Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – SETTEMBRE 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.

IT Service Management News di Cesare Gallotti è rilasciata sotto licenza Creative Commons Attribution 4.0 International License (creativecommons.org/licenses/by/4.0/deed.en_GB).
Bisogna attribuire il lavoro a Cesare Gallotti con link a http://www.cesaregallotti.it/Newsletter.html.

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- Corso di perfezionamento in digiltal forensics (Milano)

Segnalo il Corso di Perfezionamento in Criminalità Informatica e Investigazioni Digitali dell'Università di Milano:
- http://www.forensics.unimi.it/.

Il bando per iscriversi scade il 25 settembre.

Io l'ho seguito anni fa e continuo a pensare sia uno dei corsi più interessanti che abbia seguito, anche se non farò mai un'analisi forense di alcun dispositivo digitale. Ma si impara a conoscere meglio la normativa vigente non solo in materia di digital forensics e alcune tecnologie: conoscenze utili a chi si occupa di sicurezza delle informazioni, sia da un punto di vista tecnico che organizzativo. Il corso, comunque, non richiede particolari competenze tecnico-informatiche.

Ah... sì: sono il presidente dell'associazione degli ex alunni (www.perfezionisti.it; siamo quasi mille), quindi sono decisamente parte in causa.

****

02- Pubblicata la ISO/IEC 27701 (già 27552) sui sistemi di gestione privacy

E' stata finalmente pubblicata la norma ISO/IEC 27552 con un nuovo numero: ISO/IEC 27701. Il titolo è sempre lo stesso: "Security techniques -- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -- Requirements and guidelines":
- https://www.iso.org/standard/71670.html.

E' già stata adottata come standard europeo (EN) e pertanto potrà anche essere indicata come EN ISO/IEC 27701.

Tutto quanto detto e scritto finora rimane valido anche dopo la numerazione. In particolare, ricordo un mio articolo:
- https://www.agendadigitale.eu/sicurezza/privacy/gestione-dei-dati-personali-ecco-le-novita-della-norma-iso-iec-27552/.

Dovrò modificare il mio VERA, ma era una cosa già in programma (ho intenzione di fare un unico VERA privacy e 27001; spero di non fare una schifezza).

PS: grazie a Sandro Sanna per avermi segnalato un refuso (avevo scritto nel titolo "17701" al posto di "27701").

****

03- Nuove ISO/IEC 20000-2 (guida) e 20000-3 (ambito)

Sono stati pubblicati due standard che "completano" la nuova versione della ISO/IEC 20000-1, norma di requisiti sulla gestione dei servizi IT.

Il primo è la guida che accompagna i requisiti ed è la ISO/IEC 20000-2:2019 dal titolo "Information technology -- Service management -- Part 2: Guidance on the application of service management systems":
- https://www.iso.org/standard/72120.html.

Il secondo è la guida per stabilire l'ambito di applicabilità dei requisiti ed è la ISO/IEC 20000-3:2019 dal titolo "Information technology -- Service management -- Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1":
- https://www.iso.org/standard/72121.html.

****

04- ISO/IEC 27102 sulle cyber-insurance

E' stata pubblicata la ISO/IEC 27102:2019 dal titolo "Information security management - Guidelines for cyber-insurance":
- https://www.iso.org/standard/72436.html.

Mi sembra sia un buon documento, che elenca le possibili cose da assicurare:
- responsabilità verso altri;
- costi per rispondere agli incidenti, inclusi i costi diretti (costi di notifica, per il personale, per i consulenti) e indiretti per la perdita di informazioni e quelli per la perdita di immagine;
- ricatti;
- interruzioni delle attività;
- multe e penali per mancato rispetto della normativa vigente;
- multe e penali per mancato rispetto dei contratti;
- danneggiamenti.

Ulteriori elementi sono considerati, incluse le possibili esclusioni.

Mi paiono invece poco approfondite le parti relative alla valutazione dei controlli esistenti. Però credo che non possa essere altrimenti: in caso contrario avrebbero dovuto riscrivere le ISO/IEC 27001 e 27002.

****
05- Qualche considerazione sulla TIA-942 (e le sue certificazioni)

Recentemente ho scritto un articolo e fatto una presentazione sugli standard e le certificazioni per i data centre:
- articolo: https://www.ictsecuritymagazine.com/articoli/gli-standard-en-50600-e-iso-iec-ts-22237-per-i-data-center/;
- presentazione: http://www.cesaregallotti.it/Pubblicazioni.html.

A questo proposito Alessandro Gaspari di Euris mi ha scritto in merito alle "certificazioni" sulla TIA-942. Io nel seguito riporto quanto mi ha scritto.

