Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – GENNAIO 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.

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.

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- Nuova edizione libro "Sicurezza delle informazioni" (anche in inglese)

In questi giorni sto pubblicando una nuova edizione del mio libro "Sicurezza delle informazioni". Non ci sono grandi novità. Quelle che ci sono, sono riprese da segnalazioni già fatte in questa sede.

Più di un anno fa, avevo deciso di tradurlo in inglese (mi sono fatto aiutare!) e, rileggendo le bozze, ho trovato errorini e cose da aggiornare (incluse alcune considerazioni in materia di privacy, come è ovvio dopo l'uscita del GDPR). Avrò sicuramente aggiunto altri errori e mi sarò dimenticato altre cose.

Attenzione che sto caricando le edizioni (pdf A4, epub e derivati come kindle, edizione cartacea in formato letter) un po' alla volta, anche perché devo sempre verificare un po' di cose prima che la versione sia corretta.

Pertanto, per chi non può fare a meno di comprare una copia del mio libro (grazie! grazie! grazie!), segnalo di fare attenzione a che in copertina ci sia scritto "versione del gennaio 2019)".

Il mese prossimo invierò i link.

****

01- Guida ETSI per un SOC

Franco Vincenzo Ferrari di DNV GL mi ha segnalato che ETSI ha pubblicato la ETSI GS ISI 007 V1.1.1 (2018-12) dal titolo "Information Security Indicators (ISI); Guidelines for building and operating a secured Security Operations Center (SOC)":
- https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=50920.

Questo documento è importante perché la Direttiva NIS (recepita dal nostro D. Lgs. 65 del 2018) richiede ai fornitori di servizi essenziali di attivare processi di rilevazione, trattamento e segnalazione degli incidenti di sicurezza informatica, spesso compito di un SOC.

Personalmente, non credo che la lettura di una Linea guida come questa possa insegnare veramente come realizzare e operare un SOC (per questo ci sono sicuramente validi libri), ma è certamente un ottimo riferimento.

****

02- Guida alla sicurezza IT dell'US Dept. of Health and Human Services

Il SANS NewsBites del 4 gennaio (www.sans.org) segnala la pubblicazione della serie di documenti "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients" da parte dell'US Dept. of Health and Human Services:
- https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx.

Un commento di un curatore del SANS segnala che questa guida è un cambio di direzione perché si basa sulle "buone pratiche", non sul "rischio". Secondo molti è un male, ma secondo me è un bene, fino ad un certo punto. Come dice lo stesso curatore del SANS NewsBites, per una vera valutazione del rischio sono necessari tempo e competenze (oltre che soldi) e spesso i risultati non sono poi così strabilianti. Allora ben venga un elenco di "buone pratiche" su cui è possibile ragionare e non un vago richiamo (come oggi va di moda) alla valutazione del rischio senza una seria valutazione delle soluzioni oggi disponibili.

E' vero che domani le soluzioni saranno diverse, ma almeno qualcuno ci spiega quelle di oggi.

A dire il vero, non mi sembra che questa guida presenti cose particolarmente innovative o relative alla sanità (persino la "Cybersecurity Practice #9: Medical Device Security" non mi è sembrata particolarmente significativa). Però confesso di non averla letta con particolare attenzione.

****

03- Guide per avviare collaborazioni in materia di sicurezza IT

Il National Cyber Security Centre (NCSC) dei Paesi Bassi ha pubblicato delle guide per migliorare le collaborazioni settoriali, geografiche o di filiera in materia di sicurezza informatica:
- https://www.ncsc.nl/english/cooperation.

Questo può essere un ulteriore tassello per l'applicazione della Direttiva NIS (la notizia l'ho ricevuta da un tweet di @enisa_eu). Mi chiedo quanto questo argomento sarà sviluppato. In Italia abbiamo, come elemento positivo, una storia di distretti industriali da cui attingere. Penso però che, alla fine, a meno che qualche Pubblica amministrazione (come già succede in alcuni casi) non promuova alcune collaborazioni, i grandi fornitori di servizi IT metteranno sul mercato i loro servizi di SOC "generalisti".

Sono curioso di vedere come andranno le cose.

****

04- Differenze tra sicurezza IT e sicurezza ICS (e non solo)

Da un tweet di @yvetteagostini, segnalo questa breve riflessione dal titolo "IT+OT Cyber security experts?":
- lnkd.in/eE5j5qs.

In sostanza dice che chi si occupa di sicurezza informatica (orientata alla difesa di riservatezza, integrità e disponibilità) non può riutilizzare gli stessi concetti alla sicurezza industriale (sicurezza per OT o Operational technology o per ICS o Industrial Control Systems, di cui fanno parte gli SCADA). Infatti la sicurezza per OT si concentra sulla difesa di sicurezza fisica (safety), affidabilità (reliability) e produttività (productivity). A maggior ragione, non è pensabile una roba come la "convergenza di sicurezza IT e OT".

Non sono molto d'accordo (per esempio perché sono convinto che la sicurezza IT debba anche considerare la produttività e la sicurezza OT debba anche considerare la riservatezza; gli altri parametri sono sovrapponibili), ma trovo istruttivo questo sottolineare la differenza culturale tra le due materie.

È innegabile che, per affrontare bene una materia, è necessario capirne la cultura di fondo. Questo l'ho visto, per esempio, quando ho affrontato la qualità dopo essermi dedicato alla sicurezza delle informazioni e poi, nella mia crescita professionale, sono ritornato alla sicurezza delle informazioni e poi alla gestione dei servizi, alla continuità operativa, alla privacy, eccetera. Ogni materia ha le sue peculiarità e queste vanno capite e apprezzate prima di farle "convergere".

