Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – OTTOBRE 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- Correzioni alle ISO/IEC 27001 e 27002

Sono stati pubblicati due documenti di correzione rispettivamente della ISO/IEC 27001 e della ISO/IEC 27002 (grazie a Franco Ferrari di DNV GL per avermi avvisato).

Correzioni francamente non molto illuminanti. Ai controlli 8.1.1 e 8.1.3, in un paio di punti si è corretto "asset" con "informazioni e altri asset".

La cosa interessante è che erano state proposte altre correzioni per riferimenti incrociati sbagliati, frasi non concluse, eccetera, ma furono bocciati perché quegli errori non compromettono la comprensione della norma. Invece, meno male che sono state apportate queste correzioni.

A parte il sarcasmo, i più puntuali potranno trovare le correzioni sul sito della ISO (www.iso.org) con i documenti dal titolo:
- ISO/IEC 27001:2013/Cor.1:2014(en);
- ISO/IEC 27002:2013/Cor.1:2014(en).

I documenti veri e propri, per quanto io li abbia visti, non sono riuscito a scaricarli (manca proprio l'opzione). Ma è sufficiente chiedere di vedere la preview e li si legge (però ho dovuto usare IE e non Firefox).

****

02- Come non fare verifiche

Negli ultimi mesi mi è capitato di discutere su "come fare verifiche", sia come auditor, sia come consulente (dove le verifiche hanno lo scopo di raccogliere informazioni per un "assessment").

1 - Gli orali

Un primo approccio sbagliato prevede di svolgere verifiche solo attraverso interviste orali ai manager.

Tutti però dovremmo conoscere la relatività della narrazione. Si ricordi il racconto "Nel bosco" di Akutagawa o il film "Rashomon" di Kurosawa, che hanno reso artisticamente quanto non esistano narratori onniscenti e affidabili; per racconti più recenti, consiglio la prima stupenda stagione del telefilm "True detective".

Questo per dire che gli intervistati tendono a non raccontare difetti nei processi in cui sono coinvolti ed enfatizzano invece le carenze che giustificano l'avvio di progetti che invece vorrebbero iniziare. Quando queste narrazioni sono raccolte da una persona che le ordina non costituiscono però il risultato di una verifica professionale, che dovrebbe essere invece completa, esaustiva e il più possibile imparziale. Solo una verifica sul campo presso gli operatori e l'analisi diretta dei processi e dei loro risultati possono testimoniare come sono nella realtà, se sono adeguati, se presentano dei rischi che un manager spesso non rileva (in caso contrario, a cosa servirebbero gli specialisti?).

Ogni volta che ho avuto l'opportunità di fare verifiche sul campo ho trovato carenze più numerose e diverse di quelle segnalate dai manager nelle interviste.

Nell'ambito della sicurezza questo approccio presenta un'ulteriore difetto: ai consulenti viene spesso chiesto (e i consulenti spesso propongono) di fare una valutazione della sicurezza solo attraverso interviste ai manager e dei vulnerability assessment tecnologici, senza però mai analizzare quanto sta in mezzo, ossia le attività del personale tecnico.

Questo perché succede? Perché i manager non vogliono vedere messa in discussione la loro competenza e i verificatori temono la complessità di una verifica sul campo (per esempio, un conto è prendere nota del fatto che sono svolti e documentati i test, un altro è capire se sono completi e adeguati).

2 - La sala riunioni

Un secondo approccio sbagliato prevede di svolgere verifiche solo della "governance" o del "sistema di gestione".

Il termine "sistema di gestione" è quello usato per gli standard ISO 9001 ("Sistema di gestione per la qualità"), ISO/IEC 20000 ("Sistema di gestione per i servizi") e 27001 ("Sistema di gestione per la sicurezza delle informazioni"). Qui, alcuni intendono "sistema di gestione" come "sistema direzionale", dimenticando che la definizione non si limita ai soli "elementi per stabilire obiettivi, politiche e processi", ma anche agli "elementi per raggiungere gli obiettivi", tra cui, ovviamente, ci sono anche le attività operative.

Questo approccio, quindi, prevede di verificare solo le politiche, le procedure, la pianificazione e il monitoraggio delle azioni dei manager e altre cose documentali. Questo avviene spesso in una comoda sala riunioni.

Però, per comprendere se i processi sono veramente efficaci, e quindi se la governance o il sistema di gestione lo sono, non ci sono altri mezzi che vederli sul campo.

