Cesare Gallotti

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

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- Stato delle norme ISO/IEC 270xx - Aprile 2020

Si è appena concluso il 62mo meeting dell'ISO/IEC JTC 1 SC 27. Doveva essere a Sanpietroburgo, ma si è invece tenuto tutto in ambiente virtuale. Esperienza decisamente difficile, ma riuscita (anche se si è confermato che gli incontri fisici sono più efficaci di quelli virtuali).

Hanno partecipato più di 120 delegati da 34 Paesi.

La delegazione italiana era composta da 7 persone, tra cui: Fabio Guasconi (Presidente), Andrea Caccia, Alessandro Cosenza, Stefano Ramacciotti, Daniele Tumietto e me stesso.

Per quanto riguarda le norme del WG 1, non ci sono grosse novità. Mi limito, come al solito, ad indicare lo stato di avanzamento di alcune norme:
- ISO/IEC 27002 (controlli di sicurezza): sono proseguiti i lavori e sono stati fatti molti commenti; per migliorare ulteriormente la qualità della norma, gli esperti hanno ritenuto opportuno "rallentarne" l'uscita, che a questo punto sarà, nella migliore delle ipotesi, ad autunno 2021;
- ISO/IEC 27003 (guida all'uso della ISO/IEC 27001): confermata così com'è;
- ISO/IEC 27005 (sul risk management): sono proseguiti i lavori, ma la pubblicazione della nuova versione è ancora lontana (nella migliore delle ipotesi, sarà nel 2022);
- ISO/IEC 27013 (relazioni tra ISO/IEC 20000-1 e ISO/IEC 27001): sono proseguiti i lavori e si spera di pubblicare ad autunno 2021.

La norma ISO/IEC 27558, con i requisiti di accreditamento degli organismi di certificazione per svolgere gli audit ISO/IEC 27701, è una norma di competenza del WG 1 e del WG 5 (dedicato alla privacy). Per questa norma sono state fatte tre scelte importanti:
- dare un'accelerazione ai lavori in modo da pubblicarla, auspicabilmente, per metà 2021 (non mi dilungo nei dettagli tecnici; dico solo che non sarà un "International Standard", ma una "Technical Specification");
- avviare una richiesta di commenti specifica per il calcolo dei tempi di audit (io qui prevedo un grande macello per poi "accontentarsi" del solito calcolo basato sul numero di persone in ambito);
- sarà numerata ISO/IEC 27006-2; così l'attuale ISO/IEC 27006 sarà numerata ISO/IEC 27006-1.

Per quanto riguarda le norme del WG 5 (privacy), segnalo solo:
- ISO/IEC 29134 (sulla PIA): sarà avviato un lavoro di "correzione".

Per il WG 4, che si occupa di norme più tecniche, mi sono interessato a quelle sull'IoT e sull'industriale (ISO/IEC 24391, Guidelines for IoT domotics security and privacy; ISO/IEC 24392, Security reference model for industrial internet platform; ISO/IEC 27030, che cambierà numero in ISO/IEC 27400, IoT security and privacy – Guidelines; 27402, IoT security and privacy – Device baseline requirements) e sono meno interessato ad altre norme, anche se il titolo sembra promettente, perché temo possano essere troppo fuffose (la nuova edizione della ISO/IEC 27032, Guidelines for Internet security; ISO/IEC 27035, sulla gestione degli incidenti). Ad ogni modo, non sono riuscito a seguire i lavori di nessuna di queste norme e me ne dispiace molto.

Il prossimo meeting sarà a metà settembre a Varsavia (Polonia). Speriamo...

Ringrazio Fabio Guasconi (e non solo...) per avermi segnalato alcuni errori presenti in questo breve articolo.

****

02- ISO/IEC 21964 sulla distruzione dei supporti

Segnalo la norma ISO/IEC 21964 con titolo "Destruction of data carriers". La norma è del 2018, ma solo ora, grazie a UNI che l'ha inserita a catalogo (in lingua inglese) e a Franco Vincenzo Ferrari di DNV GL, ne sono venuto a conoscenza.

La norma è divisa in 3 parti e questo è il link alla prima parte:
- https://www.iso.org/standard/72204.html.

L'argomento è la distruzione dei supporti fisici, quindi non tratta di cancellazione sicura, ma proprio di distruzione o triturazione o tecniche simili.

