Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – GENNAIO 2016

****

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- OWASP Top 10 Proactive Controls 2016 (e il Joel Test)

L'OWASP ha pubblicato la OWASP Top 10 Proactive Controls 2016:
- https://www.owasp.org/index.php/OWASP_Proactive_Controls.

Questa notizia mi è stata riferita dalla Newsletter d'information de HSC <newsletter@hsc-news.com>.

L'articolo della newsletter, richiama un punto di cui ho già parlato anche io in passato: per la sicurezza delle applicazioni web, purtroppo il riferimento è la OWASP Top 10, ossia la lista delle 10 vulnerabilità più diffuse delle applicazioni web, che però rappresentano l'inverso del problema:
- https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

Ringrazio quindi OWASP per aver presentato la nuova lista.

L'articolo della newsletter, richiama anche la lista di buone pratiche di Joel Spolsky:
- http://www.joelonsoftware.com/articles/fog0000000043.html.

L'ho letta con dolore, pensando a quante volte non ho visto applicati i 12 punti:
- usare un sistema di controllo dei file;
- fare in modo che le build siano prodotte in un solo passaggio;
- fare build almeno ogni giorno;
- usare un sistema di ticketing per tracciare i bug;
- correggere i bug prima di scrivere nuovo codice;
- mantenere un piano di lavoro;
- scrivere le specifiche;
- assicurare ai programmatori un ambiente di lavoro tranquillo;
- fornire ai programmatori gli strumenti migliori;
- avere dei tester;
- in fase di selezione del personale, far scrivere del codice ai programmatori;
- chiedere all'"uomo della strada" di fare dei test di usabilità.

Per ciascun punto è fornita una spiegazione molto utile.

La lista è del 2000 e forse qualche voce potrebbe essere aggiornata. Ciò non toglie che dovrebbe essere studiata e applicata con attenzione.

****

02- Top 10 dei rischi legati alle tecnologie sanitarie per il 2016

Marco Fabbrini mi ha segnalato il documento "Top 10 Health Technology Hazards for 2016" (bisogna registrarsi):
- https://www.ecri.org/Pages/2016-Hazards.aspx.

Marco segnala soprattutto due rischi legati alla sicurezza IT: errate configurazioni e uso improprio delle porte USB.

Interessante osservare che, malgrado i siti dedicati alla sicurezza IT segnalano i rischi di intrusione informatica e la diffusione di dati personali, questo report non li considera. Infatti qui l'attenzione è posta sulla salute fisica dei pazienti.

****

03- Vulnerabilità firewall Juniper

È stata trovata una backdoor nei firewall Juniper (notizia dal Sans NewsBites). Sono già disponibili degli exploit per sfruttarla. Il primo articolo è più tecnico:
- https://community.rapid7.com/community/infosec/blog/2015/12/20/cve-2015-7755-juniper-screenos-authentication-backdoor;
- http://arstechnica.com/security/2015/12/researchers-confirm-backdoor-password-in-juniper-firewall-code/.

Una prima considerazione riguarda i produttori di firewall: evidentemente non fanno un riesame del codice (code review) prima di immettere sul mercato i loro prodotti. Ho letto una notizia secondo la quale CISCO ha intenzione di avviare un programma di code review; questo vuol dire che neanche loro la facevano!

Una seconda considerazione riguarda tutti noi, utilizzatori di questi prodotti. Evidentemente non possiamo rinunciare ai firewall, né possiamo essere sicuri della loro efficacia.

Sembra quindi che abbiano ragione coloro che promuovono l'uso di più firewall diversi in serie per assicurare la "difesa in profondità". Chi critica questo approccio fa notare che più tipi di firewall necessitano un numero maggiore di competenze, rendono meno efficiente la loro gestione e aumentano le vulnerabilità potenziali. Certamente, questi discorsi sono molto interessanti per le aziende medio-grandi, ma non per le piccole, che al massimo hanno una sola persona addetta alla gestione dei sistemi informatici.

