Cesare Gallotti

**********

**IT SERVICE MANAGEMENT NEWS –APRILE 2020 - FORMATO #IORESTOACASA E #ANDRÀTUTTOBENE**

**********

Newsletter mensile con novità su 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- Brevissimo editoriale**

Buongiorno. Spero stiate tutti bene, anche se forse un po' annoiati, sicuramente preoccupati per gli impatti sul lavoro (le nostre economie domestiche), forse un po' stanchi (soprattutto chi ha figli in casa).

Le prospettive sul futuro non sono sempre ottimistiche, ma sono solo previsioni e dovremo aspettare.

Intanto in questa newsletter ci sono 3 pezzi proprio su vari impatti che l'emergenza nazionale ha sulla sicurezza delle informazioni e su alcuni insegnamenti che possiamo trarne (o su alcune conferme di lezioni che già conoscevamo). Per non appesantire la lettura, li ho messi alla fine.

#AndràTuttoBene

**********

**01- Standard: ISO 22313:2020 sulla business continuity**

Franco Vincenzo Ferrari di DNV GL Business Assurance mi ha segnalato la pubblicazione della nuova versione della ISO 22313 dal titolo "Guidance on the use of ISO 22301":
- https://www.iso.org/standard/75107.html.

Non l'ho (ancora) letta e quindi non la commento.

**********

**02- Standard: Pubblicata una correzione alla ISO/IEC 27006**

Pubblicato l'Amendment 1 della ISO/IEC 27006:2015 ("Requirements for bodies providing audit and certification of information security management systems":
- https://www.iso.org/standard/77722.html.

Poca roba, di (scarso) interesse anche per gli organismi di certificazione. Piccole puntualizzazioni su cose marginali.

Più importante (mi segnala Franco Vincenzo Ferrari del DNV GL) che abbiano corretto qualche imprecisione in merito al calcolo delle giornate di audit.

Ricordo che la ISO/IEC 27006 è la norma che devono applicare gli organismi di certificazione, non le organizzazioni che intendono certificarsi.

**********

**03- Libro: IoT Security e Compliance**

E' uscito il libro "IoT Security e Compliance" della Community for Security del Clusit:
- https://iotsecurity.clusit.it.

Anche io appaio tra gli autori (e ci ho lavorato parecchio insieme agli altri).

**********

**04- Libro "Tecnologia e diritto"**

Ho finito di leggere i 3 volumi di "Tecnologia e Diritto" di informatica giuridica (il link è al solo primo volume):
- https://shop.giuffre.it/tecnologia-e-diritto-i-fondamenti-d-informatica-per-il-giurista.html.

E' un libro destinato agli studenti dell'Università di giurisprudenza e pertanto molte cose non sono esposte in modo direttamente utilizzabile dalle aziende e molti argomenti non sono di interesse per chi si occupa di consulenza alle aziende. Ma proprio qui sta l'interesse di questi libri: permettono di farsi un quadro generale dell'informatica giuridica e dei suoi temi più significativi.

Penso che proprio la capacità di avere un quadro più generale di un argomento debba essere una caratteristica degli "esperti" e pertanto raccomando la lettura di questi libri.

Ultima nota: tranne i due capitoli sulla blockchain (che si perdono in riflessioni fumosissime), il libro è scritto anche molto bene. Cosa che non guasta...

**********

**05- Linee guida AgID per usare SPID per firmare**

Diego Padovan degli Idraulici della privacy ha segnalato le Linee guida AgID contenenti le "Regole Tecniche per la sottoscrizione elettronica di documenti ai sensi dell'art. 20 del CAD":
- https://anorc.eu/attivita/firmare-i-documenti-con-spid-emanate-le-linee-guida-agid/.

I destinatari delle Linee Guida sono i fornitori dei servizi SPID. Ma interessa anche chi con SPID ha poco a che fare perché potrà utilizzare SPID per sottoscrivere atti e contratti aventi validità giuridica. Molto utile.

**********

**06- Servizi di test malware online**

Ho "scoperto", da una sezione del libro "Tecnologia e diritto: Volume III" scritta da Paolo Dal Checco, questi due siti che permettono di verificare i programmi e i file su computer sicuri e remoti, in modo da poter rilevare la presenza di malware:
- https://any.run/;
- https://hybrid-analysis.com/.

Questi siti permettono invece di verificare se un sito web, soprattutto se poco noto, contiene materiale rischioso:
- https://urlscan.io/;
- https://www.virustotal.com/gui/home (questo permette anche di verificare file).

