Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – LUGLIO 2018

****

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- Breve editoriale

Come ogni fine luglio, ne approfitto per augurare a tutti buone vacanze. Per chi sa di cosa parlo: io sono già "in giro" per un progetto piuttosto importante. Questo però non mi impedisce (per fortuna!) di tenermi aggiornato e continuare con l'impegno preso con questa newsletter.

In questa prima parte del 2018, dopo la sbornia di GDPR, vedo due argomenti che vorrebbero essere "the next big thing", anche se si tratta di cose non recentissime (succede sempre nel nostro campo che la "novità" non è tale): intelligenza artificiale e blockchain. Sembrano la soluzione per tutto. Io preferisco aspettare, ma ogni tanto butto un occhio.

Quindi: buon agosto a tutti, qualsiasi cosa facciate!

La newsletter va in vacanza e tornerà a metà settembre (o un poco dopo).

****

01- Slide del DFA Open Day 2018

Le slide del DFA Open Day 2018 sono state pubblicate sul sito all'indirizzo:
- http://www.perfezionisti.it/open-day/dfa-open-day-2018/.

I temi trattati sono stati i seguenti:
- impatti economici del phishing, malware e social engineering;
- l'apporto della digital forensics al contrasto alla vendita online di sostanze stupefacenti;
- Visione artificiale per riconoscere volti e oggetti nei social media;
- Ediscovery e Artificial Intelligence.

****

02- Nuova ISO 19011:2018, guida per l'audit

Ho ricevuto da molti (incluso il SC 27 WG 1 e Monica Perego) la notizia che è stata pubblicata la nuova versione della ISO 19011 dal titolo "Guidelines for auditing management systems":
- https://www.iso.org/standard/70017.html.

Leggendo l'introduzione, le modifiche rispetto all'edizione del 2011 (la corrispondente edizione italiana era del 2012) sono:
- aggiunta, tra i principi dell'audit, dell'approccio basato sul rischio;
- espansione della guida sulla gestione del programma di audit, includendo i rischi relativi al programma di audit;
- espansione della guida sulla conduzione degli audit, in particolare in materia di pianificazione;
- espansione delle competenze generali degli auditor;
- aggiustamento della terminologia per riflettere il processo e non l'oggetto;
- eliminazione dell'appendice relativa alle competenze per le discipline specifiche (in quanto non più mantenibile, dato il numero delle discipline);
- espansione dell'ulteriore guida in appendice per trattare i nuovi concetti quali il contesto, leadership and commitment, audit virtuali, conformità e filiera di fornitura.

Mi permetto di fare una sola critica: tra i rischi relativi al programma di audit, a mio parere mancano quelli relativi ad un inadeguato campionamento.

****

03- Nuova ISO/IEC 27005

Come preannunciato a novembre, è stata pubblicata la nuova ISO/IEC 27005:2018 dal titolo "Information security risk management":
- https://www.iso.org/standard/75281.html.

Rispetto alla precedente versione riporta solo alcune correzioni necessarie per l'allineamento ad altre norme. Nella sostanza non è cambiato nulla e pertanto ne sconsiglio l'acquisto a chi ha già la versione del 2011 (che a sua volta non riportava grandi modifiche rispetto alla versione del 2008).

****

04- Correzione alla ISO/IEC 29100 (privacy framework)

La ISO/IEC 29100 è il "Privacy framework" della ISO e la versione in vigore è quella del 2011:
- https://www.iso.org/standard/45123.html.

Lo standard è gratuito e può essere reperito nel sito ufficiale:
- http://standards.iso.org/ittf/PubliclyAvailableStandards/.

A giugno 2018 è stato pubblicato un documento di correzione (Amd 1):
- https://www.iso.org/standard/73722.html.

Ho chiesto chiarimenti a chi ha seguito i lavori per questa correzione (ringrazio!) e mi ha segnalato i principali punti:
- eliminazione, modifica, inserimento di alcune definizioni anche a causa di presenza di riferimenti circolari;
- miglioramento di alcune espressioni utilizzate nel testo che possono comportare ambiguità anche in relazioni a traduzioni della norma tecnica in altre lingue.

Conclusione: nulla di critico e nulla per cui precipitarsi a comprare la correzione (eh già: il documento del 2011 è gratuito, ma la correzione costa 16 CHF!).