La "certificazione" TIA-942 si dovrebbe in realtà chiamare "dichiarazione di conformità", visto che per la TIA non esiste un percorso di accreditamento. EPI si è inventata un "prodotto": il sito e bollino tia-942.org. TIA-942.org non è quindi un sito ufficiale TIA né la TIA riconosce alcuna Società come ente certificatore. La conformità al momento può essere rilasciata da chiunque, ma ovviamente, avendo promosso bene il servizio tia-942.org il risultato è che tutti finiscono lì.

Molto recentemente, ad agosto 2019, TIA ha lanciato uno schema di certificazione, con il supporto dell'ente di accreditamento Certac (a me ignoto):
- https://www.tiaonline.org/press-release/tia-launches-ansi-tia-942-accreditation-scheme-for-certification-of-data-centers-selects-certac-to-manage-program/.

Per quanto riguarda EPI, essa ha solo la licenza per erogare la formazione, come dichiarato nel sito ("…have entered into a licensing agreement that allows EPI to build and conduct international certified training courses for the ANSI/TIA-942 Telecommunications Infrastructure Standards for Data Centres. The courses will initially be launched in Asia, but will eventually become available to Data Centre professionals worldwide"):
- https://www.epi-ap.com/content/19/23/TIA_and_EPI_announce_Licensing_Agreement_for_ANSI/TIA-942_Training

A questo proposito, sono interessanti due articoli (precedenti però all'avvio dello schema di certificazione sopra citato):
- https://www.capitoline.org/data-centre-audit-2/tia-942-audit-and-certification/;
- https://www.linkedin.com/pulse/standards-v-update-john-booth-mbcs-cdcap/.

Per concludere, Alessandro ci ha tenuto a ricordare che ha fatto la formazione e le relative certificazioni con EPI e che le loro persone sono molto competenti con esperienze internazionali di alto livello. Il punto chiave è quindi che EPI non ha "un'esclusiva" sulle certificazioni TIA-942.

****

06- PSD2 - Pubblicazione in Gazzetta ufficiale

Avevo segnalato poco tempo fa la Direttiva PSD2, che le banche hanno sicuramente già trattato, ma che è di interesse per tutti per la richiesta di autenticazione forte fatta a tutti i negozi virtuali:
- http://blog.cesaregallotti.it/2019/06/psd2.html.

Franco Vincenzo Ferrari di DNV GL mi ha segnalato questo articolo dal titolo "Fintech, l'Italia adegua le norme alla direttiva Psd2", relativo ai soli istituti di pagamento e istituti di moneta elettronica:
- https://www.corrierecomunicazioni.it/finance/e-payment/fintech-litalia-si-adegua-alle-nuove-norme-psd2/.

L'articolo sintetizza le disposizioni di vigilanza pubblicate in Gazzetta ufficiale a luglio:
- www.gazzettaufficiale.it/eli/id/2019/08/19/19A05009/sg.

Tra l'altro, queste disposizioni si affiancano a quelle relative alle banche, di cui scrissi a luglio (io confesso di essermi un po' perso):
- http://blog.cesaregallotti.it/2019/08/aggiornamento-delle-disposizioni-di.html.

****

07- Digital content directive

Da un tweet di @Silvia_Mar_ vedo che è stata approvata la Digital content directive:
- https://ec.europa.eu/info/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/digital-contract-rules_en.

Dovrà essere recepita dagli stati membri entro 2 anni (giugno 2021).

La Direttiva riguarda il commercio elettronico di beni digitali (dalla pagina della European Commission imparo che le precedenti Direttive riguardavano il commercio elettronico di beni fisici) e permette di rispondere a problemi dei clienti finali come file musicali (o ebook o video) comprati che non funzionano su un dispositivo o software che non funzionano più. La Direttiva tratta di prodotti acquistati con denaro o anche gratuiti (spesso acquistati fornendo dati personali).

****

08- Aggiornamento delle Disposizioni di Vigilanza di Banca d'Italia

La Banca d'Italia, a luglio 2019, ha aggiornato le Disposizioni di Vigilanza per le banche (segnalazione di Enzo Ascione di Intesa Sanpaolo):
- https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/circolari/c285/index.html.

L'ultimo aggiornamento del 23 luglio 2019 riporta molte indicazioni sulla gestione, la sicurezza e la disponibilità dei sistemi informatici. A me non sembrano indicazioni particolarmente innovative, ma le ho lette molto superficialmente.

Per non impazzire e cercare i singoli cambiamenti, il file "Aggiornamento n. 28 del 23 luglio 2019" riporta solo le parti aggiornate, ossia quelle relative ai sistemi IT.