Sempre nell'ambito delle norme ISO più legate all'informatica come le ISO/IEC 20000 e 27001 (ma credo che ciò avvenga anche negli altri settori) alcuni teorizzano la natura particolare delle norme in questione. Però ho visto fare audit in sala riunioni anche per la qualità e vedo fare audit sul campo per tutte le altre. Temo che nel settore dell'informatica ci siano troppi "professionisti" che sanno discettare di processi in senso generale, ma hanno difficoltà a capire le differenze tra gestione dei sistemi e delle applicazioni (giusto per fare un esempio) o a capire perché Telnet non sia sicuro (questo l'ho visto con i miei occhi).

Il fatto che la ISO 9001 sia ritenuta una norma "semplice" o "inutile" è proprio dovuto al fatto che alcuni la interpretano erroneamente come un "insieme di documenti". E quindi pregherei i professionisti seri e preparati di non fare altrettanto con altre norme perché questo approccio ci porterà a degradare il mercato.

3- Le speranze

Un terzo approccio sbagliato prevede di svolgere verifiche dei piani e delle procedure, senza verificare come sono attualmente i processi. Questo approccio è un derivato del precedente e anch'esso prevede l'uso di una comoda sala riunioni per tutta la durata della verifica.

Certamente i piani di miglioramento futuri sono importanti perché danno conto di quanto un'organizzazione sia attenta alla realtà che la circonda e voglia adeguarsi, per quanta fatica questo comporti.

Però non riesco a considerare efficace un processo di sviluppo perché è previsto che tra un mese saranno svolti i test di quanto consegnato ai clienti, mentre fino ad oggi non lo si è mai fatto. Oppure efficace un processo di continuità operativa perché oggi si sta finendo di redigere i piani di continuità.

Interessante vedere come il "processo alle intenzioni" sia reputato una cattiva pratica, ma invece si consideri corretto il "processo alle buone intenzioni".

Ancora una volta: agli auditor e ai consulenti è richiesto di valutare la conformità a standard, politiche e procedure o l'efficacia dei processi attraverso prove materiali (o, per cattiva traduzione, a "evidenze"). Non attraverso le buone intenzioni.

Ho purtroppo l'impressione che chi propugni altri metodi lo faccia per pigrizia (lato auditor) o per furbizia (lato auditee), ma questo è fare solo del male alla cultura di "buona gestione".

****

03- Linee guida hardening

L'iniziativa del CIS di pubblicazione di guide sulla configurazione sicura dei sistemi risale a diversi anni fa, ma io la segnalo solo ora (anche grazie ad un cliente che me l'ha fatta ricordare):
- https://benchmarks.cisecurity.org/downloads/multiform/index.cfm

Le guide sono molto varie: dai sistemi operativi noti, ad alcuni middleware e apparati. C'è anche una guida sulle metriche (tra l'altro, mi pare interessante).

Solitamente i sistemisti "sanno" come configurare server, apparati, applicazioni e altro. Mi chiedo spesso come abbiano acquisito questo sapere. Secondo me si tratta di "esperienza acquisita in modo non strutturato". Forse l'uso di guide riconosciute potrebbe migliorare la sicurezza dei sistemi; o forse no...

Per scaricare le guide è necessario fornire un indirizzo di e-mail, non necessariamente esistente.

****

04- Apple e le forze dell'ordine

Pasquale Stirparo ha segnalato alla mailing list di DFA (www.perfezionisti.it) il fatto che Apple ha pubblicato delle "Legal Process Guidelines" con le istruzioni che devono seguire le forze dell'ordine diUSA, EMEIA, Giappone e APAC quando vogliono svolgere delle indagini e richiedono informazioni "sugli utenti che usano prodotti e servizi Apple o da dispositivi Apple":
- http://www.apple.com/privacy/government-information-requests/

Trovo questa iniziativa molto interessante. Secondo me, quasi nessuna azienda italiana ha una linea guida per gestire eventuali richieste da parte dell'autorità giudiziaria. Non dico si debba diffonderle per dare istruzioni alle forze dell'ordine come fa Apple (figurarsi!), ma qualcosa bisognerebbe fare. Al minimo, indicare internamente un referente interno nel caso arrivino richieste di questo tipo e disporre di un riferimento di un legale competente da consultare.

