Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – FEBBRAIO 2020

****

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- 18 e 19 marzo 2020: mio intervento su IoT e ISO/IEC 27701 al Security summit
02- VERA 5 in inglese
03- EN 16234-1: 2019 - Quadro e-Competence (e-CF)
04- Le peggiori password del 2019
05- Mean Time to Hardening
06- Antivirus Avast free e la rivendita dei dati
07- EBA Guidelines on ICT and security risk management
08- Notizie su di me: Comunicato stampa Patch AI
09- Privacy: Primi ammonimenti sulle violazioni di dati personali
10- Privacy: ENISA on-line tool for the security of data processing
11- Privacy: Linee guida EDPB su videosorveglianza
12- Privacy: Il DPO deve essere un legale (ma forse anche no) - Puntata AGCM
13- Privacy: NIST privacy framework
14- Privacy: Ispezioni GDPR della GdF (un resoconto)

****

01- 18 e 19 marzo 2020: mio intervento su IoT e ISO/IEC 27701 al Security summit

Il 18 e il 19 marzo interverrò al Security summit di Milano.

L'intervento del 18 marzo alle 9.30 riguarda il libro “IoT Security e Compliance: gestire la complessità e i rischi”, che sarà pubblicato in quei giorni;
- https://securitysummit.it/agenda-details/520.

L'intervento del 19 marzo alle 16.30 è su "Certificazione della protezione dei dati personali" e Io cercherò di spiegare in pochissimi minuti la ISO/IEC 27701 (sento già la musichetta di Mission impossible):
- https://securitysummit.it/agenda-details/532.

****

02- VERA 5 in inglese

Ho caricato la versione in inglese di VERA 5.

La trovate qui insieme alla versione in italiano aggiornata alla 5.0.1 (ho corretto un piccolo refuso):
- https://www.cesaregallotti.it/Pubblicazioni.html.

****

03- EN 16234-1: 2019 - Quadro e-Competence (e-CF)

E' stata pubblicata la nuova versione dell'e-CF. La notizia me l'ha data la newsletter I see T di Uninfo:
- https://uninfo.it/index_pages/news/focus/1580812766424.html.

Ricordo che e-CF permette di classificare le competenze in ambito informatico e può servire per la ricerca di determinate competenze, come peraltro promosso da AgID.

Io non sono un grande fan di questa iniziativa perché la trovo un po' troppo elaborata. Ciò non ostante, penso che sia comunque utile conoscerla, visto che è alla base anche di norme italiane relative ai profili professionali in ambito sicurezza (UNI 11621-4) e privacy (UNI 11697).

****

04- Le peggiori password del 2019

La pagina "Here are the most popular passwords of 2019":
- https://nordpass.com/blog/top-worst-passwords-2019/.

Mi rendo conto che la pagina è soprattutto utile a NordPass, produttore di uno strumento di password management che non conosco e che non posso né raccomandare né sconsigliare, ma si tratta sempre di una buona risorsa.

In passato l'iniziativa era di TeamsID, altro Password manager (o è lo stesso che ha cambiato nome? non ho proprio verificato), ma quest'anno non l'ha ripetuta.

****

05- Mean Time to Hardening

Niccolò Castoldi mi ha segnalato questo interessante articolo dal titolo "Mean Time to Hardening: The Next-Gen Security Metric":
- https://threatpost.com/mean-time-hardening-next-gen-security-metric/151402/?mc_cid=9b25b37c64&mc_eid=e2b3a4cb20.

Ho i miei dubbi sull'applicabilità di quanto scritto, ma è indubbiamente interessante il ragionamento sui tempi da rispettare per l'hardening: 24 ore (che lo stesso autore ritiene molto sfidanti).

****

06- Antivirus Avast free e la rivendita dei dati

Aldo Colamartino mi ha segnalato questo interessante articolo:
- https://www.ilsoftware.it/articoli.asp?tag=Avast-nell-occhio-del-ciclone-la-versione-free-rastrella-i-dati-degli-utenti_20626.

Non è il primo caso di questo tipo, ma mi pare interessante che proprio attraverso un prodotto di sicurezza siano trattati con tanta disinvoltura i dati degli utilizzatori.