**********

**07- Articolo di approfondimento sul CMMC**

Segnalo questo articolo di Giustino Fumagalli e Paolo Sferlazza dal titolo "Una nuova frontiera nelle certificazioni di sicurezza cyber: Il CMMC":
- https://www.ictsecuritymagazine.com/articoli/una-nuova-frontiera-nelle-certificazioni-di-sicurezza-cyber-il-cmmc/.

Mi sembra un articolo molto chiaro che permette di capire bene cos'è questo CMMC, anche dal punto di vista tecnico.

Del CMMC avevo già accennato a febbraio 2020, facendo riferimento a due altri articoli in inglese:
- http://blog.cesaregallotti.it/2020/02/cybersecurity-maturity-model.html.

Il modello al momento si trova a questo URL:
- https://www.acq.osd.mil/cmmc/draft.html.

**********

**08- Privacy: micromarketing, microtargeting e profilazione**

Mi sono trovato spesso a pensare alla profilazione così come espressa dal GDPR e alla segmentazione dei alcune offerte commerciali.

Spesso, molte aziende inviano messaggi pubblicitari a clienti che hanno comprato prodotti simili (che io chiamo "prodotti gemelli", anche se non è un termine riconosciuto) a quello in promozione. Ho sempre pensato che non si tratti di profilazione secondo la definizione del GDPR ("trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica").

A questo proposito ho scoperto il "micro marketing", che invece mi sembra rientri maggiormente nella profilazione. Per approfondire l'argomento, c'è ovviamente la pagina di Wikipedia:
- https://it.wikipedia.org/wiki/Micromarketing.

Per i più interessati, l'articolo, del 2000, "Dalle carte fedeltà a Internet: l'evoluzione del micromarketing" di Lugli e Ziliani si trova on line (io ho trovato anche un pdf):
- https://www.yumpu.com/it/document/view/19497092/dalle-carte-fedelta-a-internet-levoluzione-del-escp-europe.

Sottopongo queste riflessioni a chi si fosse posto le mie stesse domande sulla profilazione.

**********

**09- COVID-19: Le App per il tracciamento**

Questo mese ho guardato con attenzione questo argomento, per interesse professionale e personale. Raccolgo tutto in questa notizia e mi scuso per la sua lunghezza.

Tra l'altro, proprio oggi la notizia è che è stata scelta l'applicazione per l'Italia, basata su Bluetooth in modo da ridurre la raccolta di dati centralizzata (ringrazio Glauco Rampogna degli Idraulici della privacy per questo link):
- https://www.open.online/2020/04/17/coronavirus-arriva-immuni-app-per-il-tracciamento-dei-contagi-scelta-dal-governo/.

E' la soluzione basta su Blutooth, sulla cui utilità ho parecchi dubbi, come ho già scritto.

Continuo (e non solo io!) ad avere molti dubbi in proposito, ma approfondisco nel seguito.

La prima applicazione emersa in cronaca è quella usata in Corea del Sud. Un articolo tra i tanti, che mi sembra molto esaustivo (grazie a un retweet di @brunosaetta):
- https://www.valigiablu.it/coronavirus-dati-tecnologia/.

Questo articolo, sempre su Valigia Blu, ma da un tweet di @fpietrosanti, parla di Singapore:
- https://www.valigiablu.it/coronavirus-singapore-contact-tracing-tecnologia-privacy/.

Molte critiche. Credo che questo articolo (da un retweet di @gbgallus) riassuma la questione:
- https://www.techeconomy2030.it/2020/03/21/coronavirus-contact-tracing-emergenza-sanitaria-cancella-altri-diritti/.

Riccardo Lora degli Idraulici della privacy ha condiviso questa riflessione di Matteo Flora dal titolo "La Guida Completa allo Stato di Polizia":
- https://www.youtube.com/watch?v=rsu-LHNcyEM.

Il mio commento è che troppo spesso si pensa alla tecnologia senza pensare a tutti gli altri fattori (anche altri dicono, con parole più o meno diverse, questa stessa cosa). Siamo, come al solito, in mano a quelli che ragionano per tool e non per cultura e processi. Questo porta sempre a risultati negativi, come ho già scritto in passato.

