Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – DICEMBRE 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

****

****

00- Editoriale e Buone feste

Questa volta non sommergo i miei lettori sulle mie elucubrazioni (anche se ne avrei alcune...). Visto che le feste si avvicinano, vi auguro Buone feste e basta.

****

00- VERA 4.3

A chi piacciono certi regali di Natale, ho pubblicato la nuova versione di VERA. La trovate in questa pagina:
- http://www.cesaregallotti.it/Pubblicazioni.html.

****

01- Pubblicata la ISO/IEC 27011 per le TLC

È stata pubblicata la seconda edizione del 2016 della norma ISO/IEC 27011 dal titolo "Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations":
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=64143.

Si tratta di una raccolta di controlli di sicurezza, da aggiungere a quelli della ISO/IEC 27002, per gli operatori di telecomunicazioni..

****

02- Pubblicata la 27035 sulla gestione degli incidenti

Sono state pubblicate le nuove norme ISO/IEC 27035 e ne è stata quindi cancellata la versione del 2011.

La nuova ISO/IEC 27035 è divisa in due parti. La prima ha titolo "Principles of incident management":
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=60803.

La seconda parte ha titolo "Guidelines to plan and prepare for incident response" (di 145 pagine, ossia molto lunga):
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62071.

Trovo interessante l'appendice C, che propone un esempio di categorizzazione degli incidenti, per gravità e ambito. Non credo sia un esempio ottimale, ma almeno c'è.

****

03- Pubblicata ISO/IEC 27050 sull'electronic discovery

È stata pubblicata da poco la ISO/IEC 27050-1 "Electronic discovery -- Part 1: Overview and concepts":
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63081.

Le parti 2 (Guidance for governance and management of electronic discovery) e 3 (Code of Practice for electronic discovery) sono ancora in bozza.

****

04- ISO 9002 - Linea guida per la ISO 9001

È stata pubblicata la ISO/TS 9002:2016 dal titolo "Guidelines for the application of ISO 9001:2015":
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=66204.

Mi è stata segnalata in una conversazione tra auditor DNV GL. Il commento che ha accompagnato la notizia è stato "I contenuti non sono proprio rivoluzionari, ma vale la pena leggerla". Condivido.

****

05- Parlamento EU e sicurezza nel settore energia

Fabio Teoldi mi ha segnalato quanto segue: il Parlamento Europeo recentemente ha pubblicato il Rapporto "Cyber Security Strategy for the Energy Sector", scaricabile dal sito dello European Parliament Think Tank:
- http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2016)587333.

Non si tratta di uno studio con consigli per gli operatori, ma rappresenta una base di partenza per approfondire la materia.

****

06- Elenco dispositivi per la firma elettronica qualificata

Mi segnala Franco Ferrari di DNV GL questo articolo di Andrea Caccia dal titolo "Elenco dei dispositivi certificati per la firma elettronica qualificata (firma digitale)":
- https://www.linkedin.com/pulse/elenco-dei-dispositivi-certificati-per-la-firma-digitale-caccia.

Grazie a tutti e due.

****

07- Vulnerabilità nel protocollo NTP

Il protocollo NTP è quello che consente di sincronizzare gli orologi di pc e server in modo che abbiano tutti lo stesso orario (perché è divertente vedere l'orologio di John Belushi in Animal House, ma non averlo nella realtà). Normalmente i sistemi operativi hanno installato un codice open source e freeware con il nome ntpd e realizzato da un gruppo di persone dal nome NTP.org.

Intorno a giugno 2016 hanno scoperto numerose vulnerabilità nel ntpd, con impatto soprattutto sui sistemi operativi Windows.

E a quel punto si scopre che questa storia l'abbiamo già sentita, anche se con protagonisti diversi. Allora il protagonista principale era OpenSSL, ma la storia è ancora quella: si scopre che un protocollo importantissimo e diffusissimo è mantenuto da pochissime persone che non ricevono neanche un supporto economico sufficiente per continuare a lavorarci.

Non commento oltre perché queste storie sono sconfortanti. Ringrazio quindi Marco Fabbrini per avermi segnalato questo articolo:
- http://www.infoworld.com/article/3144546/security/time-is-running-out-for-ntp.html.

E non disperate. Alla fine sono riusciti a riparare le vulnerabilità (dal SANS NewsBites):
- http://www.theregister.co.uk/2016/11/23/ntp_patch_time_rolls_around_again/.

****

08- Cybersecurity Playbook

Confesso che tutte e due i termini del titolo della pubblicazione "Cybersecurity Playbook" mi innervosiscono. Però, essendo scritta da Pete Herzog, mi sono sforzato di darle un'occhiata. Si tratta di 27 pagine di raccomandazioni di sicurezza informatica, sintetiche, chiare e ben scritte.

Alcune misure sono anche originali rispetto alle tante pubblicazioni che ci sono in giro.

Ne consiglio la lettura:
- https://www.barkly.com/comprehensive-it-security-plan.

****

09- NIST Systems Security Engineering

Il NIST ha pubblicato la NIST Special Publication 800-160 dal titolo "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems":
- http://csrc.nist.gov/publications/PubsSPs.html#800-160.