****

05- La lunga storia degli HSM (seconda puntata)

A luglio segnalai (su indicazione di Stefano Ramacciotti) un post sulla lunga storia degli HSM:
- http://blog.cesaregallotti.it/2014/07/la-lunga-storia-degli-hsm.html

Andrea Caccia, che di queste cose si occupa, mi ha aggiornato e io copio e incollo la sua gentile e-mail:
<< Proprio oggi (15 settembre 2014), l'OCSI ha pubblicato il primo certificato di un HSM per firma remota, che è quindi certificato CC EAL4+ secondo i requisiti di legge:
- http://www.ocsi.isticom.it/index.php/elenchi-certificazioni/prodotti-certificati#c0214

Il problema è che questo prodotto non è stato certificato entro i termini indicati dal decreto per predisporre i piani di migrazione.

Quindi, se è pur vero che ora l'apparato c'è, dopo tanti anni di autocertificazione, è anche vero che non è arrivato secondo i tempi che il decreto richiedeva e credo che questo porterà a parecchie discussioni. >>

****

06- Definizioni di cloud

Dopo l'articolo di settembre sul cloud forensics (http://blog.cesaregallotti.it/2014/08/cloud-forensics.html), mi hanno inviato due commenti interessanti.

Il primo, di Andrea Rui:
<< Mi permetto di dissentire su un requisito utilizzato per dare la definizione tecnica del concetto di Cloud: "Da un punto di vista meramente pratico un cloud esiste se esiste almeno un hypervisor (VMM)".

L'utilizzo di un hypervisor che consenta la coesistenza di più VM su un unico hardware è utile (anzi è necessario) nel caso che si vogliano far coesistere sistemi virtuali indipendenti e concorrenti. Esistono soluzioni 'Cloud' (tipicamente del tipo SaaS) che non necessitano di hypervisor, in quanto la separazione dei dati degli utenti viene garantita a livello architetturale ed applicativo, senza che sia indispensabile l'intermediazione di uno strato di virtualizzazione. >>

Il secondo, di Maurizio Nastro:

<< Il NIST, nella sua definizione di Cloud ("The NIST Definition of Cloud Computing", SP800-145), fa riferimento alla virtualizzazione nella parte relativa al "Resource Polling": The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand ...

Dalla definizione non è chiaro se il NIST intenda la virtualizzazione come condizione necessaria per un servizio Cloud.

La Cloud Security Alliance la interpreta come condizione non necessaria (https://cloudsecurityalliance.org/education/white-papers-and-educational-material/white-papers/, white paper "Virtualization Security By Chris Brenton", slide 3,4,5), in accordo con quanto scrive Andrea Rui. >>

Grazie Andrea e Maurizio per il vostro contributo. Vediamo se altri concordano o dissentono.

****

07- Cybersecurity nei dispositivi medici

Massimo Cottafavi di Reply mi ha segnalato la pubblicazione della guida "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices":
-
http://www.fda.gov/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356186.htm

Riporto quanto mi scrive:
<<Questo link porta ad un articolo di presentazione della guida:
- http://www.usatoday.com/story/tech/2014/10/01/fda-medical-devices-cybersecurity/16543731/

Mi sembra un passo importante anche solo per rimarcare e consapevolizzare rispetto alla criticità di un settore (quello medicale appunto) che ha fatto passi da gigante in termini di evoluzione tecnologica negli ultimi anni senza che a ciò sia corrisposta una altrettanto rapida ascesa nei sistemi di governo ed indirizzamento della sicurezza.>>

Condivido l'opinione di Massimo. La guida è più che altro un elenco di principi ed un rimando ad altri documenti. Trovo positivo che non abbiano scritto un altro elenco di controlli di sicurezza informatica.

****

08- Cyber Defence Symposium

Toto Zammataro di Intellium mi ha segnalato gli atti del Cyber Defence Symposium:
- http://www.rid.it/index~phppag,3_id,314.html

La lettura di alcuni articoli, tra cui quello di Toto Zammataro stesso ("Anatomia di un CERT") e quello di Marco Mattiucci ("Cybersecurity, Cyber Forensics e Digital Forensics: stato, evoluzioni ed attività dell'Arma dei Carabinieri"), è molto interessante, per quanto didattica.

Altri interventi, purtroppo, sono troppo commerciali.

****

09- Application whitelisting technology

Confesso la mia ignoranza sull'esistenza di tecnologie di application whitelisting. Ma andiamo con ordine.