****
09- Perimetro di sicurezza cibernetica

Sono in dubbio se dare questa notizia, viste le incerte sorti del Governo, ma lo faccio per completezza. E' stato presentato un Disegno di legge sul "perimetro di sicurezza cibernetica", ossia una sorta di NIS dedicata ad altri servizi. Meglio leggere l'articolo di Corrado Giustozzi su Agenda
Digitale:
- https://www.agendadigitale.eu/sicurezza/perimetro-di-sicurezza-cibernetica-cosi-rendera-litalia-piu-cyber-protetta/.

Personalmente, oltre a deprimermi per l'uso improprio del termine "cibernetico", mi chiedo perché avere la NIS e poi questa (per non parlare del Dlgs sulle infrastrutture critiche): troppa roba e apparentemente confusa.

Dall'articolo vengo poi a sapere che è stato istituito recentemente il "Centro di valutazione e certificazione nazionale" per la valutazione dei prodotti IT, come peraltro previsto dalla Direttiva NIS. Dovremo vedere cosa succederà anche in merito a questi schemi di valutazione, visto che potenzialmente saranno numerosi e si potrà fare fatica a districarsi tra loro.

****
10- Sulle assicurazioni IT

Tommaso Assandri, mio lettore, mi ha segnalato che Consip ha assegnato una gara per dare a Sogei una copertura assicurativa sui "cyber risk".

La documentazione di gara si trova qui:
- http://www.consip.it/bandi-di-gara/gare-e-avvisi/gara-cyber-risk-ii-rischio-per-sogei.

Interessante, nella "Documentazione di gara", il documento "All. 4 Cyber Secondo rischio_DEF.pdf" perché finalmente sono riportati rischi informatici veri e propri e non solo quelli relativi a danneggiamenti fisici o furti di apparati o dispositivi.

Segnalo poi che Sogei ha dichiarato di avere ulteriori polizze:
- Frode Informatica-Infedeltà;
- RC professionale II rischio.

Sulle assicurazioni di sicurezza informatica e delle informazioni avevo scritto in precedenza con molte critiche. Penso che le critiche rimangano valide, ma almeno vedo qualcosa di

nuovo.

Tommaso Assandri mi ha anche segnalato questo articolo (ne avevo già segnalati altri 2 in precedenza) dal titolo "The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks":
- https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks.

Questo articolo, in gran parte, dice come alle aziende convenga pagare il riscatto richiesto dai ransomware e poi ricevere il rimborso dell'assicurazione, alimentando però la criminalità.

L'articolo presenta anche un'altra analisi: vista la carenza di dati reali su cui basare i calcoli necessari al bilanciamento delle polizze, risulta che le assicurazioni IT sono molto profittevoli per le compagnie di assicurazioni, visto che le loro perdite in questo settore sono solo del 35% (in altre parole: raccolgono 100 di premi e ne spendono 35 in risarcimenti).

****
11- Sviluppatori e sicurezza

Su Crypto-Gram del 15 agosto è segnalato un articolo di ZDNet dal titolo "No love lost between security specialists and developers":
- https://www.zdnet.com/article/no-love-lost-between-security-specialists-and-developers/.

Riguarda un'indagine condotta presso gli sviluppatori e i professionisti della sicurezza e Bruce Schneier riporta alcuni dati:
- il 49% dei professionisti della sicurezza (immagino quindi di estrazione sistemistica o reziaria) denuncia fatica nel rendere prioritarie le correzioni delle vulnerabilità presso gli sviluppatori;
- il 68% dei professionisti della sicurezza pensa che meno della metà degli sviluppatori sia capace di individuare le vulnerabilità nel codice prima di passarlo in ambiente di test;
- il 70% degli sviluppatori, dall'altra parte, dichiare di non riceve alcun aiuto o linea guida per scrivere codice sicuro.

Io non sono un gran sostenitore di tutte queste indagini ("survey"), ma penso che queste indicazioni siano molto interessanti.

****
12- Sicurezza dei micro-services (guida NIST)

Il NIST ha pubblicato la SP 800-204 dal titolo "Security Strategies for Microservices-based Application Systems":
- https://csrc.nist.gov/publications/detail/sp/800-204/final.

La segnalo perché recentemente vedo che questo approccio è sempre più utilizzato e quindi questa guida può essere utile.

****
13- Furto di identità con email

Da Crypto-Gram del 15 agosto 2019 segnalo questo articolo dal titolo "My job application was withdrawn by someone pretending to be me":
- https://www.bbc.com/news/business-48995846.