****

05- Linea Guida Applicativa sulla norma UNI ISO 37001:2016 per la prevenzione della corruzione

Segnalo questa pubblicazione dell'associazione Conforma dal titolo "Linea guida applicativa sulla nuova UNI ISO 37001:2016 per la prevenzione della corruzione":
- http://www.associazioneconforma.eu/news/14-generali/158-convegno-conforma-la-nuova-norma-uni-iso-37001-2016-per-la-prevenzione-della-corruzione-5.html.

Non ho letto con attenzione questa linea guida, però mi sembra ben fatta.

Va detto che non conosco bene la ISO 37001 perché non ho mai avuto l'opportunità di applicarla, quindi evito di commentarla. Però penso sia materia da "tenere sotto controllo" da chi si occupa di sicurezza delle informazioni e privacy.

****

06- Privacy: Articoli sul GDPR?

In questo mese ho segnalato pochi articoli sul GDPR, come peraltro avevo previsto.

Non era difficile fare la profezia: una volta passata la data del 25 maggio, era facile osservare che molti aspetti del GDPR erano già stati affrontati negli articoli che ho di volta in volta segnalato: le differenze rispetto al Codice, il ruolo dei responsabili, le basi legali e in particolare il legittimo interesse, i trasferimenti extra-UE, eccetera.

Questo mese mi sono stati segnalati alcuni articoli, tra cui uno di Pizzetti sul consenso (che riprende una cosa già segnalata a maggio: http://blog.cesaregallotti.it/2018/05/linee-guida-wp-art-29-su-consenso-e.html):
- https://www.agendadigitale.eu/sicurezza/gdpr-tutti-gli-equivoci-del-consenso-nei-contratti-ecco-una-guida/.

Un ulteriore articolo di Biasotti sulla "morte" dell'incaricato (roba nota e stranota e che tra l'altro non condivido, visto che continua a suggerire l'obsoleta, anche per il Codice privacy per chi lo avesse letto con un minimo di attenzione, "lettera di nomina"):
- https://www.puntosicuro.it/security-C-124/privacy-C-89/sapevate-che-l-incaricato-del-trattamento-morto-AR-18239/.

Per chi si sentisse ancora insicuro su cosa dice il GDPR, raccomando prima di tutto di leggerlo e poi di seguire le molte testate che nel tempo ho segnalato (in italiano ci sono ICT Security Magazine, Agenda Digitale, Punto Sicuro). Raccomando però prudenza quando il testo richiede di "nominare" i responsabili, fornire lettere alle persone autorizzate al trattamento (senza pensare al *vero* processo di autorizzazione, che non necessita di lettere), registrare il consenso per "maggiore tutela" o quando la base giuridica è altra, formulare una DPIA per ogni trattamento, nominare un DPO "a prescindere".

Raccomando inoltre di non impiegare troppo tempo nel leggere interpretazioni sempre più sofisticate o nel ricercare sempre "l'ultima notizia" (qui per esempio non segnalo il discorso annuale del Garante perché, alla fin fine, non dice niente di nuovo). Raccomando invece di studiare meglio i processi aziendali: quanto si è visto in questi mesi rileva la necessità di capire come funzionano i processi di acquisto e vendita e di contrattualizzazione (per soddisfare l'articolo 28), le "normali" comunicazioni aziendali (che non richiedono firme per ricevuta), la gestione delle autorizzazioni informatiche e non informatiche (che non dovrebbero prevedere letterine insulse da firmare).

In futuro segnalerò solo gli interventi particolarmente interessanti e innovativi.

****

07- Privacy: Rapporto sulla manipolazione dei social

Da Crypto-Gram di luglio, ribatto la pubblicazione del rapporto "Deceived by design" della Norwegian Consumer Council:
- https://www.forbrukerradet.no/side/facebook-and-google-manipulate-users-into-sharing-personal-data/.

In pochissime parole: Facebook e Google cercano di rendere difficilmente accessibili le funzionalità per aumentare la propria privacy, sconsigliano costantemente gli utenti di disattivare alcune funzionalità e cercano costantemente di far loro attivarne altre.

Il discorso potrebbe estendersi ai dispositivi mobili e alle loro applicazioni (un incubo!).

