Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – LUGLIO 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- Standardizzazione: UNI CEI ISO/IEC 27002:2014

Finalmente è uscita la versione italiana della ISO/IEC 27002:2013 ed ha codice UNI CEI ISO/IEC 27002:2014. Purtroppo gli anni sono diversi e quindi si dovrà citare la "ISO/IEC 27002:2013" o la "UNI CEI ISO/IEC 27002:2014". Altri metodi denotano scarsa conoscenza della materia.

La ISO/IEC 27002 è una lettura consigliata per quanti vogliono occuparsi di sistemi di gestione per la sicurezza delle informazioni, anche se ci sono punti in cui è troppo generica o ripetitiva.

Faccio i complimenti a Fabio Guasconi, che ha coordinato il non semplice lavoro di traduzione delle 86 pagine della norma.

La norma è acquistabile sul sito dell'UNI: http://store.uni.com (la versione italiana della UNI CEI ISO/IEC 27002:2014 costa 98 Euro, mentre la versione inglese costa 75 Euro; infine la ISO/IEC 27002:2013 costa 153 Euro; non capisco che differenza ci possa essere tra queste ultime due).

Bisogna fare attenzione al metodo scelto da UNI per proteggere il diritto d'autore: si può aprire il file solo sul proprio computer e quindi va necessariamente stampato subito, per evitare che un crash ce lo faccia perdere per sempre.

****

02- Legale: Tribunale di Napoli ed efficacia probatoria dei log

Un'azienda ha provato che un suo dipendente accedeva abusivamente alle caselle di e-mail dei colleghi. Il dipendente è ricorso è ha vinto.

La storia è interessante perché, una volta tanto, il ricorso non è stato vinto a causa di informative inesistenti o scritte male o per regole di sicurezza informatica carenti, ma perché non è stata provata l'efficacia probatoria dei log.

Infatti è stato nominato un CTU (Consulente tecnico d'ufficio) che "ha constatato come sia stato possibile recuperare solo una copia dei log senza possibilità di verifica della conservazione sui sistemi di origine. I sistemi aziendali prevedono, infatti, un sistema di sovrascrittura dei file di log originari che sono andati così distrutti e l'implementazione di copia dei file di log" e pertanto "i sopra citati dati non siano attendibili né affidabili. L'azienda non ha adottato adeguate misure per attestare e precostituirsi l'immodificabilità e attendibilità dei file di log". " Nel momento in cui è stata effettuata la copia dei log che ricollegano al pc del ricorrente l'indirizzo Ip utilizzato – il contenuto del file non è stato sottoposto a nessun controllo di integrità al fine di sancire l'identità assoluta con il dato nel suo contenuto originale, così come prodotto dal sistema. Secondo il CTU, in assenza di tali garanzie, il dato dei file di log è alterabile. I log sono stati infatti esportati su file di testo, consultabili e alterabili con un normale strumento di edizione".

Si legge quindi che: "Osserva il CTU che, pur potendosi prospettare in astratto varie modalità di conservazione dei dati che avrebbero inconfutabilmente determinato la loro immodificabilità e attendibilità, le stesse non sono state adottate dal datore di lavoro; il sistema avrebbe dovuto produrre log firmati digitalmente e marcati temporalmente.

L'articolo di Altalex:

- http://www.altalex.com/index.php?idu=264948&cmd5=021c46ab76df2fd7050bbc8c56ed7fe1&idnot=67750

Di esso non condivido assolutamente le conclusioni (che gli adempimenti privacy erano formalistici e non sostanziali, la necessità di adottare sistemi di audit esterni certificati, la necessità di formazione per le aziende (che ci stanno a fare gli avvocati e i consulenti?). Condivido invece il richiamo al Provvedimento del Garante privacy del 1 marzo 2007.

****

03- Legale: Garante e biometria

Massimo Cottafavi di Spike Reply mi ha segnalato lo schema di Provvedimento del Garante in materia di biometria:

- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3132642

In particolare, mi ha segnalato le citazioni della ISO/IEC 27001. In poche parole, il Garante prevede per le organizzazioni certificate ISO/IEC 27001 delle semplificazioni in materia di misure di sicurezza per gli strumenti biometrici.

Non mi dilungo su alcune imprecisioni, la prima delle quali è che parla di un'inesistente ISO/IEC 27001:2006 e che non prende in considerazione la nuova norma del 2013 o la sua traduzione del 2014.

