Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – LUGLIO 2019

****

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.

La newsletter è inviata via MailUp, offerta da Team Quality S.r.l.

Per iscriversi, cancellarsi e leggere l'informativa privacy: http://www.cesaregallotti.it/Newsletter.html.

Sulla stessa pagina è possibile consultare l'informativa sul trattamento dei dati personali.

****

Indice

****

00- Editoriale estivo

Anche questo numero di luglio esce un po' più tardi del solito (io spero sempre di inviare la newsletter il 15 del mese, ma non ce la faccio quasi mai).

Anche questo agosto la newsletter se ne starà in vacanza e spero che anche il prossimo settembre la newsletter riprenderà ad uscire (ir)regolare come sempre.

Ringrazio i miei lettori "consolidati" perché continuano a leggermi e quelli nuovi per la fiducia che mi hanno dato.

Auguro a tutti un buon agosto, qualsiasi cosa facciate.

Grazie!

Cesare

****

01- Raccomandazione UE sulla cibersicurezza nel settore dell'energia

Segnalo questo articolo dal titolo "Cybersecurity nel settore energetico, ecco le raccomandazioni della Commissione europea":
- https://www.agendadigitale.eu/infrastrutture/cybersecurity-nel-settore-energetico-ecco-le-raccomandazioni-della-commissione-europea/.

Mi sembra interessante osservare che questa "Raccomandazione UE 2019/553 della Commissione del 3 aprile 2019 sulla cibersicurezza nel settore dell'energia" presenta indicazioni che potrebbero essere considerate anche in altri settori e nell'ambito industriale più generale.

Il link dell'articolo riporta alla raccomandazione in italiano. La pagina con le versioni nelle altre lingue dell'Unione è questa:
- https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32019H0553.

****

02- Tecnologia: NIST NISTIR 8228 su IoT

Il NIST ha pubblicato il documento NISTIR 8228 dal titolo "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks":
- https://csrc.nist.gov/publications/detail/nistir/8228/final.

Tratta dell'IoT in modo generale, senza approfondire i campi di applicazione (industriale, automobili, sanità, eccetera).

A mio pare è più interessante la parte analitica sui rischi, mentre le misure di sicurezza sono espresse in modo troppo generale e approfondimenti li avrei graditi.

****

03- Tecnologia: Strumenti per la sicurezza applicativa

Credo che gli strumenti per la sicurezza delle applicazioni software siano tra i meno considerati, anche se oggi sempre più necessari.

Tutto ha un'origine storica: inizialmente la sicurezza era solo una questione di infrastruttura informatica, non delle applicazioni. Per quanto oggi tutti siano consapevoli che non è più così (e da tempo) c'è ancora carenza di reale competenza, anche sugli strumenti che si possono utilizzare. Come consulente e auditor chiedo sempre se sono usati strumenti per il controllo del software: quasi mai sono usati strumenti per il controllo della sicurezza, qualche volta sono usati quelli per il controllo della qualità e spesso non è usato niente (anzi... sono guardato con sorpresa).

Non mi proclamo esperto e quindi non so giudicarlo appieno, ma segnalo questo articolo dal titolo "10 Hottest DevSecOps Tools You Need To Know About":
- https://www.crn.com/slide-shows/security/10-hottest-devsecops-tools-you-need-to-know-about/1.

Dovrebbe essere utile almeno come punto di partenza.

****
04- Tecnologia: Sistemi operativi per smartphone

Una cosa che mi preoccupa è la massa di dati che sto dando a Google. Sono già migrato a Qwant come motore di ricerca e ora sto cominciando ad usare il loro sistema di mappe (e non abbandono il mio vecchio TomTom).

Per quanto riguarda il cellulare potrei passare ad Apple, ma non sopporto la chiusura dell'iOS. Per Android sono incuriosito dai progetti di sistemi alternativi.

Uno l'ho visto segnalato da Luca Bonesini (mio collega di tanti anni fa). Si tratta del progetto /e/:
- https://e.foundation/.

Un altro progetto l'ho visto più di recente ed è il PostmarketOS:
- https://postmarketos.org/blog/2019/06/23/two-years/.