****

08- Privacy: sentenza Cassazione sulla necessità del consenso per newsletter

C'è ancora qualcuno che si propone di inviare "newsletter" a clienti e potenziali clienti senza il consenso esplicito, rifacendosi al concetto di "consenso soft" (previsto dal nostro Codice per i clienti già acquisiti

da un'azienda) e ad un considerando del GDPR. Continuo a ricordare che questo non è previsto dal GDPR, come anche precisato dall'Opinione del WP Art. 29 di cui avevo già dato notizia a suo tempo (blog.cesaregallotti.it/2018/05/linee-guida-wp-art-29-su-consenso-e.html).

La sentenza n. 17278/2018 della Cassazione civile, anche se basata sul Codice privacy e ad un fatto avvenuto nel 2013 o 2014, propone un'ulteriore lettura. Infatti ritiene lecito "obbligare" alla ricezione di email pubblicitarie coloro che si iscrivono ad un servizio Internet "non essenziale" e "fungibile":
- http://www.dirittifondamentali.it/giurisprudenza/cassazione-civile-e-tribunali-di-merito/anno-2018/cass-civ-17278-2018/.

Nella conclusione, la sentenza condanna però l'azienda perché non aveva reso abbastanza esplicito il consenso (con "spunte" distinte e chiare e non con una frase generica come "acconsento al trattamento dei miei dati personali come da pagina web x") e, pedantemente, richiede che l'informativa indichi i settori merceologici o i servizi cui i messaggi pubblicitari saranno riferiti.

Per i più frettolosi è possibile leggere i soli punti 2.6 e 2.7.

****

09- NIS: altri articoli

In merito al recepimento della Direttiva NIS, segnalo questi altri due articoli di Luca Tosoni.

Il primo ha titolo "Direttiva NIS, così è l'attuazione italiana (dopo il recepimento): i punti principali del decreto":
- https://www.agendadigitale.eu/sicurezza/attuazione-della-direttiva-nis-lo-lo-schema-decreto-legislativo/.

Il secondo ha titolo "Decreto Nis, ecco i prossimi passi dopo l'approvazione":
- https://www.agendadigitale.eu/sicurezza/decreto-nis-ecco-i-prossimi-passi-dopo-lapprovazione/.

****

10- Ruoli, responsabilità e adempimenti utili e inutili

Un mio articolo su ICT Security Magazine:
- https://www.ictsecuritymagazine.com/articoli/ruoli-responsabilita-e-adempimenti-utili-e-inutili/.

Non credo di averlo scritto in modo molto chiaro, ma spero che alla fine si capisca il fatto che bisogna evitare di creare ruoli inutili e di prendere esempio dal passato.

****

11- Algeria spegne Internet per evitare truffe agli esami

Da Crypto-Gram di luglio, segnalo questa notizia dal titolo "Algeria blocks internet to prevent students cheating during exams":
- https://www.theguardian.com/world/2018/jun/21/algeria-shuts-internet-prevent-cheating-school-exams.

E' certamente una notizia "di colore", ma ci ricorda che le soluzioni estreme vanno sempre considerate e non per forza evitate. Per esempio: bloccare tutte le porte USB dei PC e bloccare ogni forma di

installazione di software, evitare ogni forma di BYOD (e quindi non mettere a disposizione neanche la webmail).

Ovviamente è da evitare anche l'eccesso di zelo. Ma non si può prendere una decisione bilanciata senza conoscere le possibili alternative e valutarle seriamente.

****

12- Furto di documenti via DropBox

Per chi ancora non teme l'uso di strumenti di file sharing all'interno delle organizzazioni, segnalo la recente condanna di un tecnico (fornitore) che ha rubato circa 5.000 documenti al suo cliente (la Marina USA), semplicemente trasferendoli a se stesso via Dropbox:
- https://www.bleepingcomputer.com/news/legal/engineer-found-guilty-of-stealing-navy-secrets-via-dropbox-account/.

Commento di Lee Neely (del Comitato editoriale di SANS NewsBites da cui ho tratto la notizia): "Una volta che si autorizza il traffico tramite piattaforme di collaborazione cloud, è quasi impossibile distinguere quando questi servizi sono usati per scopi lavorativi o personali. Qualche mitigazione è possibile impedendo l'installazione dei client di questi servizi o identificando gli utenti che usano Internet per poi poterne tracciare le azioni".