Sempre più prodotti propongono agli utenti di inviare i dati a scopi di "analisi delle prestazioni", ma è ovvio che forse questa non sia l'unica finalità.

****

07- EBA Guidelines on ICT and security risk management

Enrico Toso di Deutsche Bank mi ha segnalato la pubblicazione delle EBA Guidelines on ICT and security risk management:
- https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management.

Riporto quanto mi scrive Enrico e lo ringrazio.

<<
Anche se dal titolo non è esplicito, questa Guideline di EBA (Autorità di Vigilanza Europea) si applica al settore finanziario e in particolare alle istituzioni (istituti di credito e di investimento) oltre che alle relative Autorità Competenti Nazionali, per garantire la sicurezza delle operazioni di pagamento. In quest'ottica sostituirà anche la precedente "Guidelines on security measures for operational and security risks of payment services" (EBA/GL/2017/17) e si propone di regolamentare il settore dei pagamenti anche per quello che riguarda l'accesso delle Fintech e delle cosiddette Terze Parti (o TPP) al mondo dell'Open Banking.

E' frutto di un paio di anni di gestazione e contiene (in fondo) anche gli esiti della consultazione pubblica rispetto a cui esprime delle valutazioni ragionate (per recepirle o rifiutarle).
>>

****

08- Notizie su di me: Comunicato stampa Patch AI

Non faccio pubblicità nel mio blog e nella mia newsletter, ma questa volta c'è il mio nome su un articoletto del Sole 24 Ore:
- https://www.diritto24.ilsole24ore.com/art/avvocatoAffari/newsStudiLegaliEOrdini/2020-01-31/stefanelli-stefanelli-fianco-patchai-la-compliance-materia-gdpr-144610.php.

Quando mai mi ricapiterà?

****

09- Privacy: Primi ammonimenti sulle violazioni di dati personali

Questa notizia l'avevo presa sotto gamba: la Provincia di Trento ha inviato un'email alle famiglie con bambini non in regola con l'obbligo vaccinale con i nominativi in chiaro (ossia non nel campo bcc o ccn):
- https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9261234.

La newlsetter del Garante l'aveva infatti messa sotto il titolo "Salute: Garante, no alla e-mail con più indirizzi in chiaro" e non mi sembrava potesse dire cose nuove o inaspettate. Ma qualcuno mi ha fatto notare che il titolo sarebbe potuto essere "Primi ammonimenti su data breach" e la cosa, credo, si fa molto più interessante perché fornisce un'idea di come il Garante intende approcciare le situazioni.

****

10- Privacy: ENISA on-line tool for the security of data processing

Giulio Boero e Pierfrancesco Maistrello mi hanno segnalato il "ENISA on-line tool for the security of data processing":
- https://www.enisa.europa.eu/risk-level-tool.

Bisogna poi premere sull'icona "Evaluating the level of risk for a personal data processing operation".

Riporto il commento di Giulio Boero, che condivido:

<<
Questo tool mi pare molto "dritto allo scopo" (come un po' l'approccio dell'ENISA ultimamente, senza troppi fronzoli e molto pragmatico) e anche graficamente gradevole.

E' basato fondamentalmente su due punti:
- un self-assessment calibrato sui controlli ISO/IEC 27001:2013 per "vedere" il posizionamento di un'organizzazione rispetto al trattamento dei dati personali; alla fine si può anche esportare un report abbastanza utile;
- un tool che verifica il rischio sul trattamento dei dati personali a partire dalle classiche domande RID fino ad arrivare a quesiti più verticali riguardanti la relazione tra il dato personale trattato e la criticità rispetto al settore di business dell'organizzazione.
Forse la formula finale (la classica threat*impact = risk) poteva essere migliorata, ma come detto l'idea di fondo è che questo tool sia utile e costituisca una buona (ottima?) base di partenza; ed è qualcosa che forse mancava e di cui si sentiva il bisogno.
>>

Riporto anche il commento di Pierfrancesco Maistrello e dico che condivido anche questo:

<<
Il tool non permette di valutare l'abbattimento del rischio in relazione alle misure adottate.