È anche per questi motivi che ho sempre cercato di non fare elenchi di correlazione tra norme sulla sicurezza (ISO/IEC 27001), sulla gestione dei servizi (ISO/IEC 20000-1), sulla privacy e altro. Ed è anche per questi motivi che evito l'uso dell'espressione "cybersecurity", visto che è usato in modo molto vago, per includere o escludere la sicurezza IT o OT, a seconda dell'interlocutore.

****

05- Sensibilizzazione 04 - Materiale NCSC

Dark Reading Weekly segnala che lo statunitense National Counterintelligence and Security Center (NCSC) ha messo online del materiale di sensibilizzazione:
- https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield/ncsc-awareness-materials.

I video mi sembrano molto interessanti. Non proprio divertentissimi, ma interessanti. Il resto del materiale mi sembra di difficile interpretazione (io, perlomeno, faccio fatica a capirlo). Tutto è in inglese, ma può isprirare inziative in italiano (per chi ne avesse voglia).

****

06- Bufale su Internet

Penso che le bufale (o "fake news", come si usa dire oggi in inglese) siano un argomento non proprio pertinente il mio mestiere, ma comunque interessante.

Infatti siamo testimoni di bufale relative alle misure di sicurezza o adempimenti inesistenti (o non più inesistenti). Siamo anche testimoni di paure ingiustificate su possibili attacchi quasi impossibili (inclusi i terremoti a Milano) e di sottovalutazione di attacchi molto più probabili (come quelli su alcuni servizi accessibili dal web).

E' per questo che segnalo qualche link che @sramakk ha condiviso su Twitter sulle bufale su Wikipedia (forse in questi giorni avrà notato qualche esempio o avrà incontrato qualcuno troppo entusiasta di Wikipedia). Uno è di uno che è riuscito a far circolare false citazioni (sperando che a sua volta non sia una bufala):
- https://www.wired.it/internet/2014/01/15/come-ho-fregato-tg-politici-e-giornali-con-wikipedia/.

Un altro è su alcune bufale particolarmente significative:
- https://www.ilpost.it/2015/04/18/wikipedia-affidabilita/.

Più o meno negli stessi giorni, ho notato anche questo tweet di @Chronotope che suggeriva un articolo dal titolo "How Much of the Internet Is Fake? Turns Out, a Lot of It, Actually", dedicato al fatto che sono create misure, utenze e contenuti solo per generare numeri utili alla pubblicità (e al denaro, ovviamente):
- https://nymag.com/intelligencer/2018/12/how-much-of-the-internet-is-fake.html.

E sempre negli stessi giorni ho visto un tweet sulla propaganda politica e sull'uso distorto dei canali di comunicazione (la stessa foto, innocente, usata in più di 180 articoli razzisti!):
- https://twitter.com/bknsty/status/1081954569196879872.

****
07- Penale per Facebook per ritardo nella riattivazione di un account sospeso immotivatamente

Luca De Grazia mi ha informato di un'interessante sentenza: Facebook è stata punita perché disabilitò un'utenza senza assicurarle un minimo di diritto di difesa.

Luca De Grazia mi ha segnalato l'articolo su Quotidiano Giuridico:
- http://www.quotidianogiuridico.it/documents/2018/12/20/sospensione-immotivata-dell-account-penale-per-facebook-in-caso-di-ritardo-nella-riattivazione#.

Segnalo altri due articoli sulla medesima questione. Uno è giornalistico da Italia Oggi:
- https://www.italiaoggi.it/news/stop-alle-censure-immotivate-da-parte-di-facebook-2321752.

Un altro è più tecnico, da Studio Cataldi:
- https://www.studiocataldi.it/articoli/32919-facebook-non-puo-disattivare-un-account-senza-motivo.asp.

****

08- Foto dei figli sui social network

Da un tweet di @a_oliveri, segnalo questo articolo dal titolo "Foto sui social dei figli minorenni, i genitori rischiano fino a 10mila euro di multa":
- https://www.repubblica.it/tecnologia/2018/01/08/news/multa_foto_figli_social-186077784/.

Credo che queste vicende dicano tanto sulla cultura del "non abbiamo segreti per nessuno; anzi... facciamo vedere a tutti i fatti nostri!". Questa cultura va capita da chi si occupa di sicurezza delle informazioni e di privacy, perché si concretizza in violazioni di dati.

****
09- GDPR: verificata dal Garante la conformità dei Codici deontologici

Il Garante ha aggiornato i codici deontologici per allinearli al GDPR:
- https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9069732.

Oggi si chiamano "Regole deontologiche". Se ho capito correttamente, non riportano novità rispetto alle precedenti versioni.

Per i più scrupolosi, la notizia è accompagnata da riflessioni sul fatto che non è stata avviata una consultazione pubblica.

****
10- Garante privacy e aggiornamenti sulle autorizzazioni generali

Il Garante privacy ha avviato i lavori relativi agli aggiornamenti sulle autorizzazioni generali. La notizia sulla newsletter fa il punto delle autorizzazioni che non sono più valide ("hanno cessato completamente i loro effetti"):
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069012.

Il Provvedimento (doc. web 9068972), invece, fa il punto su quelli che risultano compatibili con il GDPR e prevede di avviare una consultazione pubblica per aggiornarle:
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9068972.

Quindi: siamo ancora all'idea di bozze. Ci saranno i soliti che si agiteranno, ma in realtà ci sarà da aspettare.

****