Il commento non è molto originale e le misure proposte sono facilmente aggirabili se agli utenti sono forniti dispositivi portatili che possono connettersi a qualunque wi-fi e su cui è possibile installare qualsiasi software.

****

13- Società di audit PCI citata in giudizio

La notizia è che la società di audit PCI Trustwave è stata citata in giudizio dalle società di assicurazione che hanno dovuto pagare i danni a seguito dell'intrusione nei sistemi della società Heartland.

La mia prima fonte è la newsletter SANS Newsbites:
- https://www.sans.org/newsletters/newsbites/xx/54.

Segnalo un articolo su Dark Reading:
- https://www.darkreading.com/application-security/insurers-sue-trustwave-for-$30m-over-08-heartland-data-breach/d/d-id/1332248.

Vedo però che la società è già stata oggetto di citazioni, per esempio nel 2014, come racconto questo articolo sempre di Dark Reading:
- https://www.darkreading.com/risk/compliance/target-pci-auditor-trustwave-sued-by-banks/d/d-id/1127936.

Purtroppo i due articoli non mi sembrano collegati, ma dovrebbero esserlo (per esempio, come è finita con le banche che hanno chiesto danni sempre alla società di audit?). In questo caso, mi mancano informazioni e la capacità di trovarle. Se qualcuno ne dovesse avere, lo pregherei di diffonderle. Anche perché, in qualità di auditor, sono preoccupato.

****

14- WPA3

Da Crypto-Gram di luglio: sono state pubblicate le specifiche del WPA3, il protocollo sicuro per le connessioni wi-fi che sostituirà l'attuale WPA2:
- https://www.wired.com/story/wpa3-wi-fi-security-passwords-easy-connect/.

I dispositivi saranno però disponibili tra qualche tempo.

****

15- Dati automotive compromessi per un errore del fornitore

In questi giorni sto ricordando la necessità di non concentrarsi sui fornitori cloud, ma su tutti i fornitori (anche non informatici).

Come per magia, su SANS NewsBites questa notizia su un server mal configurato di un fornitore non cloud:
https://www.infosecurity-magazine.com/news/robotics-supplier-error-leaks/.

Altra cosa interessante: si tratta di una violazione di dati... non personali.

****

16- Attacco ai fornitori di energia USA

Un attacco (informatico) ai fornitori di energia USA che ricorda quanto sia importante prestare attenzione ai fornitori. Infatti l'attacco è stato condotto inviando email con link a siti compromessi al personale dei piccoli subfornitori:
- https://www.bbc.co.uk/news/technology-44937787.

****

17- Assicurazioni sui rischi informatici

Su LinkedIn (ringrazio soprattutto Dany Elie Aronovitch per avermi fornito il link e il commento giusto), ho visto che il Comune di Reggio Emilia si è dotato di una polizza assicurativa “Rischi informatici".

Il commento di Dany Elie Aronovitch: "Durante la prima gara, di ottobre 2017, la parte di cyber andò deserto (nessuna offerta presentata), poi i miracoli del gdpr hanno fatto il resto. Qui il link":
- https://www.comune.re.it/Sottositi/AvvisiPubblici-Profilocommittente.nsf/SottoSitoDocumentiFull/4543E29448D82B30C12581C20036C5FD?opendocument&FT=V&TAG=Esiti%20di%20gara.

Per il post completo su LinkedIn:
- https://www.linkedin.com/feed/update/urn:li:activity:6426006584371007488.

Questa non mi pare essere una polizza "per tutti", ma studiata per uno specifico bando.

Periodicamente ritorna il discorso "polizze assicurative". Finora ho visto solo cose che riducevano il tutto ai "normali" danni informatici. Ora ho avuto notizia di questa polizza (offerta dalla Compagnia Chubb European Group Limited) e un'altra offerta da Mansutti (in tutti e due i casi non ho però accesso al modello di contratto vero e proprio). Mi sembrano più rispondenti alle necessità di chi si occupa di sicurezza delle informazioni, però chiedo se altri hanno maggiori e migliori informazioni.