Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – MARZO 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

****

01- Privacy: Linee guida sulla notifica di violazione dei dati personali

Franco Ferrari di DNV GL mi ha segnalato la pubblicazione delle "Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01)" del WP Art. 29:
- http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

Sono molto importanti, perché stabiliscono un punto di riferimento autorevole per capire quali eventi vanno notificati al Garante e agli interessati.

Franco Ferrari mi ha anche segnalato un articolo di Adalberto Biasotti cheriassume la linea guida:
- https://www.puntosicuro.it/security-C-124/privacy-C-89/pubblicata-la-linea-guida-sulla-notificazione-in-caso-di-violazione-dei-dati-AR-17875/.

****
02- GDPR e legittimo interesse

Pierfrancesco Maistrello (che ringrazio) mi ha segnalato la seguente pubblicazione dal sito di IAPP e dal titolo "Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation":
- https://iapp.org/media/pdf/resource_center/DPN-Guidance-A4-Publication.pdf.

Mi pare molto interessante ed ecco i miei appunti:
- il considerando 47 prevede che il marketing diretto possa essere considerato (in certe circostanze) come trattamento di legittimo interesse per il titolare (sembrerebbero inclusi i casi in cui il "commerciale di fiducia" chiama ogni tanto il cliente; rimane sempre attivo il diritto di opposizione dell'interessato);
- trattamenti svolti nel legittimo interesse del titolare possono avere le seguenti finalità: prevenzioni di frodi, trasmissione di dati dei dipendenti all'interno di un Gruppo aziendale, sicurezza informatica, audit interni o ad altre organizzazioni, mantenere il nome delle persone che hanno chiesto la cancellazione dei propri dati personali (anche se qui si ha un riferimento circolare), registrazione delle attività (p.e. in un gestionale o per il check-in in un hotel, web analytics;
- altri esempi del documento non mi convincono per niente.

****
03- Privacy: Circolare INL sulla videosorveglianza e lavoratori

Paolo Clavi mi ha segnalato questo articolo relativo ad una recente circolare dell'Ispettorato Nazionale del Lavoro (INL) in materia di videosorveglianza:
- http://www.dottrinalavoro.it/notizie-c/inl-installazione-e-utilizzazione-di-impianti-audiovisivi.

A mio parere l'articolo è esaustivo e riassume il contenuto della circolare.

Paolo mi scrive: "introduce un principio assolutamente innovativo: la possibilità di non indicare l'esatta posizione ed il numero delle telecamere da installare, tenuto conto che il layout degli uffici potrebbe cambiare nel tempo e costringerebbe ad onerosi

aggiornamenti della pratica. Resta fermo il fatto che le riprese effettuate devono essere coerenti e strettamente connesse con le ragioni legittimanti il controllo e dichiarate nell'istanza. In fondo è un po' un atteggiamento in sintonia con il GDPR e il principio di accountability: la cosa importante è rispettare i principi, sulle modalità si lascia all'azienda la scelta di quelle opportune.

Il testo contiene poi altre interessanti innovazioni, come la mancata necessità della richiesta di autorizzazione in caso di installazione di telecamere in zone esterne estranee alle pertinenze della ditta (es. il suolo pubblico, anche se antistante alle zone di ingresso all'azienda), nelle quali non è prestata attività lavorativa. In fondo, se l'accordo sindacale o l'autorizzazione DTL derivano dalla necessità di informare e tutelare i lavoratori, quando i lavoratori si trovano all'esterno dell'azienda si trovano nelle stesse condizioni di qualsiasi cittadino, per i quali sono sufficienti cartelli informativi ed eventuale esercizio dei diritti di accesso ai dati".

Ci sono anche altri aspetti. Quello che a me colpisce di più è la possibilità di inquadrare direttamente l'operatore, ma solo per tutela della "sicurezza del lavoro" o del "patrimonio aziendale". Questa finalità, però, potrebbe sconfinare facilmente nell'uso delle inquadrature per controllare le prestazioni dei lavoratori (il call centre che decurtava un'ora di stipendio a chi andava in bagno è notizia recente: http://www.corriere.it/cronache/cards/centralinisti-call-center-pagati-33-centesimi-l-ora/finta-busta-paga_principale.shtml).

****

04- Articolo sulle certificazioni privacy

Segnalo questo articolo di ICT Security Magazine dal titolo "GDPR perché certificarsi - La vera ragione economica e il fenomeno della selezione avversa". Ho trovato qualcuno di più critico di me.
- https://www.ictsecuritymagazine.com/articoli/gdpr-perche-certificarsi-la-vera-ragione-economica-fenomeno-della-selezione-avversa/.