Un malloppo di 257 pagine. L'ho sfogliato e mi sembra un po' troppo teorico. Ho trovato più interessante l'Appendice G del corpo del documento.

****

10- Mio errato riferimento al GDPR

Nell post su PIA e valutazione del rischio in ambito privacy (http://blog.cesaregallotti.it/2016/10/privacy-pia-e-valutazione-del-rischio_28.html) ho fatto un errore: ho indicato che il GDPR (il Regolamento europeo sulla privacy) ha come riferimenti "Regolamento 169/2016", mentre si tratta del 679/2016.

Il post ora è corretto.

Ringrazio Agostino Oliveri (di Sicurdata) e Andrea Praitano (di Business-e) per avermi corretto.

Andrea, poi, in ambito PIA, ricorda che il CNIL francese ha pubblicato dei documenti ben fatti su questo argomento (io li avevo segnalati a suo tempo, ma un promemoria non guasta):
https://www.cnil.fr/en/privacy-impact-assessments-cnil-publishes-its-pia-manual.

****

11- Privacy a scuola (opuscolo del Garante)

Il Garante privacy ha pubblicato un opuscolo dal titolo "La scuola a prova di privacy":
http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/5601934.

È soprattutto indirizzato a chi opera nella scuola, ma può essere utile a tutti.

****

12- Privacy shield approvato dal Garante

Dalla newsletter del Garante (e una gentile segnalazione di Ivo Trotti di TNS Italia, che ringrazio), segnalo che il Garante privacy italiano ha autorizzato il trasferimento dei dati personali negli USA alle organizzazioni che aderiscono al Privacy shield.

Non ripercorro la storia del Safe Harbor e del Privacy Shield. Ecco quindi la decisione del Garante:
- http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/5652873.

Ovviamente non troverete alcun link alla lista delle organizzazioni che hanno aderito al privacy shield. Sarebbe troppo facile. Però una semplice ricerca sul web fornisce il link:
- https://www.privacyshield.gov/list.

Non ho studiato il Privacy shield framework, ma capisco che un'azienda USA può aderire per dati HR (cioè per trattare i dati del personale dipendente) e/o dati non-HR.

****

13- Dare più privacy per migliori prestazioni

Non so quanto questo articolo (segnalato da Crypto-gram di novembre) dal titolo "Want People to Behave Better? Give Them More Privacy" riguardi effettivamente la sicurezza delle informazioni e la normativa sulla privacy, però mi sembra comunque interessante:
- https://www.psychologytoday.com/blog/the-outsourced-mind/201604/want-people-behave-better-give-them-more-privacy.

In sintesi: se i datori di lavoro e i manager controllano di meno i lavoratori, questi tendono ad auto-organizzarsi in modo più efficiente e lavorare con miglliori prestazioni.

Credo che ciò sia degno di riflessione. Certamente bisogna bilanciare le esigenze di controllo (necessarie) con quelle di auto-gestione e responsabilizzazione delle persone.

****

14- Cloud Adoption & Risk Report Q4 2016

Marco Fabbrini mi ha segnalato il report "Cloud Adoption & Risk Report Q4 2016" della Skyhigh (neanche sapevo che esistesse questa azienda). Il rapporto è presentato da un interessante articolo dal titolo "Cloud use could be putting businesses at risk":
- http://betanews.com/2016/11/17/cloud-use-business-risk/.

È breve e dice cose già note, che però è bene non dimenticare. Per esempio il fatto che le clausole contrattuali sono spesso negative per i clienti: il 69,7% non specifica di chi è la proprietà dei dati, solo l'8,7% assicura di non trasferire i dati a terze parti (qui però bisognerebbe capire le eccezioni), solo il 16% si impegna a cancellare i dati in caso di chiusura del contratto.

L'articolo si conclude ricordando che i siti di conversione di documenti da/a pdf, sebbene spesso ritenuti innocui, sono spesso usati per convertire dati molto critici, ma questi siti hanno clausole di garanzia per i clienti molto deboli (e quindi dovremmo chiederci cosa ci guadagnano offrendo il servizio di conversione).

I più interessati possono scaricarsi il rapporto completo dal titolo :
- https://www.skyhighnetworks.com/cloud-computing-trends-2016/.

Io mi sono solo letto l'estratto presentato nella pagina web e l'ho trovato molto interessante.

****

15- Segnalazione di copia slide

Settimana scorsa avevo segnalato delle slide su privacy e sanità:
- http://blog.cesaregallotti.it/2016/11/dati-e-sanita.html.

Paola Generali GetSolution mi ha segnalato che le slide da 52 a 105 sono copiate da sue slide già presentate in varie occasioni allo SMAU e dedicate al nuovo GDPR:
- http://www.smau.it/speakers/paola.generali/.

Mi spiace essere stato implicato in una faccenda così e spero sia chiaro a tutti che non approvo in alcun modo il copia-incolla di materiale altrui, anche se liberamente disponibile. Certamente si può cogliere ispirazione per alcune cose (sennò dovremmo iniziare sempre da zero e non ci evolveremmo), però penso che chi diffonde conoscenza debba essere capace di elaborarla autonomamente.