Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – GIUGNO 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

****
00- Richiesta di aiuto (modelli in Word)

Con gli Idraulici della privacy vorremmo pubblicare a breve un libro sul GDPR e io ho l'incarico di impaginarlo. Però non ho un buon modello in Word per un libro di questo genere (potrei convertire tutto in LaTeX, ma sarebbe un lavoraccio).

Chiedo quindi se qualcuno dei miei lettori può aiutarmi.

****

01- Considerazioni sul rischio

Ho letto un articolo sulla percezione del rischio COVID-19 e ho pensato che alcuni spunti possono essere di interesse anche a chi si occupa di sicurezza delle informazioni e, in generale, di rischi. L'articolo ha titolo "La società a rischio zero - Abbiamo raggiunto l'immunità di gregge psicologica?":
- https://www.linkiesta.it/2020/05/rischio-coronavirus-paura/.

Innanzi tutto l'articolo ribadisce il concetto di accettabilità del rischio. Qui la scala è notevolmente più ampia (si parla di migliaia di vite umane) di quanto normalmente è richiesto alle organizzazioni che analizzano il rischio di sicurezza delle informazioni, dei progetti, di qualità o di efficacia di un sistema di gestione. Però è importante riflettere sull'accettabilità del rischio anche in altri ambiti.

Altro punto è sintetizzato dalla frase "La percezione del rischio è un fenomeno sociale" e dal grafico che riporta quanto alcuni rischi sono percepiti e quanto sono invece oggettivamente pericolosi.

Aggiungo che è interessante osservare come a inizio marzo, quando i numeri del COVID-19 erano ancora ipotetici, in giro a Milano c'era pochissima gente; mentre adesso, dopo più di 30.000 morti, le strade sono piene. E' evidente che la preoccupazione pochi mesi fa era palpabile mentre oggi genera insofferenza. Sono cose, penso, da considerare anche in ambito aziendale (fatte le dovute proporzioni) quando si stabiliscono le misure per affrontare il rischio: quelle più che accettabili oggi potrebbero essere viste con fastidio (e quindi attuate male) tra pochi giorni.

Un altro spunto riguarda il sondaggio, sempre in merito al COVID-19, fatto tra studenti di medicina e di economia. Esso ci dice che i primi sono molto più prudenti dei secondi in merito alla riapertura. Questo può farci ragione sul fatto che i consulenti (interni ed esterni) e gli auditor i vari specialisti di sicurezza e privacy sono sempre molto più prudenti dei dirigenti di un'organizzazione, ma non necessariamente hanno ragione. Credo sia la dimostrazione del fatto che la ragione sia nel mezzo e sia sempre necessario mediare tra il rigore proposto dagli specialisti e una maggiore rilassatezza propugnata dai loro interlocutori. Per fare un esempio, tra chi propone di avere password di almeno 16 caratteri e chi non le vorrebbe proprio, la mediazione degli 8 caratteri è proprio quella che viene incontro ai due punti di vista che necessariamente devono venirsi incontro).

****

02- Mio articolo sulla scuola e il falso mito del "tool"

Avevo già scritto una breve cosa su come la scuola abbia affrontato male, da un punto di visto informatico, l'emergenza COVID-19. Ho scritto quindi un articolo che mi è stato pubblicato con il titolo "Shock digitale per la scuola, smontiamo il falso mito del tool":
- https://www.agendadigitale.eu/scuola-digitale/shock-digitale-per-la-scuola-smontiamo-il-falso-mito-del-tool/.

Ovviamente commento solo alcuni problemi di tipo informatico (ovviamente ne vedo altri, ma, come il pasticcere milanese, mi limito al mio mestiere).

****

03- Linee guida AgID per la sicurezza nel procurement ICT

Franco Vincenzo Ferrari di DNV GL mi ha segnalato la pubblicazione delle "Linee guida: La sicurezza nel procurement ICT" di AgID:
- https://trasparenza.agid.gov.it/archivio28_provvedimenti-amministrativi_0_122261_725_1.html.