****

05- Nuova privacy per telemarketing (precisazione 2)

Avevo segnalato il nuovo provvedimento normativo su privacy e telemarketing:
- http://blog.cesaregallotti.it/2018/02/nuova-privacy-per-telemarketing.html

Alessandro Borgese degli Idraulici della privacy mi ha segnalato che "manca ancora il decreto attuativo e pertanto le novità introdotte vedranno la luce tra un po'". Lo dimostra inviandomi questo articolo di Repubblica del 2 febbraio:
- http://www.repubblica.it/economia/2018/02/02/news/difese_contro_il_telemarketing_la_rivoluzione_puo_attendere-187679069/.

Riassumo dicendo che "ad ora sono in vigore solo alcune delle novità: l'obbligo del telemarketer a chiamarci con un numero in chiaro e la corresponsabilità dell'azienda committente della campagna telefonica illecita (finora invece era sanzionabile solo l'agenzia esecutrice di quest'ultima)". E che "il punto centrale è il nuovo registro delle

opposizioni, una delle novità che devono aspettare il decreto attuativo per entrare in vigore. Il nuovo registro include anche i numeri riservati e quelli cellulare".

****

06- Direttiva NIS - Bozza di decreto italiano

Franco Ferrari di DNV GL mi ha segnalato questo interessante articolo dal titolo "Attuazione della Direttiva NIS, lo stato dopo lo schema di decreto legislativo":
- https://www.agendadigitale.eu/sicurezza/attuazione-della-direttiva-nis-lo-lo-schema-decreto-legislativo/.

Dopo tutto il parlare di GDPR, è bene ricordare che le Direttive devono essere "tradotte" dagli Stati membri in una Legge nazionale. In Italia, la "traduzione" avviene attraverso Decreti legislativi.

La Direttiva 2016/1148 (cosiddetta "NIS") impone un elevato livello di sicurezza (basato su un'analisi del rischio) delle reti e dei sistemi informatici delle organizzazioni che operano in alcuni settori (energia, trasporti, banche, mercati finanziari, sanità, fornitura e distribuzione di acqua potabile e infrastrutture digitali; nonché motori di ricerca, servizi cloud e piattaforme di commercio elettronico).

Il Consiglio dei Ministri italiano ha recentemente pubblicato la prima bozza ("schema") di D. Lgs. di recepimento della Direttiva NIS. Quindi l'articolo commenta questa bozza. Penso quindi che sia utile cominciare ad affrontare il tema NIS, senza approfondirlo troppo, visto che le bozze potrebbero essere modificate abbondantemente.

Non commento ulteriormente, visto che l'articolo mi pare esaustivo.

****

07- Pubblicata la ISO/IEC 27103 sulla cybersecurity

E' stata pubblicata la norma ISO/IEC 27103, dal titolo "Cybersecurity and ISO and IEC Standards":
- https://www.iso.org/standard/72437.html.

Si tratta di un Technical report, non di uno standard. Esso elenca i punti chiave del NIST CSF e gli associa i controlli della ISO/IEC 27002 e di altre norme. Un po' anche per dire "guardate che questa cybersecurity è sempre stata parte del nostro lavoro".

È noto che non sono un fan delle "correlazioni": penso che ogni standard abbia un punto di vista diverso e che prima di tutto questo punto di vista vada capito. L'uso di liste di correlazione fa spesso dimenticare i diversi punti di vista e porta a lavori troppo meccanici.

****

08- Nuova ISO 31000 sulla gestione del rischio

Franco Ferrari (di DNV GL) e Gennaro Bacile (di Studio QSA) mi hanno segnalato la pubblicazione della nuova versione della ISO 31000, dal titolo "ISO 31000:2018 - Risk management — Guidelines":
- https://www.iso.org/standard/65694.html.

Gennaro, gentilmente, mi ha inviato un suo commento, che io riporto qui di seguito.

La ISO 31000:2018 non ha novità sconvolgenti rispetto alla precedente versione del 2009. L'intento della nuova versione era quello di trovare un adeguato compromesso tra esigenze di chiarezza, bisogno di approfondimento e necessità di sintesi.

In effetti, il nuovo testo si presenta non solo più conciso, ma comprende anche alcuni cambiamenti sostanziali come ad esempio l'importanza data ai fattori umani e culturali nel raggiungimento degli obiettivi di un'organizzazione e una maggiore enfasi su una più solida integrazione del "risk management" con il processo decisionale e, più in generale, all'interno di un sistema di gestione strategico e operativo.

Come Italia avevamo insistito per un approfondimento su due aspetti, relativi alla necessità di:
- considerare l'etica tra i criteri di riferimento per la valutazione dei rischi;
- chiarire meglio significato e correlazione tra i concetti di opportunità, minacce/pericoli e rischio, sui quali i punti di vista sono molto "variegati".

Dell'etica comunque non se ne parla se non sottintesa tra le righe e sui concetti di minacce e opportunità in relazione al rischio è stata fatta confusione (una nota alla definizione di rischio è stata modificata all'ultimo momento, rendendo quindi la relazione tra minacce e opportunità e rischi molto confusa e non condivisible).

