poddle:
- http://www.cnet.com/news/apple-dumps-ssl-3-0-for-push-notifications-due-to-poodle-flaw/

****

12- Tecnologia: Nogotofail

Dal gruppo infotechlegale.it di LinkedIn giro la notizia: Google ha pubblicato uno strumento di verifica della sicurezza della rete denominato Nogotofail. Sembra essere dedicato alle vulnerabilità relative a TLS/SSL:
- https://github.com/google/nogotofail

Sarebbe interessante vedere se saranno pubblicate delle estensioni per un maggiore controllo della sicurezza di altri aspetti.

Chiedo ai lettori come questo strumento si affianca a un Nessus (o, meglio, OpenVAS che è gratuito): da quanto ho studiato, ques'ultimo dovrebbe rilevare queste e altre vulnerabilità e, quindi, il Notogofail sarebbe uno strumento inutile.

****

13- Tecnologia: Linee guida hardening (puntata 2)

Il mese scorso ho scritto un articolo sulle linee guida per l'hardening:
- http://blog.cesaregallotti.it/2014/10/linee-guida-hardening.html

Stefano Ramacciotti (che ringrazio) mi ha fatto notare che non ho citato le linee guida della NSA:
- https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/index.shtml

In effetti avevo guardato quelle relative ai sistemi operativi e alle applicazioni e mi erano sembrate troppo orientate ai sistemi domestici. Stefano però mi ha fatto notare che quelle per gli apparati CISCO sono eccezionali.

****

14- Tecnologia: messaggistica sicura

Dal gruppo Italian Security Professional di LinkedIn giro questo link:
- https://www.eff.org/secure-messaging-scorecard

Mette a confronto la sicurezza degli strumenti di messaggistica. Accanto a quelli molto noti come Whatsup, Skype e Viber, ce ne sono altri molto più sicuri.