In poche parole: un tizio aveva fissato un appuntamento di lavoro con un'azienda, ma

qualcun altro ha creato un account gmail con il suo nome e cognome e ha disdetto l'appuntamento.

Questo per ricordarci che oggi pensiamo spesso all'indirizzo email come un "documento di identità", ma che invece non ha alcuna caratteristica di sicurezza. Questo ci ricorda anche che molti attacchi possono richiedere competenze tecnologiche pressoché nulle.

****

14- Progettare l'accessibilità dei servizi IT - Poster

Da un tweet di Daniela Quetti, riporto le sue parole: "segnalo questi bellissimi poster che vanno oltre l'accessibilità definita per legge; dovrebbero essere appesi in qualsiasi luogo in cui si progettano servizi digitali":
- https://ukhomeoffice.github.io/accessibility-posters/.

Io non tratto solo di sicurezza, ma anche di qualità e di gestione dei servizi IT e quindi questa segnalazione non è assolutamente fuori tema. Però voglio ricordare che anche chi si occupa di sicurezza deve pensare all'accessibilità anche nella sua accezione più vasta (che potrei denominare con "comodità"), visto che uno dei principi della sicurezza è il KISS: "keep it simple (and stupid)".

****

15- Sull'inutilità delle presentazioni (Power Point)

In molti negano l'utilità di Power Point e io comincio a pensare che abbiano ragione.

Intanto ecco un articolo nato osservando un concorso in cui i partecipanti dovevano replicare un articolo in una presentazione:
- https://www.inc.com/geoffrey-james/harvard-just-discovered-that-powerpoint-is-worse-than-useless.html.

I motivi per cui PowerPoint è inutile (o dannoso) è che cala l'attenzione nei partecipanti se un oratore ripete le cose già scritte (ricordo bene il corso di Algebra all'Università; tanto più che i lucidi (all'epoca si usavano quelli!) ripetevano le cose del libro) e poi le necessità di creare diapositive rende la logica del discorso carente, l'approfondimento nullo.

A mio parere non bisogna neanche esagerare nel rifiuto totale delle presentazioni (lo stesso Bruce Schneier dice che per i corsi deve far uso di presentazioni), però tutto questo fa riflettere (io però continuo a non capire quelli che fanno le offerte in PowerPoint).

****

16- Le immagini della sicurezza (da re-immaginare)

Su Crypto-Gram del 15 agosto è presente un articolo dal titolo "Wanted: Cybersecurity Imagery":
- https://www.schneier.com/blog/archives/2019/07/wanted_cybersec.html.

In poche parole: tutte le immagini e i video sulla sicurezza presentano le stesse figure (tizio con il cappuccio, tizio nel buio che smanetta su una tastiera, lucchetto) e la Hewlett Foundation ha lanciato un concorso per promuovere nuove idee:
- https://www.openideo.com/challenge-briefs/cybersecurity-visuals.

Ho letto la presentazione "Reimagining Visuals for Cybersecurity Design Research" (si trova in fondo alla pagina) e l'ho trovata molto interessante.

Io faccio presentazioni per professionisti e quindi non sono un buon caso da analizzare, però cerco di evitare le solite immagini. Ingenuamente uso mie foto che in realtà non c'entrano molto con la presentazione stessa (nella mia testa un collegamento c'è, ma molto molto tenue); ho visto che in molti non fanno proprio alcuno sforzo (quando invio articoli, li invio sempre con una mia foto che viene regolarmente cambiata, visto che "non si sa mai", con lucchetti, tizi con cappuccio o anche nuvolette) e sarebbe invece bello vedere più fantasia.

****

17- Privacy e "Non ho niente da nascondere"

Questo mese ho visto richiamata 2 volte la questione della privacy e di chi "non ha niente da nascondere".

Un primo elemento è questo articolo, ormai del 2007, di Daniel J. Solove (da un tweet di @raistolo):
- https://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565.

L'articolo, a mio parere, è vecchio e, a mio parere, non dice nulla di veramente significativo, anche perché allora alcune cose non erano state dimostrate.

Questo video di Duck Duck Go, invece, mi sembra molto più significativo (non riesco a ricostruire da chi io abbia ripreso il retweet):
- https://vimeo.com/352982792.

Per la cronaca: io uso Qwant come motore di ricerca e quasi non uso Facebook (ma uso WhatsApp e limito l'uso di Twitter e LinkedIn alle sole cose professionali), però penso che il video colga i punti salienti del perché il "non ho niente da nascondere" non è un atteggiamento condivisibile.

****

18- The DPO Handbook (del programma T4DATA)

E' stato pubblicato il "The DPO Handbook: Guidance for data protection officers in the public and quasi public sectors on how to ensure compliance with the European Union General Data Protection Regulation (Regulation (EU) 2016/679):
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9127859.