Molto più interessante per numerose novità, oltre che per i due punti di cui sopra, è la revisione della IEC/ISO 31010, il cui DIS è stato approvato a metà febbraio. Nella nuova versione è previsto un diagramma di Ishikawa modificato (con indicate le classiche famiglie di cause-effetti: ambiente, materiali, fornitori, personale, processi, infrastrutture). È forse una banalità, ma comunque è un nuovo modo di pensare fuori dagli schemi (una sorta di pensiero laterale) che è frutto di un nostro contributo. La sua applicazione è risultata piuttosto interessante ed apprezzata da chi ci ha provato.

****

09- Nuova edizione della ISO 22300 (definizioni per la continuità)

Franco Ferrari di DNV GL mi ha segnalato la pubblicazione della nuova versione della ISO 22300, dal titolo "ISO 22300: 2018 - Societal security - Terminology":
- https://www.iso.org/standard/68436.html.

Ne ho parlato con Gennaro Bacile. Anche lui ha trovato ridicola la definizione di activity (un insieme di processi) e di process (un insieme di attività), in ovvio riferimento circolare. C'erano anche nella ISO 22301:2012 e purtroppo la definizione di activity non è stata modificata (la definizione di process non dovrebbe esserlo, visto che stabile da numerosi anni, condivisa da tantissime norme ISO e tra le definizioni base del HLS).

****

10- Continuità operativa: le definizioni fondamentali

Articolo mio dal titolo "Continuità operativa: le definizioni fondamentali":
- https://www.ictsecuritymagazine.com/articoli/continuita-operativa-le-definizioni-fondamentali/.

Segnalo anche questo articolo, che mi è stato segnalato da Claudio Sartor su Twitter dal titolo "Il Grande Malinteso – Business Continuity e Cyber Resilience" (lo trovo un po' troppo generico, ma è interessante):
- https://www.ictsecuritymagazine.com/articoli/grande-malinteso-business-continuity-cyber-resilience/.

****

11- Due lezioni dai seggi

No. Non parlerò della campagna elettorale, né dei risultati. Ho solo due foto sui seggi che costituiscono due interessanti lezioni.

Lezione 1: Sviluppo e progettazione. La busta 7(R) in alto va infilata nella busta in basso:
- https://www.linkedin.com/feed/update/urn:li:activity:6379233027293265920.

Lezione 2: Capacity management. Le schede inutilizzate (in basso; sono quelle del mio seggio) vanno inserite nella busta 4(R) in alto:
- https://www.linkedin.com/feed/update/urn:li:activity:6379234134224617473.

****

12- CISCO Annual cybersecurity report 2018

Dal SANS NewsBites, riprendo la notizia della pubblicazione del "2018 Annual Cybersecurity Report" della Cisco:
- https://www.cisco.com/c/en/us/products/security/security-reports.html.

Non mi pare ci siano cose particolarmente rilevanti o innovative (a meno che qualcuno più paziente di me non me le segnali), ma sicuramente è utile saperle (ed è utile anche vedere quali di queste cose "invitano" ad usare i prodotti e servizi della Cisco, in modo

da dare loro il giusto peso).

I "major findings", infatti, sottolineano:
- la diffusione degli attacchi DDoS;
- la diffusione dello spamming;
- la pericolosità degli attacchi da parte del personale interno,
- lo sfrtuttamento dell'IoT e delle reti industriali,
- i rischi derivanti dalla numerosità di prodotti e fornitori,
- l'opportunità di migliorare la sicurezza attraverso l'outsourcing (via cloud).

****

13- Libro: La vita segreta

Segnalo questo libro dal titolo "La vita segreta: Tre storie vere dell'èra digitale" di Andrew O'Hagan:
- https://www.adelphi.it/libro/9788845932151.

Non parla di sicurezza delle informazioni (se non in modo funzionale), né di GDPR.

Però, attraverso tre storie estreme (una su Assange, un'altra su Satoshi e quella in mezzo su una persona creata solo per l'ambiente virtuale) parla di identità, bisogno di privacy, bisogno di visibilità e forse altre cose.

Lo consiglio perché mi sembra dica qualcosa a noi che ci occupiamo di informatica non solo da un punto di vista puramente tecnico, ma anche culturale, se possiamo dire così.

****

14- Libro bianco della cyber security in Italia (precisazione sul documento)

Recentemente avevo segnalato la nuova edizione del Libro Bianco: "Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici". Avevo detto che i link disponibili sul sito ufficiale (https://www.consorzio-cini.it/index.php/it/) non funzionavano e avevo fornito un link alternativo.

Giancarlo Caroti mi ha fatto notare che il link alternativo rimanda all'edizione precedente del 2015 (che fu presentato a febbraio 2016 in un evento in Sapienza a cui fece un intervento lo stesso Caroti). Giancarlo mi conferma che neanche lui riesce a rintracciare e scaricare l'edizione del 2017.

Mi scuso per l'errore e, se avrò aggiornamenti, li fornirò.