Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – MARZO 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

01- Milano, 10 aprile 2019: DFA Open day 2019
02- Libro "Consapevolmente cloud"
03- La sicurezza delle informazioni non è un'opportunità
04- DM per sicurezza operatori TLC
05- Articolo sul Cybersecurity Act
06- Violenza privata impedire all'internal audit di svolgere le proprie mansioni
07- Sweep 2018: l'analisi dei Garanti sull'attuazione del GDRP
08- Prima bozza dei criteri per la certificazione GDPR
09- ETSI TS 103 645 Cyber Security for Consumer Internet of Things
10- Rapporti sulle minacce e sugli attacchi (Clusit, CrowdStrike, Symantec e BCI)
11- Un altro articolo negativo su blockchain

****
01- Milano, 10 aprile 2019: DFA Open day 2019

Insisto e ricordo che il 10 aprile pomeriggio si terrà a Milano l'annuale DFA Open day (gratuito). Per iscriversi:
- https://www.eventbrite.it/e/biglietti-dfa-open-day-2019-56637583537.

Il programma non lo abbiamo ancora stabilito completamente, ma parleremo di digital forensics (lato tecnologico e lato legale), di GDPR e chissà che altro.

Per la cronaca, sono presidente dell'associazione.

****
02- Libro "Consapevolmente cloud"

E' stato pubblicato il libro "Consapevolmente cloud", a cura della Oracle Community for Security e con l'obiettivo di presentare alcuni aspetti utili alle organizzazioni che vogliono usare servizi cloud:
- https://consapevolmentecloud.clusit.it.

Lo segnalo perché ho partecipato come revisore. Non mi pare che il libro abbia contenuti particolarmente innovativi rispetto alle numerose pubblicazioni già a disposizione. Qualche spunto però l'ho colto e mi ha fatto piacere avere la possibilità di leggerlo e commentarlo in anteprima.

****

03- La sicurezza delle informazioni non è un'opportunità

E' stato pubblicato questo mio articolo per ICT security magazine, dal titolo "La sicurezza delle informazioni non è un'opportunità":
- https://www.ictsecuritymagazine.com/articoli/la-sicurezza-delle-informazioni-non-e-unopportunita/

Era nato come una risposta provocatoria ad un post su LinkedIn. Poi ho elaborato ulteriormente i concetti.

****

04- DM per sicurezza operatori TLC

Andrea Evangelista via LinkedIn mi ha segnalato la pubblicazione del DM del 12 dicembre 2018 del Ministero dello sviluppo economico e pubblicato in G.U. il 21 gen 2019 "Misure di sicurezza ed integrità delle reti di comunicazione elettronica e notifica degli incidenti significativi":
- www.gazzettaufficiale.it/eli/id/2019/01/21/19A00317/s.

Andrea Evangelista mi dice "dettaglia l'art. 16bis e ter del Codice delle comunicazioni elettroniche. E' un po' l'equivalente del D. NIS per i servizi di comunicazione elettronica e i fornitori di reti e servizi di comunicazione".

Per completezza, il link al Codice delle comunicazioni elettroniche:
- www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-08-01;259!vig=

Qualche riflessione (cerco di unire le mie con quelle di Andrea; ogni errore e mio):
- i destinatari sono i "fornitori di servizi di reti e servizi di comunicazione elettronica", ossia i fornitori di connessione (Telco) e le società cosiddette "wholesale only", ossia quelle che hanno una concessione ex art. 25 del Codice delle comunicazioni elettroniche; non è indirizzato ai fornitori di contenuti;
- quando parla di incidenti (articolo 5), li intende solo come con impatto sulla disponibilità e non su integrità (dei dati) e riservatezza (ha come obiettivo di garantire la disponibilità e continuità dei servizi sulle reti e prevenire i cosiddetti incidenti significativi che creano "disservizi");
- interessante il sunto di un sistema di gestione per la sicurezza delle informazioni dell'articolo 4 (anche se certe rigidità normative possono essere discusse);
- interessante anche l'art. 6 comma 2 che tratta "dell'eventuale possesso di certificazioni di conformità...";
- meno apprezzabile il ricorso agli "asset" come base per la valutazione del rischio, concetto ormai ritenuto superato (ma va detto che il testo è sufficientemente ambiguo e può essere letto anche pensando alla necessità di descrivere correttamente i servizi e identificare i rischi non necessariamente per ciascun asset; usa termini come "potenzialmente in grado" e "asset propri o di terzi che contribuiscono anche parzialmente alla fornitura dei servizi...").