Il documento è in inglese ed è sponsorizzato dal nostro garante.

Non mi sembra aggiunga ulteriori elementi a quello che sapevamo già. Anzi: forse è un po' troppo generico.

Grazie a Glauco Rampogna per averlo segnalato agli Idraulici della privacy.

****

19- Privacy: la richiesta di consenso ai lavoratori può venire sanzionata

Mario Mosca degli Idraulici della privacy ha segnalato questa notizia dal titolo "Privacy, il consenso dei lavoratori a volte non basta":
- www.italiaoggi.it/amp/news/privacy-il-consenso-dei-lavoratori-a-volte-non-basta-2378468.

In sintesi: PWC in Grecia chiedeva il consenso per il trattamento dei dati personali dei lavoratori; questi hanno chiesto l'intervento del Garante (greco), che ha multato PWC.

L'articolo ricorda che il consenso non va chiesto ai lavoratori, in quanto sono in posizione subordinata e non lo darebbero "liberamente" come previsto dal GDPR. Questa posizione è anche nell'Opinione 2 del 2017 dell'Art. 29 WP e ovviamente prevede eccezioni (segnalo che non ho controllato se l'EDPB ha "aggiornato" questa opinione).

Questa notizia mi piace perché sconfessa ancora una volta la linea di pensiero del "non si sa mai". Questa linea, di per se stessa, non è sbagliata, ma spesso introduce un inutile sovraccarico di lavoro e pertanto va scoraggiata.

****
20- Privacy: Contitolarità dei tasti "Like" di Facebook

Luca De Grazia mi ha segnalato questa sentenza della Corte di Giustizia UE: il gestore di un sito Internet che utilizzi il pulsante «Mi piace» di Facebook può essere congiuntamente responsabile con il social network della raccolta e trasmissione dei dati personali dei visitatori del suo sito. Per contro, in linea di principio, non è responsabile del trattamento successivo di tali dati effettuato esclusivamente da Facebook.

La sentenza si trova qui:
http://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=5673263.

Mi pare che abbia un senso: un gestore del sito decide se usare o meno i tasti "Like" di Facebook e pertanto è titolare di una prima parte del trattamento e ne deve informare gli utenti (non credo debba fare di più, ma sono sempre pronto ad essere contestato). Per tutto il resto, è responsabile Facebook.

Credo che questa sentenza si debba estendere agli altri pulsanti utilizzabili sui siti (LinkedIn, Twitter, eccetera).

Questa sentenza me ne ricorda un'altra, di un anno fa, per cui un ente (o un'organizzazione, o un'azienda) sono co-titolari con Facebook per le pagine Facebook aziendali:
- http://blog.cesaregallotti.it/2018/06/informativa-per-i-cookies-dei-social.html.

Insomma: l'uso dei social network sembra materia semplice, ma non lo è.

Per quanto riguarda gli utenti, Glauco degli Idraulici della privacy ha segnalato alcune soluzioni (ho cercato di riassumere e quindi gli errori sono miei):
- Shariff (https://github.com/heiseonline/shariff), per i gestori di siti che usano comunque le funzionalità di Facebook, mantenendo la privacy degli utenti;
- Social Share Privacy (http://panzi.github.io/SocialSharePrivacy/) che abilita il caricamento del tasto solo su azione dell'utente.

****

21- Aggiornata sezione data breach del Garante

Mi hanno segnalato (privacy, please!) che è stata aggiornata la scheda informativa sulle violazioni dei dati personali del Garante:
- https://www.garanteprivacy.it/regolamentoue/databreach.

Chi è più bravo di me capirà le differenze rispetto a prima. Per intanto penso che questa pagina sia molto utile.

****

22- Garante e prescrizioni per i trattamenti dei dati "particolari"

Il Garante ha pubblicato il "Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101 [9124510]":
- https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9124510.

Riassumendo: si tratta degli obblighi per il trattamento di particolari categorie di dati personali (ex "dati personali sensibili") nei rapporti di lavoro e per scopi di ricerca scientifica e nel caso degli organismi di tipo associativo, delle fondazioni, delle chiese e associazioni o comunità religiose.

Sostituisce le precedenti autorizzazioni generali, oggi non più previste dal GDPR. Alcune di queste sono state riprese dall'attuale provvedimento, altre no.

Infine l'autorizzazione generale sul trattamento dei dati giudiziari da parte di privati, enti pubblici economici e soggetti pubblici non è "rinnovata" (anche se, a mio parere, qualche chiarimento sarebbe stato necessario, visto gli orrori che vedo in giro).