Dovrei studiare meglio la questione e, soprattutto, aspettare che gli smartphone di casa siano abbastanza obsoleti per fare qualche test. Per intanto mi appunto la questione.

****
05- Minacce e attacchi: errore in un'applicazione di 7-Eleven

E' noto che non mi interesso molto delle notizie sugli attacchi, in quanto solitamente non riportano informazioni utili, ma solo generiche.

Questo articolo non è tanto migliore, ma ci ricorda che bisogna prestare molta attenzione anche alle applicazioni per dispositivi mobili:
- https://www.zdnet.com/article/7-eleven-japanese-customers-lose-500000-due-to-mobile-app-flaw/.

In poche parole: il 7-Eleven giapponese ha commissionato un'applicazione che permetteva i pagamenti veloci. Questa permetteva anche di richiedere l'azzeramento della password, e la sua conseguente

modifica, senza verificare che il richiedente fosse l'utente titolare dell'account. Il risultato è che degli attaccanti hanno azzerato la password di alcuni clienti e hanno fatto acquisti con i loro soldi.

****

06- Privacy: Sanzioni GDPR (Google, Facebook, Marriott e BA) e riflessioni

In questi tempi si moltiplicano le notizie sulle sanzioni milionarie a seguito di violazioni di dati personali.

Google è stata multata per mancanza di trasparenza:
- https://www.bbc.com/news/technology-46944696;
- https://www.agendadigitale.eu/sicurezza/google-e-facebook-con-la-privacy-non-si-scherza-piu-le-prime-avvisaglie-in-europa-e-usa.

E infine Facebook per diverse violazioni:
https://arstechnica.com/tech-policy/2019/07/facebooks-ftc-fine-will-be-5-billion-or-one-months-worth-of-revenue/.

Non ne ho parlato perché in definitiva non aggiungono niente di nuovo sulle "cose da fare".

Mi hanno invece incuriosito molto le vicende della Marriott e della British Airways, ambedue sottoposte a multe miliardarie dall'ICO, ossia il Garante UK.

Un articolo sulla multa alla catena di hotel Marriott:
- http://www.ictbusiness.it/cont/news/nuova-vittima-del-gdpr-maxi-multa-anche-per-marriott-international/43277/1.html.

L'annuncio dell'EDPB sulla multa alla Marriott:
- https://edpb.europa.eu/news/national-news/2019/ico-statement-intention-fine-marriott-international-inc-more-ps99-million_en.

Su questa c'è anche un articolo più tecnico sull'attacco alla Marriott:
- https://www.zdnet.com/article/marriott-ceo-shares-post-mortem-on-last-years-hack/.

Mi pare che quelli della Marriott abbiano dimostrato molta attenzione sulla vicenda e che siano stati loro stessi a renderla pubblica. In altre parole, non mi pare che la multa sia giustificata.

Anzi: quelli della Marriott usavano una tecnologia (IBM Guardium) dedicata a lanciare allarmi relativi a "strane" query sui database. IBM sarà contenta della pubblicità gratuita, ma mi pare interessante sapere che esistono queste tecnologie (temo però che al momento siano molto costose e difficili da mantenere).

Dall'altra parte, l'ICO non si è preoccupata di rilevare gli investimenti fatti da Marriott e il livello di prevenzione adottato, ma, più o meno, ha detto: "poiché avete avuto un incidente, vuol dire che avete sbagliato e quindi dovete pagare". Non mi pare sia questo lo spirito del GDPR. Mi pare piuttosto sia di verificare se l'azienda ha fatto quanto possibile per evitare gli incidenti.

Caso simile è quello della British Airways. Qui il comunicato dell'EDPB sulla multa comminata dall'ICO:
- https://edpb.europa.eu/news/national-news/2019/ico-statement-intention-fine-british-airways-ps18339m-under-gdpr-data-breach_en.

Qui invece un articolo più tecnico che, in sostanza, dice che sarebbe stato molto ma molto difficile identificare l'attacco (sfortunatamente non spiega come prevenirlo in futuro):
- https://www.riskiq.com/blog/labs/magecart-british-airways-breach/.

