Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – APRILE 2017
****

Newsletter mensile con novità in materia di sicurezza delle informazioni, IT Service Management, Qualità.
E' possibile dare il proprio contributo e diffonderla a chiunque.

IT Service Management News di Cesare Gallotti è rilasciata sotto licenza Creative Commons Attribution 4.0 International License (creativecommons.org/licenses/by/4.0/deed.en_GB). Bisogna attribuire il lavoro a Cesare Gallotti con link a http://www.cesaregallotti.it/Newsletter.html.

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- Mailing list: scuse e richiesta di consiglio

Sono arrivato ad avere circa 700 iscritti alla mailing list. Altri hanno più seguito (iscritti, follower, contatti e amici), ma si tratta di un bel numero, considerando gli argomenti specialistici trattati.

Il mio SMTP però da dicembre blocca gli invii a più di 50 persone. Alcuni hanno ricevuto più copie della newsletter perché cercavo di capire e risolvere il problema. La soluzione tampone (o workaround) non è agevolissima e richiede pazienza.

Purtroppo poi ho avuto dei problemi al mio pc ho potuto recuperare solo la mailing list aggiornata a dicembre. Ho recuperato poi le richieste di iscrizione, ma anche questa volta alcuni riceveranno più volte la stessa newsletter. Di questo mi scuso.

Vi chiedo quindi se avete dei consigli da darmi. Vorrei evitare l'uso di servizi made in USA come Mailchimps o Google Groups perché i noti problemi di privacy. Soluzioni europee come MailUp costano e io dalla newsletter non ci guadagno quasi niente (non ho mai voluto presentare offerte economiche da "super-consulente").

Vi ringrazio anticipatamente per l'aiuto.

****

02- Rapporto Clusit 2017

Segnalo che è disponibile il Rapporto Clusit 2017 sulla sicurezza ICT in Italia, la pubblicazione di riferimento in materia:
https://clusit.it/rapporto-clusit/.

****

03- Linee guida WP Art. 29 (DPO, DPIA e altre)

Pierfrancesco Maistrello mi ha segnalato che il WP Art. 29 ha pubblicato, il 5 aprile, una nuova linea guida e la revisione di linee guida già pubblicate. Si trovano qui:
http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

Ricordo che il WP Art. 29 sarà, da maggio 2018, un comitato dei Garanti europei, quindi le sue indicazioni sono molto importanti.

La nuova linea guida è quella relativa al Privacy impact assessment (DPIA). Non sembra riportare elementi particolarmente innovativi, per lo meno per chi ha già avuto modo di riflettere su questo tema. Pierfrancesco Maistrello mi segnala però quanto è importante l'Annex 2, che riporta i "Criteria for an acceptable DPIA".

Tra le linee guida aggiornate, ha particolare rilevanza quella sul DPO. Pierfrancesco Maistrello me ne fa un riassunto: "Le modifiche sono poche e quelle più importanti sono: maggior numero di esempi di quando è necessario prevedere un DPO; un intero paragrafo relativo al DPO condiviso tra più organizzazioni".

Altre due linee guida aggiornate: sull'interoperabilità e sull'identificazione dell'autorità garante.

****

04- Servizi aziendali sul web e sicurezza

Nell'ultima newsletter HSC, ho trovato un editoriale di Hervé Schauer che tratta di un argomento che spesso mi ha fatto pensare. Ossia: se un'azienda fornisce accesso via web a email e server aziendali, automaticamente accetta che il personale acceda ai dati aziendali su dispositivi personali e possa scaricarli.

Io segnalo questo articolo perché in realtà vedo troppi miei interlocutori sorpresi dal pensiero che, sì, in effetti, permettere gli accessi via web implica permettere gli accessi da qualsiasi tipo di dispositivo anche personale.

Hervé Schauer segnala la funzionalità di accesso condizionale offerta da Office 365 e ricorda che così facendo si riduce un rischio, ma si accetta che sia Microsoft a gestire la propria Active Directory.

Ecco quindi che ho scoperto che ci sono soluzioni per ridurre il rischio degli accessi dal web alle risorse aziendali (così alcuni miei interlocutori si sorprenderanno ancora di più).

La Newsletter HSC: http://www.hsc-news.com/archives/2017/000143.html.

L'articolo di Microsoft sull'accesso condizionale:
https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access.

Nota finale: mi pare di capire che questa funzionalità sia stata introdotta meno di un anno fa, quindi forse non sono stato troppo disattento; è anche vero che sul web si evidenziano troppo gli articoli inutili sulla "cybersecurity" e troppo poco quelli veramente importanti per la sicurezza delle informazioni.

****

05- Misure minime per la PA

A ottobre 2016 avevo segnalato la pubblicazione delle "Misure minime di AgID per la PA" (con anche le mie critiche):
http://blog.cesaregallotti.it/2016/10/misure-minime-di-agid-per-la-pa.html.

Il 17 marzo 2017 AgID ha comunicato ufficialmente alle PA il dovere di predisporre una relazione, entro il 31 dicembre, sullo stato di attuazione delle medesime.

La circolare 1/2017 di AgID sulla Gazzetta ufficiale (Permalink):
www.gazzettaufficiale.it/eli/id/2017/04/04/17A02399/sg.

Il comunicato stampa di AgID:
http://www.agid.gov.it/notizie/2017/04/07/pubblicate-gazzetta-ufficiale-misure-minime-sicurezza-informatica-pa.

Ringrazio Franco Ferrari di DNV GL e Daniela Quetti per questa segnalazione.