La prima parte (Principles and definitions) definisce i 7 livelli di sicurezza con cui uno strumento può distruggere i supporti e le 3 classi di protezione a cui potrebbe aspirare un'organizzazione.

La seconda parte (Requirements for equipment for destruction of data carriers) tratta delle tecniche di distruzione per i diversi tipi di supporto, suddivise nei 7 livelli di sicurezza (quindi, per esempio, la carta può essere distrutta da strisce di 12mm a strisce di 1mm e un hard disk può essere reso "inutilizzabile" fino a essere distrutto in particelle di meno di 5 mm quadrati). Sono anche stabilite le specifiche di test delle tecniche.

La terza parte (Process of destruction of data carriers) riporta i requisiti dei processi di distruzione, per le 3 classi di protezione, nel caso in cui il controller provveda autonomomante, si affida a un fornitore presso la propria sede o a un fornitore presso la sede del fornitore.

Le norme usano il termine "shall" e quindi profetizzo facilmente che qualcuno, se non lo ha già fatto, si inventerà una certificazione.

****

03- Costituiti il CSIRT Italia e CERT-AgID

Dalla newsletter di DFA segnalo che è stato costituito il CSIRT Italia:
- https://csirt.gov.it/home

Il sito del neonato CSIRT Italia è avaro di informazioni utili, quindi copio (con qualche taglio ed evitando il termine "cibernetico") quanto riportato dal sito del CERT-PA.

Il CSIRT Italia raccoglie le attività in precedenza svolte dal CERT-PA e il CERT Nazionale, rispettivamente dedicate alle pubbliche amministrazioni ed al settore privato.

La decisione rientra nell'ambito del piano di attuazione della Direttiva NIS (Decreto legislativo 18 maggio 2018 n. 65) che – tra le altre misure – prevede anche in Italia la costituzione di un Computer Security Incident Response Team unico (cosiddetto CSIRT).

L'attività dello CSIRT è disciplinata dal DPCM 8 agosto 2019 in materia di "Disposizioni sull'organizzazione e il funzionamento del Computer Security Incident Response Team – CSIRT italiano", pubblicato in Gazzetta Ufficiale l'8 novembre 2019.

In tale quadro, i soggetti pubblici e privati, a partire dalla data menzionata, in caso di incidente informatico o di segnalazione di evento, hanno quale nuovo ed unico interlocutore lo CSIRT Italia, che già riceve le notifiche obbligatorie e volontarie degli operatori di servizi essenziali (cosiddetti OSE) e fornitori di servizi digitali (cosiddetti FSD) ai sensi della Direttiva NIS.

Concludo quindi con un commento personale: spero che la nuova struttura sia più utile delle precedenti, per lo meno nella parte visibile al pubblico, e promuova campagne di informazione più significative, come quelle, per esempio della svizzera MELANI.

Insieme al CSIRT (grazie a Franco Vincenzo Ferrari di DNV GL Business Assurance per avermi segnalato la notizia), nasce il CERT-AgID, che si occuperà di mantenere e sviluppare servizi di sicurezza preventivi e attività di accompagnamento utili alle pubbliche amministrazioni per favorire la crescita e la diffusione della cultura della sicurezza informatica:
- https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2020/05/07/cert-agid-promozione-sicurezza-informatica-nella-pa.

Dal sito e dalla descrizione non mi sono chiarissime le differenze tra CERT-AgID e CSIRT Italia; forse il primo si occupa più di "consulenza", mentre il secondo più di monitoraggio e allerta; se così è, allora trovo fuorviante il nome "CERT" a una struttura che non svolge attività di "risposta" e anche il sito perché molto dedicato alle minacce e alle CVE (non diversamente dal sito del CSIRT Italia).

Il sito web è:
- https://cert-agid.gov.it/.

Altre due considerazioni:
- c'è un netto miglioramento rispetto a prima, visto che avevamo 2 CERT o CSIRT (CERT PA e CERT Nazionale) e ognuno di essi faceva sia parte reattiva sia parte preventiva, solo che uno era dedicato ai privati e l'altro era dedicato alla Pubblica amministrazione, con ovvia dispersione di competenze senza una vera ragione tecnica (ci si chiede chi avesse pensato a quella suddivisione e quali ragioni tecniche presentato, oltre alla moltiplicazione delle posizioni dirigenziali);
- la documentazione è ancora poca e non datata (!), ma mi sembrano interessanti le linee guida per lo sviluppo sicuro (forse del 2019) e di configurazione del software di base (forse del 2017).