Il punto chiave è che sono esonerati dall'obbligo di istanza di verifica preliminare le organizzazioni già certificate ISO/IEC 27001 che estendono il proprio ambito di certificazione ai meccanismi crittografici. Per chi non è certificato è disponibile un percorso diverso. Massimo Cottafavi riflette:
"se uno è certificato ma non intende ampliare l'ambito di certificazione (per tanti motivi, il primo dei quali è il costo), apparentemente non può neanche seguire la strada alternativa".

Penso che abbia ragione e spero che il Garante modifichi il Provvedimento (ho mandato la riflessione seguendo la procedura).

****

04- ITIL: Eliminare il processo di Configuration management

In questo articolo, segnalato dal gruppo ITIL & ISO20000 Service Management + ITSM di LinkedIn, è proposta l'eliminazione del processo di configuration management da ITIL:
- https://community.servicenow.com/community/learn/blog/2014/06/27/dear-itil-please-kill-off-the-configuration-management-process

Il punto chiave è che troppe persone cercano di avere un database omnicomprensivo e accuratissimo degli asset collegati all'informatica. Solitamente, chi non adotta ITIL ma cerca di lavorare bene ha più "database" (degli asset personali come pc e cellulari, dei sorgenti se sviluppano, dei sistemi collegati alla rete, degli impianti, eccetera) e, quando possibile, con automatismi che permettono di identificare le variazioni da un momento all'altro.

Non credo, quindi, che il processo di configuration management vada eliminato. Piuttosto va riconosciuto e promosso nel modo più corretto e più funzionali alle reali esigenze di chi offre servizi e delle diverse funzioni coinvolte (ciascuna con le sue diverse esigenze).

Da questo argomento ne viene fuori un altro: spesso, chi applica ITIL o altri standard parla di "processo" unico, quando invece lo stesso processo deve essere istanziato in più parti. Per esempio, il change management di un mainframe non può essere lo stesso del change management di un sistema Windows (per non parlare poi del fatto che il loro responsabile deve essere diverso). Così il configuration management degli asset personali deve essere gestito con strumenti e da persone diverse del configuration management della rete o dei server.

****

05- ITIL: Registro dei certificati ITIL

E' attivo il registro delle persone certificate ITIL (da notizia del gruppo EXIN Certified Professionals di LinkedIn:
- http://www.itil-officialsite.com/candidate-register/candidate-register.aspx

****

06- Tecnologia per la sicurezza: Blackphone

Ormai in molti ne parlano: il cellulare a prova di privacy. Il blackphone si basa su Android e utilizza un insieme di apps per la sicurezza, per navigare senza essere tracciati, eccetera:
- http://arstechnica.com/security/2014/06/exclusive-a-review-of-the-blackphone-the-android-for-the-paranoid/

Al momento li hanno esauriti (cosa "solo" 630 Euro):
- https://store.blackphone.ch/

Tutto molto interessante, se solo non avete già dato tutti i vostri dati a Google o Apple o Microsoft. Difficile...

****

07- Cloud Service Level Agreement Standardisation Guidelines

La Commissione Europea ha pubblicato le "Cloud Service Level Agreement Standardisation Guidelines" (ringrazio Giacomo Orlando della segnalazione):
- http://europa.eu/rapid/press-release_IP-14-743_en.htm
- https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines

Il documento è interessante. Ma continuo a pensare che ci siano troppe linee guida per la gestione dei fornitori cloud, mentre per i fornitori di servizi informatici non cloud non c'è quasi nulla, sebbene loro gestione lasci spesso a desiderare. Tra l'altro, nel documento non ho trovato alcun requisito non applicabile a fornitori di servizi IT non cloud.

Quindi mi piacerebbe vedere almeno una linea guida una sulla gestione in generale dei fornitori dei servizi IT (per cui prevedere anche qualche requisito in più di quelli che ci sono nel documento).

****

08- Minacce e attacchi: Attacco a Code Spaces

Il 17 giugno è stato attaccato il servizio Code Spaces, che è rimasto indisponibile per molti giorni (oggi, 16 giugno, il servizio è ancora indisponibile). Code Spaces offre un servizio cloud di configuration management per i codici sorgenti e si basa sull'infrastruttura (sempre cloud) di Amazon.