In sintesi, lo strumento dice:
1. ecco qui un processo documentato e dimostrabile di valutazione del rischio;
2. a fronte dei risultati, ti sforno una lista di misure che applicherai.
>>

Io aggiungo due cose a cui bisogna stare attenti:
1- i calcoli sono tutti basati sul massimo e le formule sono molto ma molto più semplici di quanto la presentazione fa immaginare; approvo l'approccio, ma si rischia di rimanere delusi;
2- per la valutazione delle minacce, sono fatte tante domande intermedie, ma alla fine chiede una valutazione complessiva; il meccanismo non è quindi automatico; ancora una volta: nulla di male ma si rischia la delusione.

Non mi resta che ringraziare Giulio e Pierfrancesco per la segnalazione.

****

11- Privacy: Linee guida EDPB su videosorveglianza

L'EDPB ha pubblicato la versione finale delle "Guidelines 3/2019 on processing of personal data through video devices". A luglio aveva pubblicato una prima versione per consultazione pubblica:
- https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

Al momento non mi sembra disponibile la versione in italiano.

Dopo una prima lettura, segnalo alcuni aspetti per me degni di nota:
- non è sempre richiesta la PIA, soprattutto per i casi tipici in cui è usata la videosorveglianza (ossia la sicurezza, con un numero limitato di persone che accedono ai video in tempo reale o registrati); da osservare che neanche il "Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto" del nostro Garante impone la PIA per ogni tipo di videosorveglianza;
- è lungamente trattata la "eccezione per scopi domestici";
- sono altrettanto lungamente trattate le basi legali per il trattamento, ma è chiaro che in molti casi queste non possono includere il consenso;
- non tratta, purtroppo, il caso di pubblicazione di video di eventi;
- include, e questo è importante, un capitolo sul trattamento di dati biometrici (riconoscimento facciale), che potrebbe essere considerato anche più in generale e non solo per i video;
- sulle informative propone un nuovo modello rispetto a quello del Garante (ma nulla vieta di adattare il precedente) e richiede che sia disponibile un'informativa più dettagliata rispetto a quella minima sul cartello;
- stabilisce che, per la video sorveglianza, 72 ore di conservazione sono normalmente sufficienti e che un tempo più lungo debba essere giustificato (ricordiamoci che il nostro Garante ha stabilito che il tempo "normale" è di 24 ore e il massimo non dovrebbe essere superiore ai 7 giorni);
- sono suggerite misure di sicurezza non molto dissimili da quelle del Provvedimento italiano del 2010, ma comunque, in alcuni casi, più dettagliate.

****

12- Privacy: Il DPO deve essere un legale (ma forse anche no) - Puntata AGCM

Sulla questione del DPO avvocato, si è inserita anche l'Autorità garante della concorrenza. Nel bollettino 1/2020 si trova infatti la decisione AS1636:
- https://www.agcm.it/pubblicazioni/bollettino-settimanale/2020/1/Bollettino%201/2020.

In breve: "l'Autorità auspica che le amministrazioni in indirizzo valutino con attenzione i requisiti da inserire nei propri bandi per la selezione dei RPD al fine di evitare restrizioni all'accesso alle selezioni che possano risultare sproporzionate e ingiustificate". In particolare dice: "con specifico riferimento al requisito dell'iscrizione all'albo professionale degli avvocati, esso appare discriminatorio e non giustificato".

Grazie a Pierfrancesco Maistrello per averlo segnalato agli Idraulici della privacy.

****

13- Privacy: NIST privacy framework

Avevo visto la notizia in giro, ma l'ho guardato grazie all'insistenza di Giancarlo Caroti. Si tratta del NIST privacy framework:
- https://www.nist.gov/privacy-framework.

Ho purtroppo visto confermate le mie ipotesi iniziali.

La prima riguarda la complessità: in tempi in cui molte persone devono capire cosa fare, si trovano misure le "Risk Assessment"

e "Risk Management Strategy", le cui differenze sono ovvie, ma, allo stato pratico, non utili. Questo mi intristisce di più, perché dimostra quanto sia cambiato un ente che apprezzavo tantissimo per i suoi documenti pragmatici.