Per esempio, ecco alcuni elementi culturali a cui ho pensato e che non ho visto approfonditi da quelli che vogliono l'applicazione:
- nei Paesi asiatici l'uso della mascherina è molto più diffuso anche per le "normali" influenze (guardatevi in giro e pensate a quanti non si mettono la mascherina per non sembrare buffi; una mamma infermiera mi ha detto che sua figlia ha pianto quando l'ha vista con la mascherina);
- nei Paesi asiatici, solitamente, le persone appena possono stanno più distanti che da noi (giusto sabato ho visto uno che a piedi superava un'altra a non più di 5 cm di distanza e mi sono chiesto perché tanta fretta; al supermercato si vede sempre il "corridore" che, evidentemente per tornare a casa in fretta, si avvicina a tutti e senza mascherina se non obbligato);
- nel nostro Paese il richiamo alle regole genera fastidio e anche derisione, piuttosto che solidarietà (un giorno, dal fruttivendolo, mi sono arrabbiato con il garzone che, senza mascherina, continuava a passarmi vicinissimo e, ovviamente, io ho fatto la figura del rompiscatole, non lui quella dello sconsiderato);
- le mascherine sono tornate disponibili da pochissimo tempo.

Proprio il 30 marzo è uscito un articolo sul Corriere della Sera dal titolo "Controlli: 5.000 multati (e 50 positivi in giro)". Il problema non è quindi l'uso delle tecnologie, se una domenica 50 persone positive vanno in giro e 5.000 vanno in giro senza alcuna ragione:
- https://www.corriere.it/politica/20_marzo_30/coronavirus-sabato-nero-controlli-5000-multe-quei-50-positivi-spasso-8dae3e98-71f8-11ea-b6ca-dd4d8a93db33.shtml.

Sulla questione delle mascherine, sempre il 30 marzo è uscito un articolo sul Corriere della Sera:
- https://www.corriere.it/dataroom-milena-gabanelli/coronavirus-perche-non-si-trovano-mascherine/7233d98a-71fc-11ea-b6ca-dd4d8a93db33-va.shtml.

Mi vengono poi ulteriori domande sulla reale capacità di usare questi strumenti, su quante persone competenti ci sono in giro per installarli, usarli efficacemente e mantenerli. Visto che già nelle aziende private vedo situazioni imbarazzanti, mi permetto di avere qualche dubbio per un progetto pubblico di questa dimensione (e ho anche dei dubbi sui tempi; ora che sarà tutto pronto spero che l'emergenza sarà finita).

La newsletter Guerre di rete riporta una sintesi degli interventi in materia (ringrazio Glauco Rampogna degli Idraulici della privacy per la segnalazione):
- https://guerredirete.substack.com/p/guerre-di-rete-contact-tracing-a.

Di questo articolo (molto "giornalistico") trovo particolarmente interessanti le domande poste: << Ma la finalità qual è? E qui la risposta non può essere solo quella di "tracciare i contatti dei contagiati". Una volta raccolti i contatti di un contagiato, cosa succede, a livello individuale, al singolo, ma anche a livello globale? Che procedure sanitarie si attiveranno, e sono in grado di scalare su numeri che potrebbero essere molto consistenti? Come si integrano i dati della app col resto delle misure da prendere e le risorse del sistema sanitario? Con la capacità di fare test o di assistere persone che devono stare isolate? O la si userà solo per mettere in quarantena volontaria e fai-da-te migliaia di persone che secondo la app sono state vicine a un contagiato? e staranno in quarantena in casa con altre persone? e loro come si

comporteranno? (Anche sulla cancellazione dei dati, se si dice che verrà fatta al raggiungimento della finalità bisogna specificare quale sia e quando verrà raggiunta). >>

Da un punto di vista più tecnico, segnalo come notevole la ricerca e l'analisi di Paolo Attivissimo (ringrazio sempre Glauco per la segnalazione):
- https://www.zeusnews.it/n.php?c=27995.

Anche Bruce Schneier (a sua volta citando Ross Anderson) dice la sua sulle applicazioni di tracciamento:
- https://www.schneier.com/blog/archives/2020/04/contact_tracing.html

Fa un po' di riflessioni sul fatto che l'efficacia di un'applicazione di tracciamento non è provata, che bisognerà affrontare i falsi positivi e i falsi negativi e che, soprattutto, senza un metodo economico, veloce e accurato per verificare lo stato di salute, l'applicazione è inutile. E' la risposta tecnologica a un problema che invece è sociale.

Inoltre Bruce Schneier riporta la riflessione di Ross Anderson che dice che tutto nasce da un falso sillogismo (in questo caso, un sillogismo cicliico): qualcosa deve essere fatto e l'applicazione è qualcosa e quindi dobbiamo farlo.