****

05- Articolo sul Cybersecurity Act

A dicembre è stato raggiunto l'accordo per il Regolamento europeo detto "Cybersecurity act".

Questo Regolamento è importante perché:
- affida ad ENISA un ruolo più operativo, in particolare per quanto riguarda la gestione degli incidenti;
- introduce lo schema di certificazione europeo per i prodotti e i servizi informatici (che dovrà comunque essere ulteriormente specificato).

Su questo tema, segnalo questo articolo (anche se usa malamente il termine "cibernetico") dal titolo "Cybersecurity Act, ecco cosa ci aspetta dopo la Direttiva NIS":
- https://www.agendadigitale.eu/sicurezza/cybersecurity-act-ecco-cosa-ci-aspetta-dopo-la-direttiva-nis/.

Segnalo che non approfondisce gli schemi di certificazione dei prodotti. Oggi, come indicato, ne sono in vigore alcuni, ma basati su schemi diversi; in particolare in Italia sono usati i Common criteria (ISO/IEC 15408), mentre in altri Paesi sono stati introdotti altri requisiti. Sarebbe interessante fosse condotta un'analisi su questi schemi (nel caso fosse già stata fatta, invito a segnalarmela).

****

06- Violenza privata impedire all'internal audit di svolgere le proprie mansioni

Luca de Grazia mi ha segnalato questo articolo de Il quotidiano giuridico, dal titolo "È violenza privata impedire all'internal audit di entrare in azienda e svolgere le proprie mansioni", relativo ad un'interessante sentenza della Cassazione penale:
- http://www.quotidianogiuridico.it/documents/2019/02/25/e-violenza-privata-impedire-all-internal-audit-di-entrare-in-azienda-e-svolgere-le-proprie-mansioni#.

La sentenza l'ho trovata sul sito http://www.italgiure.giustizia.it/sncass/, inserendo nel campo di ricerca 4779/2019.

****

07- Sweep 2018: l'analisi dei Garanti sull'attuazione del GDRP

I Garanti europei hanno condotto nell'ultimo quadrimestre del 2018 un'indagine "a tappeto" sullo stato di attuazione del GDPR. Il nostro Garante ha pubblicato una sintesi dei risultati:
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9088164.

Si scopre che, in realtà, l'indagine non è veramente "a tappeto", visto che è stata condotta su soggetti selezionati. In Italia sono stati selezionati Regioni e Province autonome, nonché le rispettive società controllate. I risultati non sono particolarmente soprendenti, ma forniscono un'indicazione sui punti considerati più importanti dalle autorità Garanti.

****

08- Prima bozza dei criteri per la certificazione GDPR

L'European Data Protection Board (EDPB) ha pubblicato la bozza ("versione per consultazione pubblica") delle "Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679":
- https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en.

Siamo ancora lontani dall'avere i criteri di certificazione rispetto al GDPR. Questi sono i criteri per valutare i criteri di certificazione. Sono, insomma, meta-criteri.

****

09- ETSI TS 103 645 Cyber Security for Consumer Internet of Things

Segnalo questa pubblicazione di ETSI dal titolo "Cyber Security for Consumer Internet of Things":
- https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=54761.

E' scaricabile gratuitamente e senza registrazione.