****

04- Documento ENISA sulla sicurezza del software

ENISA ha pubblicato il rapporto "Advancing Software Security in the EU":
- https://www.enisa.europa.eu/publications/advancing-software-security-through-the-eu-certification-framework.

Sono 16 pagine molto dense.

Infatti da una parte il paragrafo 2.4 "Existing standards and good practices" riporta alcuni documenti significativi relativi allo sviluppo sicuro. In particolare, io non conoscevo per niente l'OWASP ASVS, che ho invece trovato molto interessante (anche se avrei preferito, come al solito, un documento di "progettazione" e non di "verifica"):
- https://owasp.org/www-project-application-security-verification-standard/.

Il capitolo 3, dedicato ai problemi relativi alla sicurezza del software, anche se molto corto, riporta considerazioni che non ho mai trovato altrove. Le raccomandazioni, ossia i successivi passi che ENISA e altre istituzioni europee potrebbero prendere, mi sembrano anch'esse di adeguata profondità (anzi... evitano proprio di citare la solita "formazione", che è sì importante, ma sembra il rifiugio di chi non ha idee).

****

05- Articolo su TISAX

A novembre 2019 avevo segnalato TISAX, uno schema relativo ai sistemi di gestione per la sicurezza delle informazioni per il settore automotive.

Paolo Sferlazza di Gerico Security mi ha segnalato un suo recente articolo in materia:
- https://www.ictsecuritymagazine.com/articoli/tisax-la-valutazione-del-livello-di-maturita-della-sicurezza-delle-informazioni-nellambito-automotive/.

L'articolo è interessante e approfondisce la questione.

****

06- Articolo sulla protezione delle piattaforme tecno-industriali

Segnalo questo articolo dal titolo "Protezione delle piattaforme tecno-industriali. Compliance NIS e oltre" di Giulio Carducci:
- https://www.ictsecuritymagazine.com/articoli/protezione-delle-piattaforme-tecno-industriali-compliance-nis-e-oltre/.

L'articolo propone un approccio per la valutazione del rischio relativo alla sicurezza OT (tradotta, molto bene, a mio parere, con "tecno-industriale").

L'articolo ha il pregio di non nascondere i punti di "semplificazione" dell'approccio battezzato IPSEM. Ma questi passaggi sono molto ben spiegati e giustificati, sia facendo riferimento alle caratteristiche peculiari dell'ambiente tecno-industriale, differente da quello "gestionale", sia alle solite caratteristiche del rischio relativo alla sicurezza delle informazioni.

Per la cronaca: Giulio Carducci è stato uno dei miei maestri, ma questo articolo l'ho "scoperto" da solo e mi fa piacere segnalarlo.

****

07- Incidente MailUp

La mia newsletter è su MailUp e il 25 aprile 2020 mi è stato comunicato che è stato rilevato un incidente.

Su questo evento ho visto pochissime notizie. Anzi... ho trovato solo questa:
- https://www.cybersecurity360.it/legal/privacy-dati-personali/data-breach-mailup-coinvolto-il-responsabile-del-trattamento-la-lezione-appresa/.

Interessante è il fatto che ritengano "riservate" le comunicazioni inviate, quando però è compito dei titolari fornirle agli interessati.

In sintesi, l'incidente è stato rilevato il 24 aprile e si tratta di "un sofisticato attacco ransomware di elevata intensità". Come in tutti gli attacchi ransomware, i dati sono risultati indisponibili, ma poi MailUp li ha ripristinati entro il 27 aprile. Le analisi inviate non dicono se ci sono evidenze di trasmissione dei dati.

Detto questo, i dati personali di cui io sono titolare sono gli indirizzi email dei destinatari delle newsletter. La loro violazione non presenta un rischio per i diritti e le libertà delle persone fisiche, visto che l'incapacità di ricevere la newsletter può rappresentare sì un disagio, ma non può compromettere i diritti e le libertà delle persone fisiche. Per quanto riguarda la possibile violazione della riservatezza, questa può dimostrare l'interesse dell'interessato verso la qualità, la sicurezza delle informazioni e la privacy, ossia materie che non compromettono i diritti e le libertà delle persone fisiche.

Tutto ciò considerato: non farò alcuna notifica al Garante, ma sto avvisando comunque gli interessati con questa newsletter.