Pare che un attaccante abbia iniziato con un DDoS e abbia anche sfruttato delle credenziali di accesso alla rete interna di Code Spaces ottenute con del phishing. Obiettivo: chiedere un riscatto per sospendere l'attacco.

Gli analisti hanno subito cominciato a dibattere sul fatto che l'accesso ai pannelli di amministrazione del servizio Code Spaces poteva essere prevenuto se si fosse basato su un'autenticazione a multi-fattori (o con one-time-password; insomma, come quando bisogna usare una password temporanea che viene inviata via SMS o e-mail).

Non solo questo, però, va considerato. Ma anche: la mancanza di un business continuity plan, l'errore di un utente che ha risposto ad un'email fraudolenta e non se ne è accorto neanche in un secondo momento (o forse non ha avvisato nessuno), il fatto che questo utente (mia deduzione) abbia usato una

password con molti privilegi per un sito che può essere oggetto di phishing. Tutte cose, tra l'altro, non solo applicabili al cloud.

La notizia l'ho ricevuta dal SANS NewsBites che a sua volta segnala questa pagina web:
- http://searchsecurity.techtarget.com/news/2240224102/Multifactor-authentication-key-to-cloud-security-success

****

09- Minacce e attacchi: Wind e Exchange

In giugno due notizie di interruzione di servizi si sono imposte. La prima è il "blackout di Wind": l'operatore di telecomunicazioni ha avuto un problema di "configurazione dei router" che ha bloccato la connettività dei suoi utenti per diverse ore:
- http://www.tomshw.it/cont/news/blackout-wind-sotto-la-lente-dell-agcom/57277/1.html
- http://www.forexinfo.it/Wind-Infostrada-le-cause-del

L'altro caso riguarda il blocco di Office 365: il servizio cloud di Micorosoft è rimasto fermo per 9 ore per un "problema hardware":
- http://www.ictbusiness.it/cont/news/exchange-online-attivo-dopo-nove-ore-di-blocco/32712/1.html

Le due notizie mi sembrano in qualche collegate, anche se non saprei dire esattamente come: forse perché piccoli errori hanno messo in difficoltà tantissime persone, forse perché si dimostra quanto siamo dipendenti da servizi con SLA non perfettamente garantiti, forse perché le mitiche grandi imprese fanno anche loro degli errori.

****

10- Minacce e attacchi: Report sulla qualità del codice di Coverity

Stefano Ramacciotti mi ha segnalato questo interessante report sulla qualità del codice:
- http://softwareintegrity.coverity.com/register-for-scan-report-2013.html

Lo trovo interessante perché presenta un elenco dei tipi di difetti riscontrati nelle analisi effettuate su sorgenti C/C++ e Java. In C/C++ il più alto numero di errori rientra nei tipi "Resource leaks", "Null pointer dereferences" e "Control flow issues", mentre in Java gli errori più comuni riguardano "Null pointer dereferences", "Dodgy code" e "FindBugs: Performance".

Quello che mi chiedo è: quanti sviluppatori Java usano strumenti di analisi come FindBugs (http://findbugs.sourceforge.net/)? Quanti sviluppatori usano altri strumenti?

Ho paura della risposta...

****

11- Le assicurazioni relative agli incidenti IT sono un pasticcio

Articolo segnalato da Crypto-Gram dal titolo " The $10 Million Deductible: Why the cyberinsurance industry is a mess":

- http://www.slate.com/articles/technology/future_tense/2014/06/target_breach_cyberinsurance_is_a_mess.html

Continuo quindi la mia piccola campagna di sensibilizzazione: se neanche le assicurazioni sanno quantificare i rischi, perché ostinarsi a voler realizzare valutazioni del rischio quantitative? Per non parlare di quelle semi-quantitative (un ossimoro)?

****

12- Pianificare data center

Interessante questo articolo di ZeroUno:
- http://www.zerounoweb.it/osservatori/data-center-management/pianificare-il-data-center-un-metodo-per-evitare-errori.html

Alcuni dei 9 errori di pianificazione di un data center sono:
1- sottovalutazione dei costi operativi (da aggiungere a quelli di realizzazione iniziale);
2- stima imprecisa dei costi di realizzazione;
3- sovradimensionamento;
4- pianificazione prematura dello spazio;
5- non pensare ai possibili ampliamenti futuri;
6- progetti troppo complicati.

Viene da pensare che questi errori, con le dovute specificità, siano comuni a tanti progetti, non necessariamente di data center.