Non l'ho studiata né confrontata con la mia lista di requisiti per l'IoT (lo farò quando mai dovrò lavorarci sopra), però mi pare interessante e scritta bene, con requisiti chiari e sintetici. Sapendo che ci hanno lavorato persone competenti, sicuramente sarà completa.

****

10- Rapporti sulle minacce e sugli attacchi (Clusit, CrowdStrike, Symantec e BCI)

La primavera è il periodo in cui molte società pubblicano rapporti sulla sicurezza delle informazioni.

Io penso che molti siano poco significativi perché non forniscono informazioni realmente utili. Li segnalo perché so che a molti interessano.

Il primo è il BCI Horizon Scan Report 2019, basato sulle impressioni (!!!) degli intervistati:
- https://www.thebci.org/resource/horizon-scan-report-2019.html.

Il secondo è il Symantec Internet Security Threat Report (segnalatomi dal SANS NewsBites del 22 febbraio):
- https://www.symantec.com/security-center/threat-report.

Ricorda che gli attacchi più frequenti sono: formjacking (particolare forma di injection), Ransomware, IaaS in cloud mal configurati (in particolare S3), IoT. Non ho capito benissimo cosa siano gli attacchi Living off the Land, ma non vorrei siano gli attacchi condotti da persone interne (o comunque con accesso alla rete interna) con "normali" strumenti di amministrazione. Insomma... cose già viste e sentite.

Segnalo che non ho scaricato il report completo perché mi chiede i miei dati di contatto. Forse ci sono cose più interessanti e, se qualcuno ne dovesse avere notizia, lo prego di segnalarmelo.

Il terzo è quello di CrowdStrike (società che non conoscevo, ma il cui report è segnalato dal SANS NewsBites del 22 febbraio 2019):
- https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/.

Divertente leggere la classificazione dei gruppi di criminali sulla base della provenienza geografica e facendo uso di nomi come Kryptonite Panda o Vodoo Bear. Per il resto queste sono altre statistiche senza reale utilità (mi chiedo a cosa serva sapere la velocità, peraltro alta, con cui, una volta compromessa una rete, i criminali possono acquisire i privilegi massimi).

Il SANS segnala, tra gli altri, questo sito che riporta i risultati in sintesi:
- https://www.fifthdomain.com/industry/2019/02/21/new-report-questions-effectiveness-of-cyber-indictments/.

Infine segnalo il Rapporto Clusit 2019 sulla sicurezza ICT in Italia:
- https://clusit.it/rapporto-clusit/.

Anch'esso presenta un'enorme quantità di dati che, alla fine, non aiutano a migliorare la sicurezza informatica. Il Rapporto è in realtà una doppia pubblicazione: la prima è il rapporto vero e proprio con dati e analisi sugli eventi del 2018 e sulle previsioni per il 2019; la seconda è una raccolta di articoli, alcuni decisamente interessanti.

****

11- Un altro articolo negativo su blockchain

Per quanto poco io capisca di blockchain o, come dicono quelli che vogliono essere "meno modaioli", di distributed ledger technology (DLT), penso che sia una boiata pazzesca (a differenza della Corazzata Potemkin, che è un grande film).

Il mio parere, come già scrissi tempo fa, è da prendere con prudenza. Ma quello di Bruce Schneier, uno degli esperti di sicurezza veramente competenti e che ragiona invece di ripetere a pappagallo quello che dicono altri, va preso molto seriamente (scrive anche benissimo, tra gli altri suoi pregi).

Quindi io segnalo il suo articolo "Blockchain and Trust":
- https://www.schneier.com/blog/archives/2019/02/blockchain_and_.html.

In sintesi, anche lui pensa che la blockchain sia un termine di moda e che, nella realtà, la sua tecnologia non migliora la sicurezza e sicuramente peggiora l'efficienza dei sistemi. Lui parla di blockchain pubblica, visto che quella privata è realizzabile in mille altri modi e tecnicamente avrebbe altri nomi (è indicata con il termine "blockchain" solo perché di moda).