Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – OTTOBRE 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- NIST Security and Privacy Controls

Il NIST ha pubblicato l'aggiornamento della SP 800-53 "Security and Privacy Controls for Information Systems and Organizations":
- https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

Si tratta di una lettura impegnativa, visto che i controlli sono descritti da pagina 35 a pagina 393. In alcuni punti è troppo teorico, ma, rispetto ad altri, ha anche molte indicazioni pragmatiche.

Giulio Boero l'ha letta più approfonditamente di quanto abbia fatto io e mi dice che forse l'aggiornamento di maggior rilievo rispetto alla precedente edizione è l'aggiunta di alcuni controlli volti a

contrastare le nuove minacce, come p.e. quelli per la resilienza, la progettazione sicura dei sistemi, il governo della sicurezza e della privacy e della responsabilizzazione.

Giulio scrive: << Non mi piace (lo dichiaro apertamente a costo di attirarmi critiche accese) l'approccio alla protezione dei dati personali. Non è aggiungendo la parola "privacy" al titolo del documento, né tantomeno inserendo il termine "privacy" in ogni descrizione di controllo (anche in modo abbastanza opinabile) che si tratta di data protection. Confido nella sibillina frase del NIST, in coda ai punti "to do": "Control mappings to the Cybersecurity Framework and Privacy Framework (available soon)">>.

****

02- Aggiornamento dei controlli NIST per la sicurezza IT nel manifatturiero

Il NIST ha aggiornato il proprio "Cybersecurity Framework Manufacturing" ed è alla versione 1.1:
- https://csrc.nist.gov/publications/detail/nistir/8183/rev-1/final.

Avrei preferito qualche approfondimento in più sulle specificità del settore manifatturiero (il cosiddetto OT) rispetto all'informatica cosiddetta d'ufficio, ma già questa pubblicazione è molto utile.

****

03- NISTIR 8286 sull'integrazione tra Cybersecurity Enterprise Risk Management

Il NIST ha pubblicato il documento NISTIR 8286 "Integrating Cybersecurity and Enterprise Risk Management (ERM)":
- https://csrc.nist.gov/publications/detail/nistir/8286/final.

Stavo per classificarlo come "troppo verboso e senza elementi nuovi (incluso un calcolo del rischio "quantitativo" che quantitativo non è)". Ma arrivato a pagina 55, ecco un esempio di "Notional Enterprise Risk Register": una tabella in cui sono elencati i rischi identificati, senza che siano esaustivi e con un calcolo semplicissimo per il livello di rischio ("Exposure rating").

Questo esempio ci mostra come una valutazione del rischio possa essere molto semplice, senza dover necessariamente usare software o calcoli complessi. Ovviamente ritengo scorretto l'approccio "non esaustivo" per l'identificazione dei rischi, ma penso sia utile considerare questo esempio.

****

04- Guide to Business Continuity & Resilience di Protiviti

Protiviti ha pubblicato una "Guide to Business Continuity & Resilience":
- https://www.protiviti.com/US-en/business-continuity-faq.

Non mi ha pienamente soddisfatto perché non è abbastanza pragmatica (con esempi e modelli) per essere uno strumento veramente utile e spazia troppo tra argomenti di base e considerazioni avanzate per essere utile a chi la materia la conosce già. La struttura a domande e risposte rende poi il tutto poco chiaro.

Però ci sono alcune cose interessanti, in particolare per i settori considerati (servizi finanziari, sanità, informatica, commercio al dettaglio, energia, manifattura e pubblica amministrazione).

****

05- Minacce e attacchi: Ospedale attaccato da ransomware e morte di una donna

La notizia è circolata in questi giorni. Sandro Sanna me l'ha segnalata per primo con questo articolo:
- https://www.repubblica.it/tecnologia/sicurezza/2020/09/18/news/germania_donna_muore_durante_attacco_ransomware_all_ospedale-267735262/.

E' sicuramente difficile immaginare, progettare e realizzare, per infrastrutture di questo tipo, un piano di continuità operativa che permetta di proseguire le attività critiche anche in assenza di sistemi informatici e di attacchi ransomware. Però non viene neanche citato e questo mi lascia molto perplesso.