Infine, mi hanno intervistato per Byoblu:
- https://www.youtube.com/watch?v=hYPu4v4x-n8.

Non credo di aver fatto un bell'intervento (preferisco sempre scrivere al parlare) perché molte cose non le ho dette e ne ho dette altre inutili. Ma mi ha divertito fare questa intervista via Skype e spero di aver presentato le cose in modo equanime, presentando i punti critici senza fare allarmismo o scandalo inutile. Devo dire che la mia analisi preliminare del sito https://www.byoblu.com/ mi aveva fatto temere un approccio scandalistico che invece non ho visto alla prova dei fatti.

I commenti al video non mi trovano d'accordo perché buttano tutto in caciara. Ma almeno mi sembra che nessuno mi abbia dato (ancora) del cretino.

**********

**10- COVID-19: la privacy nei luoghi di lavoro**

Sulla privacy nei luoghi di lavoro avevo scritto il 1 marzo:
- http://blog.cesaregallotti.it/2020/03/corona-virus-e-privacy.html.

Il Garante poco dopo ha fatto un comunicato proprio su questo argomento (ringrazio un segnalatore anonimo):
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9282117.

La posizione del Garante è ovviamente più approfondita della mia (ma almeno è sulla mia stessa linea... meno male... se no ci avrei fatto una bruttissima figura!).

Su questo aggiungo che mi sto ponendo un'altra questione: se una persona è venuta nei locali di un'azienda e si è successivamente accorta di essere infetta e poi telefona all'azienda per segnalare l'evento, come deve comportarsi l'azienda? Io, indicativamente, direi che l'azienda dovrebbe identificare le persone e informare le persone con cui è entrata in contatto. E quindi questa cosa andrebbe prevista e gli interessati informati.

Certo... dovrei cercare di passare dal medico del lavoro. Però la situazione non mi sembra facile.

Detto questo, sono arrivate segnalazioni di data breach e anche reclami relativi a persone la cui privacy è stata violata perché positivi al COVID-19 (p.e. attraverso diffusione su social del nome della persona, diffusione dei risultati del test, pubblicazione del provvedimento di isolamento).

Il 16 marzo, sempre in merito alla raccolta di dati da parte delle aziende e all'elaborazione dei dati di posizionamento in possesso delle compagnie di telecomunicazioni per fronteggiare l'emergenza COVID-19, l'EDPB ha fatto una dichiarazione:
- https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_it.

Mi è sembrata meno approfondita di quello che speravo.

Ringrazio sempre la mia fonte (anonimizzata).

**********

**11- COVID-19: Le scuole, la digitalizzazione forzata e le solite lezioni**

Anche sulla scuola e la digitalizzazione di questo periodo ho scritto più del solito sempre per interesse professionale e personale.

Le scuole, causa la chiusura fisica, sono state "invitate" dal Ministero a usare strumenti di didattica a distanza. Ovviamente qualcuno va in giro a dire che si sta facendo grande opera di digitalizzazione, ma in realtà si sta facendo grande confusione.

La storia, per quanto abbia potuto ricostruire, è semplice e drammatica allo stesso tempo. A fronte dell'emergenza, sono stati identificati degli strumenti per la didattica a distanza e gli istituti sono stati invitati ad usarli. Questo senza che fossero elaborate delle istruzioni per i docenti e i genitori (il solito "armiamoci (male) e partite"), fossero fatte delle analisi per aiutare i docenti a scegliere gli strumenti e delle analisi sulla privacy.

Tra l'altro, dall'inizio dell'emergenza, l'elenco degli strumenti è cambiato senza alcuna spiegazione (dalle mie visite di fine marze e del 16 aprile, uscito Edmodo, uscita e rientrata WeSchool, entrata e poi uscita Facebook):
- https://www.istruzione.it/coronavirus/didattica-a-distanza.html.

Il Garante ha detto la sua solo il 30 marzo:
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9302778.

Molte famiglie si sono ritrovate con la necessità di mettere a disposizione dei figli degli strumenti informatici (so di alcune classi che fanno ore di lezione, ma so anche di famiglie che di digitale hanno solo i cellulari dei genitori che, ahiloro, in questi giorni devono comunque uscire per lavorare, oppure famiglie che hanno due figli, ma non due tablet o pc per far seguire le lezioni online ai due figli se in contemporanea). E chi ha i figli alle elementari, in età in cui non sono autosufficienti, ha dovuto registrarli ai sistemi, capire come funzionano e supportarli nel loro utilizzo. Quando, fino a ieri, le comunicazioni arrivavano solo via WhatsApp. Tutto questo avrà come conseguenza che al rientro alcuni saranno allineati, altri saranno indietro e di solito l'arretratezza si accompagna a difficoltà già pregresse.