****

04- Regolamento europeo privacy - Q&A della Commissione europea

Per chi fosse interessato a qualche informazione veloce in merito al quasi futuro Regolamento europeo sulla privacy, segnalo questa pagina (in inglese) della Commissione europea stessa:
- http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm.

****

05- Garante Privacy: email ex dipendente deve essere chiusa

Segnalo questo articolo di Filodiritto (con rimando al Provvedimento del Garante):
- http://www.filodiritto.com/news/2015/e-mail-garante-privacy-email-ex-dipendente-deve-essere-chiusa.html.

Sembrerebbe, ad una prima e veloce lettura, che è necessario informare preventivamente il dipendente per poi essere autorizzati ad accedere alla sua email in caso di uscita.

Leggendo il Provvedimento, al punto 2.4 sembra però che la pratica di inoltrare ad altra persona le email indirizzate ad un ex-dipendente sia illegittima in tutti i casi. Osservo che sono in molti ad attuarla, ma evidentemente devono adottare un'altra soluzione (la più semplice consiste nell'avvisare il mittente di inviare nuovamente l'email ad altro dipendente).

****

06- Normativa firme elettroniche

Luciano Quartone mi ha segnalato una sua presentazione "per illustrare la situazione attuale della normativa italiana in merito alle firme elettroniche e le principali differenze rispetto le novità che verranno con il Regolamento eIDAS".

Visto che l'argomento, per chi non ha seguito con estrema attenzione tutte le puntate, è complesso, mi pare utile segnalarla:
- http://www.lucianoquartarone.it/wp/?p=661.

Importanti saranno le modifiche che dovrebbero essere apportate al Codice dell'amministrazione digitale (CAD, Dlgs. 82 del 2005). A questo proposito, Anorc (Twitter @_ANORC) ha segnalato questo articolo dal titolo "Che resterà del CAD dopo la riforma?":
- http://www.agendadigitale.eu/identita-digitale/che-restera-del-cad-dopo-la-riforma-ecco-tutte-le-modifiche-necessarie_1885.htm.

Sempre da Anorc, segnalo la pubblicazione del D.P.C.M. del 6 novembre 2015, recante la disciplina della firma digitale dei documenti classificati:
http://anorc.it/notizia/745_Le_nuove_regole_tecniche_per_la_sottoscrizione_digitale_dei_documenti_infor.html.

L'atto lo si trova al seguente link:
- www.gazzettaufficiale.it/eli/id/2015/12/05/15A08534/sg.

****

07- Novità SPID

AgID ha comunicato i primi accreditamenti dei primi gestori di identità digitale:
- http://www.agid.gov.it/notizie/2015/12/19/spid-accreditati-i-primi-gestori-identita-digitale.

Da un tweet di @martinapennisi, segnalo questo articolo del Corriere della Sera con qualche elemento in più:
- http://www.corriere.it/tecnologia/economia-digitale/15_dicembre_18/agid-identita-digitale-identity-provider-accreditamento-spid-fe552daa-a5c9-11e5-a238-fd021b6faac8.shtml.

Franco Ferrari di DNV GL mi ha anche segnalato questo articolo dal titolo "Spid, fare in fretta. Ma attenzione a privacy e sicurezza" che propone alcune riflessioni in merito:
- http://www.corrierecomunicazioni.it/pa-digitale/38806_spid-fare-in-fretta-ma-attenzione-a-privacy-e-sicurezza.htm.

****

08- ISO/IEC TR 20000-11: relazioni tra ISO/IEC 20000-1 e ITIL

Franco Ferrari di DNV GL mi ha segnalato la pubblicazione della ISO/IEC TR 20000-11:2015 dal titolo "Guidance on the relationship between ISO/IEC 20000-1:2011 and service management frameworks: ITIL®":
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62151.

Il testo di accompagnamento è molto scarno (6 pagine con anche immagini e tabelle riassuntive) e non dice nulla di nuovo a chi conosce già la ISO/IEC 20000-1 e ITIL (può però far ridere la pretesa di dire che non sono basate l'una sull'altra ma hanno solo qualche elemento in comune).

Il resto del documento è costituito da aride tabelle di correlazione e confronti tra le definizioni usate.

****