La newsletter SANS NewsBites del 23 settembre riporta una notizia successiva ad un attacco alla catena Home Depot. L'attacco, molto semplice, era questo: un malware ha infettato i PC collegati ai POS dei negozi, in modo da inoltrare i dettagli delle carte di credito a quale malintenzionato (ma sembra che poi non siano stati usati per derubare i 56 milioni di malcapitati):
- http://www.theregister.co.uk/2014/09/18/home_depot_56m_cards_compromised/

Il danno è stato quantificato in quasi 250 milioni di dollari.

La notizia successiva riportava lamentele degli addetti alla sicurezza informatica di Home Depot perché le vulnerabilità erano state segnalate ma non considerate dai manager.

La cosa interessante è l'analisi di John Pescatore, sempre sul SANS NewsBites, ricorda che Home Depot poteva utilizzare delle tecnologie di application whitelisting, come segnalato dai "Critical security controls" del SANS stesso:
- http://www.sans.org/critical-security-controls/controls

Il controllo che ci interessa è il 2-1 che recita "Usa una tecnologia di application whitelisting che permette ai sistemi di far funzionare del software solo se è incluso in una lista e di bloccare ogni altro software. La lista può essere molto estesa e quindi può non avere impatti sugli utenti, oppure molto ridotta per sistemi critici".

Una breve ricerca su Google mi ha fatto incontrare il prodotto della Kaspersky (http://whitelist.kaspersky.com/).

Ora, io ho visto solo un'azienda che utilizza una versione ridotta di questa tecnologia (ogni notte analizza i PC degli utenti e disinstalla i programmi non autorizzati), ma non l'ho ancora vista ben pubblicizzata. Forse il motivo è in un'altra frase di John Pescatore: "Nel peggiore dei casi, la messa in funziona di una tecnologia di application whitelisting sarebbe costata a Home Depot 25 milioni di dollari, molto meno dei 250 che hanno perso". Diciamo che 25 milioni di dollari sono tanti...

Comunque, se qualche mio lettore vuole inviare dei contributi in materia, sarò ben lieto di pubblicarli.

****

10- Assumere un hacker per sbaglio

Questa è una storia interessante e starebbe bene in un libro o in un film:
- https://www.norse-corp.com/blog-140926.html

In poche parole: una donna con competenze da hacker trova lavoro nel settore marketing di una grande azienda.

Leggendo questa storia si capisce anche qualcosa di OSINT e le sue potenzialità e rischi.

****

11- TrueCrypt e CipherShed

Fabio Teoldi mi ha segnalato questa notizia: una società svizzera sta ri-ingegnerizzando TrueCrypt, ritenuto il miglior software per creare partizioni cifrate, e lo chiamerà CipherShed:
- http://www.esecurityplanet.com/open-source-security/truecrypt-getting-a-new-life.html

Il nome è terribile, ma spero si tratti di un buon prodotto, fatto da persone serie:
- https://ciphershed.org/

Per intanto, visto che funziona anche su Windows 8, io continuo a usare TrueCrypt felice e contento. Spero poi che il prodotto possa diffondersi e spingere il maggior numero di persone a prestare attenzione alla sicurezza.

****

12- PGP è da buttare?

Su Crypto-gram di settembre è riportata la notizia di un articolo molto critico su PGP:
- http://blog.cryptographyengineering.com/2014/08/whats-matter-with-pgp.html

Per un riassunto meno tecnico (sempre da Crypto-gram):
- http://thehackernews.com/2014/08/cryptography-expert-pgp-encryption-is_19.html

Per una critica all'articolo critico (sempre da Crypto-gram):
- https://pthree.org/2014/08/18/whats-the-matter-with-pgp/

La mia riflessione è un'altra, indipendentemente dai problemi tecnologici: oggi nessuno usa più strumenti crittografici per inviare e-mail in cui sono riportate informazioni o allegati molto riservati. Secondo me tutto ha origine dal fatto che nel 2002 la NAI ha smesso il supporto a PGP e gli altri progetti open-source hanno reso disponibili delle facili interfacce dopo troppo tempo (buffo, visto che una delle caratteristiche di PGP che lo resero popolare era proprio l'interfaccia grafica).

Oggi, si potrebbe fare riferimento a www.gnupg.org, ma in pochi lo fanno.