Questo articolo, in inglese, mi sembra decisamente più approfondito del precedente:
- https://www.scmagazine.com/home/security-news/ransomware/lessons-from-the-ransomware-death-cyber-emergency-preparedness-critical/.

****

06- Minacce e attacchi: Uso improprio di Excel e perdita di dati

Pietro Calorio degli Idraulici della privacy ha condiviso questa notizia:
- https://www.theguardian.com/politics/2020/oct/05/how-excel-may-have-caused-loss-of-16000-covid-tests-in-england.

Riassunto: la sanità inglese consolidava i dati dei test COVID-19 su un foglio Excel. Però Excel può trattare un massimo di un milione circa di righe (65mila nelle vecchie versioni). Il risultato è che molte righe sono state perse dal foglio usato.

Un bell'esempio di perdita di integrità.

****

07- Guida NSA per i prodotti di autenticazione a più fattori

NSA ha pubblicato una guida dal titolo "Selecting Secure Multi-factor Authentication Solutions":
- https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2356020/nsa-releases-cybersecurity-guidance-selecting-and-safely-using-multifactor-auth/.

E' sicuramente molto tecnica e le analisi non si concludono con un giudizio sintetico. Per questo va letta con molta attenzione.

Ricordo che il ricorso a strumenti di MFA è sempre più necessario, soprattutto (ma non solo!) per chi ha ampi privilegi sui sistemi e può accedervi da remoto. Purtroppo queste tecnologie sono ancora sottovalutate da molti.

****

08- Libro sulla ISO 9001:2015

Un mio cliente (Cinzia Alberici di OCS Alberici) mi ha segnalato un buon libro per capire come funziona la ISO 9001:2015. Mi piace segnalarlo anche se dopo quasi 5 anni dalla pubblicazione. Il libro si intitola "UNI EN ISO 9001:2015: Linea guida operativa":
- https://www.edizionidelfaro.it/libro/uni-en-iso-90012015.

Si tratta di un libro molto pragmatico e utile. Forse la parte di pianificazione (in particolare la gestione del rischio relativo all'efficacia del sistema di gestione) è troppo poco approfondita, ma sicuramente questo è un ottimo libro per chi vuole iniziare a conoscere la ISO 9001, essenziale anche a chi si occupa di sicurezza delle informazioni e privacy (molti principi della qualità vanno applicati anche in questi ambiti).

****

09- Sentenza sul controllo genitori su cellulari e pc degli adolescenti

Si è diffusa in questi giorni la notizia della sentenza del Tribunale di Parma che dispone che spetta a entrambi i genitori monitorare con costanza smartphone e pc dei figli minorenni anche attraverso filtri di controllo. Ringrazio Luca de Grazia per avermi segnalato la notizia.

Un articolo di giornale:
- https://www.ilsole24ore.com/art/i-genitori-devono-controllare-smartphone-e-pc-figli-adolescenti-ADvHxLn.

Un articolo di stampo più legale:
- https://www.studiocataldi.it/articoli/39789-i-genitori-devono-controllare-pc-e-smartphone-dei-figli-adolescenti.asp.

Non penso che il monitoraggio costante sia una buona strategia educativa, né penso che sia compito di un tribunale imporre strategie educative. E comunque tutto ciò non rientra tra le mie competenze professionali (anche se fare il genitore è comunque una professione).

Mi sembra però una sentenza molto discutibile perché impone misure di monitoraggio (meno efficaci di quelle di prevenzione) e una forma di educazione volta ad abituare i giovani alla vigilanza continua. Roba tipica dei nostri tempi e che continuo a non condividere.

****

10- Privacy: Provvedimento del Garante verso l'Azienda Ospedaliera Cardarelli di Napoli

Segnalo due provvedimenti del Garante tra loro correlati. Uno verso l'Azienda Ospedaliera Cardarelli di Napoli:
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9461168.

L'altro verso il fornitore della stessa AO:
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9461321.

Per un riassunto, si può vedere l'articolo nella newsletter del Garante del 30 settembre 2020:
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9461344.