A parte l'italiano lacunoso ("eleggibile" per tradurre malamente l'inglese "eligible") o dimenticato ("procurement" al posto di "approvvigionamento"), il documento è interessante.

All'inizio della lettura mi sembrava riportare le solite cose talmente vaghe da essere inutili (promuovere competenza e consapevolezza, raccogliere buone prassi e esperienze, stabilire ruoli e responsabilità, effettuare una ricognizione dei beni e servizi informatici, classificare i beni e i servizi informatici). Poi, misura dopo misura, emergono cose più precise e, a mio parere, utili. Rimane un documento "di base" con alcune cose solo teoriche, ma anche di questi documenti c'è bisogno.

****
04- ISO/IEC 21964 sulla distruzione dei supporti - Precisazioni

Avevo scritto sulle ISO/IEC 21964 sulla distruzione dei supporti:
- http://blog.cesaregallotti.it/2020/05/isoiec-21964-sulla-distruzione-dei.html.

Michele Tassinari, che ringrazio, mi ha segnalato che l'uso dei queste norme in ambito TISAX è già prescrittivo.

In quel caso, la norma di riferimento è la DIN 66399 (la ISO/IEC 21964 è il recepimento della DIN 66399). Però lo schema rimane aperto anche per altri standard.

Nelle 2 norme sono previsti 7 livelli di distruzione.

Per la TISAX, è richiesto il livello 4 per i dati confidenziali e il livello 5 per i dati segreti.

Sandro Sanna, in merito alla mia previsione che questa norma sarà usata per certificare prodotti o processi, mi informa che questo sta già succedendo con la DIN 66399 (ossia la norma che è stata recepita come ISO/IEC 21964). Mi ha quindi inviato un link con un esempio:
- https://www.reisswolf.com/en/reisswolf/certifications/din-66399/.

Sandro poi mi segnala che le norme DIN sono già usate in alcune norme. In particolare mi segnala la Decisione (UE, Euratom) 2019/1961, in particolare l'articolo 42 dove indica le modalità di "Distruzione e cancellazione periodiche di informazioni CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET":
- https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32019D1961.

****
05- Minacce e attacchi: Chiuso il sito del Gutenberg Project

Segnalo questo articolo dal titolo "La Procura di Roma ha bloccato l'accesso a Project Gutenberg, la più grande biblioteca di internet":
- https://thesubmarine.it/2020/05/25/procura-roma-bloccato-accesso-project-gutenberg/.

A parte il mio fastidio personale perché l'ho usato per leggere alcuni capolavori (e anche cose noiose, per la verità), penso che la notizia metta in luce alcuni problemi di Internet e, potenzialmente, di sicurezza delle informazioni e continuità (senza voler estendere oltre queste riflessioni): la scelta di un unico giudice può comportare l'inaccessibilità di un sito di pubblica utilità. Oggi è toccato ad un sito utile, ma non critico; domani chissà.

****

06- Minacce e attacchi: Attaccato l'ospedale San Raffaele... forse

Interessante questa notizia: Lulzsec e Anonymous dicono di aver bucato la rete del San Raffaele di Milano a metà marzo. Il San Raffaele nega. Vedremo come andrà a finire. Lancio una mia ipotesi: la data mi suggerisce che tutti (inclusi i referenti dell'IT) al San Raffaele fossero troppo occupati sul COVID-19 e la segnalazione è stata dimenticata. Forse non è andata veramente così, ma forse questo sarà quello che diranno.

Solitamente non fornisco notizie di attacchi perché non forniscono informazioni veramente utili. Qui invece penso che sia un caso interessante da monitorare.

Segnalo quindi l'articolo "Cosa sappiamo del data breach all'ospedale San Raffaele di Milano":
- https://www.wired.it/internet/web/2020/05/22/san-raffaele-lulzsec-anoymous/.