Ma questo è un ulteriore effetto dell'ampliamento della platea dei "professionisti della sicurezza e della privacy": per dimostrare di essere degno di questo titolo è necessario dimostrare sempre maggiore sofisticazione, dimenticando che la semplicità è la più alta espressione di sofisticazione. Ma questo si nota anche nell'uso a sproposito del termine "ecosistema", che è sì evocativo, ma scorretto e non degno di tecnici che, soprattutto in questi casi, dovrebbero usare "sistema".

Altra causa va ricercata nel fatto che il NIST è un organismo di supporto alle organizzazioni degli Stati Uniti, solitamente più grandi di quelle europee (e infatti adesso è ENISA quella che si sta distinguendo per le cose pragmatiche).

Ad ogni modo, a parte le mie elucubrazioni, vale sempre la pena leggere questo documento. Le misure di sicurezza, per quanto complicate, possono essere di aiuto.

****

14- Privacy: Ispezioni GDPR della GdF (un resoconto)

Alberto Bonato mi ha reso partecipe di alcune ispezioni relative al GDPR condotte dalla Guardia di finanza..

Intanto è riuscito a prendere appunti sulla check list usata, che riporto:
1) struttura ed organizzazione della società;
2) titolarità dei trattamenti;
3) distribuzione delle funzioni;
4) tipologia e natura dei dati (inclusi videosorveglianza e dati biometrici);
5) modalità di acquisizione dei consensi;
6) numero degli interessati;
7) registro dei trattamenti;
8) responsabili (esterni);
9) DPO;
10) lista dei soggetti autorizzati, istruzioni fornite e loro formazione, con messa a disposizione delle eventuali nomine ad incaricati);
11) periodo di conservazione dei dati personali (oppure i criteri);
12) procedure per i diritti degli interessati;
13) comunicazione di dati a terzi, presupposti di legittimità, categorie dei soggetti destinatari e finalità del trattamento dei destinatari;
14) modalità con cui è fornita l'informativa;
15) misure tecniche e organizzative;
16) eventuali certificazioni.

Sono un po' perplesso sul 10, ma si tratta di una check list, non di un requisito.

Il 15, a sua volta, si suddivide in:
- eventuale pseudo-anonimizzazione e cifratura;
- capacità di assicurare riservatezza, integrità e disponibilità;
- capacità di ripristino in caso di incidente fisico o tecnico;
- procedura per testare, verificare e valutare regolarmente le misure;
- principali applicazioni;
- controllo accessi (userid e password; strong authentication);
- audit interni e presso responsabili;
- eventuali alert sui sistemi;
- eventuale backup.

Si noti come siano importanti backup e controllo accessi.

In merito al punto 12 sui diritti degli interessati, la GdF ha approfondito le procedure per dare modo all'interessato di esercitare i propri diritti, chiedendo anche se erano state predisposte procedure automatizzate o cartacee

modulistica che l'interessato potesse compilare. Ma, come dice Alberto, "si è trattato di un confronto tutto verbalizzato e che poi seguirà risposta dal Garante".

Cesare Gallotti

Da osservare che hanno chiesto una relazione sul sistema informatico e hanno anche chiesto di accedere ai database per verificare la corrispondenza con il registro ai trattamenti.

In merito ad aziende con trattamento di dati sanitari, si sono soffermati sulla figura del DPO, chiedendo come il titolare fosse in grado di provare la effettiva attività del DPO. Hanno anche chiesto se esistesse una procedura "per tenere traccia dei problemi inerenti il trattamento di dati personali", ossia sulla gestione del registro delle violazioni.

I controlli hanno avuto durata tra i 3 e 4 giorni, con inizio verso le 9 del mattino e chiusura verbali intorno alle 22/23 di notte.

Ho chiesto ad Alberto come si fossero comportati gli ispettori e mi ha detto che si sono dimostrati gentili, corretti e professionali. Ho pensato che invece alcuni auditor ISO si comportano in modo ben diverso e sono contento di sapere che le nostre forze dell'ordine si siano dimostrate inappuntabili.

****

EONL (End-of-newsletter :-)