Queste sentenze mi interessano perché sono sanzionati:
1- l'uso di informativa "troppo breve";
2- l'uso scorretto della base giuridica del consenso (in questo caso, direi, il consenso è stato usato per il principio "non si sa mai", ma questo non è lecito);
3- l'attribuzione al fornitore di ruolo di titolare, mentre invece è responsabile (purtroppo molti fornitori di servizi si impongono come titolari dei trattamenti, nonostante siano da considerare come responsabili);
4- l'assenza nella documentazione contrattuale delle clausole richieste dall'art. 28 del GDPR (pratica molto diffusa quando la "nomina a responsabile" è vista come cosa a parte rispetto al contratto, a mio parere anche per colpa dei consulenti privacy che troppo spesso cercano di affermarsi come "speciali" e scollegati dal resto delle attività dell'organizzazione);
5- la conseguente assenza di istruzioni dal titolare al responsabile per assicurare la sicurezza dei dati.

Notare infine che al titolare è stato ordinato di pagare una multa di 80 mila euro, mentre al responsabile, anche perché ha agito in modo non previsto dal GDPR, una multa di 60mila euro. Questo dovrebbe ricordare che imporsi come titolare non è sempre la scelta più opportuna.

****

11- Privacy e GDPR: Linee guida EDPB su titolare e responsabile - Un commento

Avevo segnalato la pubblicazione delle linee guida EDPB su titolare e responsabile (http://blog.cesaregallotti.it/2020/09/linee-guida-edpb-su-titolare-e.html).

Segnalo questo articolo più analitico:
- https://www.key4biz.it/titolari-contitolari-responsabili-cosa-indicano-le-nuove-linee-guida-edpb/322063/.

****

12- Privacy e GDPR: Consenso e legittimo interesse

Ultimamente sto notando, insieme agli Idraulici della privacy, molti siti web che chiedono il consenso per gli interessi legittimi del titolare (in realtà questo viene proposto come possibile "opposizione al legittimo interesse").

Questi siti elencano delle finalità per cui è richiesto il "normale" consenso e poi delle finalità per cui è dichiarato l'interesse legittimo e per le quali è richiesto all'interessato di esprimere la propria volontà di opporsi (il tipico "opt-out" al legittimo interesse).

Ricordo che consenso e interesse legittimo sono due delle basi legali per cui un titolare può trattare i dati. Se la base legale per una certa finalità è l'interesse legittimo allora, ovviamente, non deve essere richiesto il consenso. Su questo, in effetti, il GDPR presenta due meccanismi tra loro potenzialmente in conflitto.

Esempi che ho recentemente verificato sono https://www.corriere.it/ (Italia), https://www.theguardian.com/international (UK) e https://www.computerweekly.com (USA).

Almeno in alcuni casi, concordo con Pietro Calorio degli Idraulici della privacy secondo cui questa è una pratica per nascondere alcune richieste di consenso e per rendere più difficile il rifiuto, visto che, per questi consensi al legittimo interesse, non viene mostrato il pulsante "rifiuta tutto", come invece

succede per i consensi "normali". Queste piattaforme che permettono questo giochino non possono considerarsi privacy by design perché non consentono un trattamento corretto.

Ringrazio ulteriormente Pietro per avermi segnalato un mio grande errore di interpretazione del GDPR (spero di aver corretto per bene).

****

13- Privacy e GDPR: Privacy accountability framework dell'ICO

Antonio Salis (ringrazio) mi ha segnalato l'Accountability framework dell'ICO (il Garante inglese):
- https://ico.org.uk/for-organisations/accountability-framework/introduction-to-the-accountability-framework/.

Devo dire che ad un approccio superficiale non è chiarissimo come usarlo, ma ecco qui:
- ci sono alcune pagine web (menu a sinistra) con spiegati gli aspetti da considerare, ognuno con dei "modi per soddisfare le aspettative" e delle domande a cui si dovrebbe rispondere "sì";
- in un'altra pagina (https://ico.org.uk/for-organisations/accountability-framework-self-assessment/) è possibile scaricare un Excel (Accountability tracker) in cui rispondere ai "modi per soddisfare le aspettative".

A me lascia perplesso: troppe domande che si concretizzano, in realtà, su poche cose e, sui punti meno ovvi, non presentano esempi o spiegazioni per i non addetti. Insomma, mi sembra un altro ennesimo modo di ripresentare il GDPR, senza però reale utilità. Non vorrei essere io troppo schizzinoso.

****