****
07- Minacce e attacchi: Mio articolo su Idiot wind

Tempo fa avevo scritto una cosa breve su un colpo di vento che aveva sparso i documenti di un'azienda. Ho approfondito un po' la questione e ne ho fatto un articolo, pubblicato da key4biz:
- https://www.key4biz.it/idiot-wind-bob-dylan-puo-aiutare-nella-valutazione-del-rischio-aziendale/307656/.

****
08- Tecnologia: Zoom e la crittografia a pagamento

Zoom ha deciso che le video conferenze saranno cifrate solo per i clienti a pagamento:
- https://www.wired.com/story/zoom-end-to-end-encryption-paid-accounts/.

L'articolo suggerisce di biasimare la scelta di Zoom. Altri, in particolare gli editor del SANS NewsBites, sono meno critici perché ritengono che anche altri parametri siano da considerare, come per esempio la sicurezza dell'interfaccia client. In questo caso, Zoom permette conferenze con molti partecipanti, mentre altri strumenti limitano il numero di partecipanti.

Questa è una questione da studiare con attenzione. Va però detto che alcune soluzioni apparentemente più sicure sono anche più instabili.

****
09- Tecnologia: NIST NISTIRs 8259 e 8259A sull'IoT

Il NIST ha pubblicato due documenti:
- NISTIR 8259A dal titolo "IoT Device Cybersecurity Capability Core Baseline"; URL https://csrc.nist.gov/publications/detail/nistir/8259a/final;
- NISTIR 8259 dal titolo "Foundational Cybersecurity Activities for IoT Device Manufacturers"; URL https://csrc.nist.gov/publications/detail/nistir/8259/final.

Li ho guardati velocemente e mi sembra siano troppo generali.

****

10- Aggiornamento certificazioni eIDAS

Andrea Caccia, che ringrazio molto, mi ha segnalato la nuova Circolare tecnica DC N° 05/2020 di Accredia:
- https://www.accredia.it/documento/circolare-tecnica-dc-n-05-2020-circolare-per-laccreditamento-a-fronte-del-regolamento-europeo-910-2014-eidas/.

Essa estende la certificazione a tutti i servizi fiduciari previsti dal regolamento eIDAS e fornisce un aggiornamento di tutti i riferimenti agli standard ETSI pertinenti.

****

11- Privacy, eIDAS e il piano cessazione per (tutti) i servizi

Un argomento spesso non trattato è il piano cessazione dei servizi informatici (e non solo). Un piano in cui prevedere alcune azioni di comunicazione ai clienti e utenti, di passaggio o meno delle consegne ad altro fornitore, di cancellazione o restituzione dei dati.

Un settore in cui questo piano è necessario è quello dei servizi fiduciari eIDAS (firma digitale e compagnia, per intenderci) e anche quello di conservazione dei documenti. Per questo, ENISA nel 2017 aveva pubblicato delle linee guida dal titolo "Guidelines on Termination of Qualified Trust Services":
- https://www.enisa.europa.eu/publications/tsp-termination.

AgID aveva pubblicato una bozza per discussione delle linee guida per il piano di cessazione del servizio di conservazione:
- https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2019/11/22/consultazione-linee-guida-il-piano-cessazione-del-servizio-conservazione.

Il Garante privacy ha segnalato alcune carenze:
- https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9347287.

Ripeto: sono questioni da considerare per tutti i servizi e quindi vale la pena approfondirle.

****

12- Privacy: assicurazioni (e non solo) sono titolari

Il Garante privacy ha risposto a un quesito relativo al ruolo soggettivo delle compagnie di assicurazione. La risposta è nel documento "Ruolo soggettivo dell'impresa assicurativa nell'ambito dei bandi di gara per l'affidamento dei servizi assicurativi":
- https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9169688.