****

07- Privacy: Codice di condotta sulle valutazioni commerciali

Il Garante ha approvato il "Codice di condotta per il trattamento dei dati personali in materia di informazioni commerciali", ossia il codice che riguarda le aziende che analizzano le caratteristiche delle aziende per elaborare valutazioni a scopo commerciale:
- https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9119868.

Ho riscritto la definizione di "attività di informazione commerciale", sperando di essere stato chiaro. Ad ogni modo, è possibile usare la definizione "ufficiale". Inizialmente, erroneamente, pensavo si trattasse dei contact centre. La lettura mi ha smentito.

I codici di condotta sono regolati dall'articolo 40 del GDPR. Interessante (come anche da comunicato stampa del Garante) è il ruolo dell'Organismo di monitoraggio (OdM), previsto dall'articolo 41 del GDPR, che dovrà essere valutato in senso all'EDPB.

Ho avuto modo di rileggere il GDPR su queste cose e mi è sembrato strano il meccanismo degli OdM (unici per ciascun codice di condotta), molto differente da quello relativo agli organismi di certificazione (che sono in concorrenza tra loro e controllati da Accredia). Ci sarebbe materia per riflettere.

Per finire, visto che potrei aver scritto sciocchezze (vi prego di segnalarmele), invito a leggere direttamente la newsletter del Garante:
- https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9120035

****

08- Privacy: Mio articolo su fornitori e GDPR

Segnalo questo mio articolo dal titolo "Fornitori, valutazione del rischio e adeguamento privacy: le linee guida":
- https://www.cybersecurity360.it/legal/privacy-dati-personali/fornitori-valutazione-del-rischio-e-adeguamento-privacy-le-linee-guida/.

Ho proposto un metodo semplice per affrontare la questione dei fornitori in relazione al GDPR e una critica all'uso dei questionari purtroppo sempre più diffusi.

****

09- Privacy: Mia intervista su ISO/IEC 27552

Elia Barbujani mi ha intervistato per Web radio ius law sulla ISO/IEC 27552:
- https://webradioiuslaw.it/speciale-adeguamento-privacy-iso-iec-27552-cosa-cambia-per-le-certificazioni-privacy/.

Notizia dell'ultima ora: forse la numerazione cambierà in ISO/IEC 27701. Giusto per rendere più semplici le cose...

****

10- Mia presentazione "Come migliorare le proprie competenze"

Il 24 maggio ho tenuto una presentazione per una sessione di studio di AIEA a Milano dal titolo "Come migliorare le proprie competenze".

Le slide sono disponibili anche dal mio sito:
- http://www.cesaregallotti.it/Pubblicazioni.html.

Credo che i soci AIEA possano vedere il video. Gli altri potranno anche farne a meno senza problemi.

****

11- Mia presentazione "Gli standard EN 50600 e ISO/IEC TS 22237 per i data center"

Il 6 giugno ho tenuto una presentazione per un BCI Forum a Milano dal titolo "Gli standard EN 50600 e ISO/IEC TS 22237 per i data center".

Le slide sono disponibili anche dal mio sito:
- http://www.cesaregallotti.it/Pubblicazioni.html.

Su questo avevo già scritto un articolo segnalato due mesi fa.

A questo proposito, poco prima di inviare questa newsletter, mi hanno segnalato questo sulla TIA-942. Ho chiesto al mio lettore se potevo citarlo, ma non mi ha ancora risposto (ma lo ringrazio lo stesso!). Nel caso, riporterò meglio il suo intervento a settembre. Per intanto lo riporto come viene.

<<
Volevo condividere con te una nota sulla certificazione TIA-942 che io in realtà chiamerei “dichiarazione di conformità”, visto che anche per la TIA non esiste un percorso di accreditamento.

EPI si è inventata un “prodotto”: il sito/bollino TIA-942.org che non è un sito ufficiale TIA né TIA riconosce EPI come ente certificatore. La conformità al momento può essere rilasciata da chiunque, ma ovviamente, avendo EPI promosso bene il prodotto tia-942.org il risultato è che tutti finiscono li.
<<

****