Di questo, la nota informativa del Ministero tratta in modo decisamente superficiale:
- https://www.miur.gov.it/web/guest/-/coronavirus-emanata-la-nota-con-le-indicazioni-operative-per-la-didattica-a-distanza.

Ma parliamo anche degli strumenti.

Io ho avuto modo di verificare Weschool e Edmodo.

Weschool non capisco perché sia indicato come strumento didattico. Sembra più una piattaforma per scambiarsi messaggi. I software usati per le BBS negli anni Novanta erano meglio: almeno visualizzavano una bandierina sulle discussioni per cui c'erano nuovi messaggi da leggere. Weschool non fa questo e quindi bisogna riguardare tutte le discussioni e vedere se ci sono risposte, se le maestre hanno messo dei commenti e così via. Una a una. Inoltre come uniche funzionalità ha la "board" e al "Wall" (come fosse Facebook), i "test" (che sembrano i sondaggi di Facebook) e la video conferenza (usando una piattaforma esterna).

Edmodo è un po' meglio perché, oltre a funzionalità "tipo Facebook", permette agli insegnanti di dare i compiti e farli visualizzare in una sezione apposta. E' possibile individuare le novità e risposte delle insegnanti osservando le notifiche (che però includono anche "tutto il resto", creando un po' di confusione) però, nella versione per tablet, non è possibile nascondere quelle notifiche già controllate.

Insomma: nulla che un uso attento dell'email o di WhatsApp non avrebbe permesso.

Ferruccio Militello, che fa il DPO per alcune scuole, mi conferma che alcune scuole superiori erano già avanti nel processo, ma altre no e hanno dovuto iniziare "in corsa" l'uso di questi strumenti, senza però che i dirigenti scolastici e gli insegnanti abbiano mai ricevuto formazione in materia, né istruzioni di base semplici (il sito del MIUR rimanda alle pagine ufficiali dei prodotti, non ottimizzate per la scuola italiana né per persone alle prime armi).

Aggiunge Ferruccio (e io appoggio il suo punto di vista): "Vale la pena sottolineare, a mio modo di vedere, che, con uno staff importante e strutturato, il MIUR avrebbe dovuto pensarci piuttosto che lasciare iniziativa ai singoli".

Io sarei brutale e direi che siamo di fronte alla solita voglia di imporre tecnologia senza farsi domande sui processi e sulle persone che la utilizzano.

A questo aggiungiamo il caso di Zoom: si è dimostrato che condivide i dati con Facebook (e molti istituti suggeriscono questo strumento per tenere le lezioni):
-
https://www.repubblica.it/tecnologia/sicurezza/2020/03/27/news/zoom_l_app_per_videoconferenze_condivide_i_dati_con_facebook-252458567/.

Poi dicono di aver risolto, ma la questione fa rabbrividire:
https://www.repubblica.it/tecnologia/sicurezza/2020/03/29/news/privacy_zoom_ripara_la_falla_di_sicurezza_non_eravamo_a_conoscenza_dei_dati_raccolti_da_facebook_-252611458/.

Poi certamente è bello pensare che ci sono strumenti gratuiti da usare, ma si sa che non sono veramente gratuiti in quanto pagati con i dati. E qui si parla di dati di minorenni. Il MIUR avrebbe forse dovuto elaborare e pubblicare una PIA per ogni strumento scelto.

C'è anche la solidarietà digitale (https://solidarietadigitale.agid.gov.it), ma questo è un altro argomento su cui dovrei riflettere molto di più: come sono stati selezionati, perché tanti offrono servizi basati sui soliti OTT (Google, Amazon, Facebook, Apple) e perché anche in questo non si sia approfittato per promuovere una digitalizzazione reale.

Sulla privacy, Biagio Lammoglia degli Idraulici della privacy ha segnalato questo articolo di Scuola Informa:
- https://www.scuolainforma.it/2020/03/31/scuola-didattica-online-il-piu-grande-data-breach-della-storia.html.

A chi mastica già di privacy non dice niente di nuovo, ma le conclusioni sono, mutatis mutandis, le mie (ossia che la didattica a distanza andrebbe guidata meglio e non lasciarla alla buona volontà dei singoli).

**********