In sostanza, se un'organizzazione stipula assicurazioni per il proprio personale, l'assicuratore è da considerare titolare del trattamento. Questo perché l'organizzazione non può creare assicurazioni e quindi questo trattamento non può essere considerato come esternalizzato.

Possiamo quindi dedurre che lo stesso discorso valga anche per le banche e per gli organismi di certificazione, visto che un'organizzazione (a meno gli ovvi casi in cui sia essa stessa una società di assicurazioni, una banca o un organismo di certificazione) non può autonomamente erogare questi servizi e quindi l'assicurazione, la banca, l'OdC non trattano i dati "per conto" (o in qualità di "delegato") del titolare.

Ovviamente questa risposta del Garante non permette di risolvere altri casi "complessi", come quelli relativi alle singole persone (p.e. medico del lavoro) o società particolari come i fornitori di connettività o le poste. Però è già un ottimo spunto.

Si osserva anche che il caso delle assicurazioni (che io ho esteso a banche e OdC) riguarda un mercato molto regolamentato e vigilato. Pertanto anche le misure di sicurezza sono regolamentate e vigilate. La

stessa cosa non si può dire per gli altri settori, dove non c'è regolamentazione stringente e relativa vigilanza, e io ribadisco la mia convinzione: anche nel caso di trasferimento ad altro titolare, il titolare mittente deve avere garanzie precise in merito al livello di sicurezza fornito dal destinatario e non può limitarsi a dire che il destinatario è titolare e quindi sono fatti suoi, visto che può scegliere tra diverse opzioni.

Ringrazio Diego Padovan per aver segnalato questa notizia agli Idraulici della privacy.

****

13- Privacy: DPIA per Immuni

Il Garante della privacy ha pubblicato un documento dal titolo "Valutazione d'impatto sulla protezione dei dati personali presentata dal Ministero della Salute relativa ai trattamenti effettuati nell'ambito del sistema di allerta Covid-19 denominato "Immuni" - Nota sugli aspetti tecnologici":
- https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9357972.

Al di là dell'argomento ormai trito e ritrito, penso che sia utile osservare i punti toccati per avere un'idea di come sono affrontati gli aspetti più criti da parte del Garante.

Il documento non riporta dettagli sulla DPIA, né su come è stata fatta e questo è un peccato perché sarebbe stato interessante.

Ringrazio Stefania Algerio per la segnalazione agli Idraulici della privacy.

****

14- Privacy: GDPR developer's guide del CNIL

Il CNIL (ossia il Garante privacy francese) ha pubblicato una GDPR developer's guide:
- https://www.cnil.fr/en/gdpr-developers-guide.

Ci sono cose molto interessanti e molto puntuali, inclusi link a piattaforme, a presentazioni più dettagliate, a documenti di approfondimento.

Al momento gli approfondimenti sono disomogenei e quindi, per esempio, sono presentati gli strumenti di gestione della configurazione del software e le linee guida di codifica sicura per C e C++, ma sono accennati ma non elencati strumenti di controllo automatico del codice prima della messa in produzione.

Però il CNIL permette di contribuire e quindi credo che in qualche futura versione questi aspetti saranno ben approfonditi.

artSicuramente quello che c'è merita già un approfondimento (io ho trovato molti punti) ed è sicuramente molto di più di quanto vedo in giro.

Ringrazio Glauco Rampogna per aver segnalato questa iniziativa agli Idraulici della privacy.

****

15- Privacy: Le 7 multe più strane per aver violato la privacy e il Gdpr

Le 7 multe più strane per aver violato la privacy e il Gdpr

Glauco Rampogna mi ha segnalato questo interessante articolo dal titolo "Le 7 multe più strane per aver violato la privacy e il Gdpr":
- https://www.wired.it/internet/regole/2020/05/25/gdpr-privacy/.

Il titolo è un po' fuorviante, ma alcune cose sono interessanti, in particolare la multa per aver usato un normale cassonetto per eliminare i dati in formato cartaceo.

****
[EONL]