****
08- Privacy: parere del Garante sul ruolo dell'OdV

Il Garante privacy ha recentemente emesso un "parere sulla qualificazione soggettiva ai fini privacy degli Organismi di Vigilanza previsti dall'art. 6, d.lgs. 8 giugno 2001, n. 231":
- https://www.aodv231.it/documentazione_descrizione.php?id=3745&sheet=&tipo=newsletter&Il-Garante-per-la-protezione-dei-dati-personali-sul-ruolo-dell-OdV-in-ambito-privacy.

In breve: i membri dell'OdV sono da considerare come "autorizzati". Alcuni non condividono perché vedono così messa in discussione la sua autonomia, ma intanto il parere del Garante approfondisce bene questa questione, inoltre a me sembra logico vedere l'OdV come parte di un'azienda (titolare), anche se indipendente da tutte le altre funzioni aziendali

Grazie a Pietro Calorio per averlo segnalato agli Idraulici della privacy. Con gli stessi Idraulici avevamo discusso mesi or sono su questa stessa questione ed eravamo giunti alla medesima conclusione (per fortuna...).

****
09- Rapporto semestrale MELANI

Due volte all'anno segnalo il rapporto semestrale della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI (Svizzera):
- https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/halbjahresbericht-2019-2.html.

Questa edizione mi ha fornito meno indicazioni del solito, forse perché sono troppo concentrato sul COVID-19.

Comunque sia, è sempre un'ottima lettura.

****

10- Protocollo COVID-19 sui luoghi di lavoro (24 aprile)

Il 24 aprile è stato aggiornato l'aggiornamento del "Protocollo condiviso sulle misure per il contrasto al Covid-19 negli ambienti di lavoro". Si trova qui:
- https://www.lavoro.gov.it/notizie/pagine/sicurezza-sul-lavoro-integrato-il-protocollo-condiviso-sulle-misure-per-il-contrasto-al-covid-19-negli-ambienti-di-lavoro.aspx/.

Ringrazio Daniela Pollino di Pidielle S.p.A. per la segnalazione.

Il protocollo stabilisce anche le modalità di ingresso in azienda, prevedendo il controllo della temperatura. Per questo è necessario quindi prevedere opportune informative privacy.

A questo punto segnalo il modello di informativa proposto dallo Studio Stefanelli. Fa riferimento al precedente protocollo del 14 marzo, ma credo vada bene lo stesso. Segnalo la pagina in cui è disponibile questo documento e anche altri:
- https://www.studiolegalestefanelli.it/it/solidarieta-digitale-smartworking.

****

11- Sistemi di videoconferenza e sicurezza

Dalla newsletter Crypto-Gram di maggio, segnalo questo post sulla sicurezza delle applicazioni di video conferenza:
- https://www.schneier.com/blog/archives/2020/04/secure_internet.html.

Qui sono segnalati due rapporti, di NSA e Mozilla, sulla sicurezza delle applicazioni di videoconferenza. Confesso che nono mi sono sembrati chiarissimi.

Il rapporto NSA specifica la presenza o meno di alcune funzionalità, ma senza ulteriori spiegazioni o aiuti (ho però trovato interessante che Google assicura la cancellazione sicura solo per le versioni a pagamento).

Il rapporto di Mozilla invece fornisce chiaramente un voto sulla sicurezza (a patto di aprire le schede una per una) ma non sulla privacy. Pertanto è necessario leggere con maggiore attenzione.

Comunque sono interessanti da leggere, visto che questi sistemi sono ormai essenziali in questo periodo di COVID-19.

****

12- Data center Amazon in Italia

Paolo Sferlazza di Gerico Security (che ringrazio) mi ha segnalato questa interessante notizia dal titolo "La nuova Regione AWS in Italia":
- https://aws.amazon.com/it/local/italy/milan/.

Non sono un fan di Amazon, ma bisogna dire che questa mossa ha un impatto interessante per quanto riguarda l'applicazione del GDPR. Sarà anche interessante vedere come questo esempio sarà seguito in Europa e in Italia.

Non poi se giudicarla una buona notizia (si creano posti di lavoro) o una cattiva notizia (un'azienda estera e non italiana ha evidentemente trovato un mercato da sfruttare).

****

13- EDPS Web site collector per l'analisi privacy

Ringrazio per questo link Nicola Nuti. L'EDPS ha messo a disposizione uno strumento per analizzare i siti web e la loro conformità relativamente alla protezione dei dati personali.

Questa è notizia non proprio recente. Ma questo articolo che spiega bene come funziona è invece recente:
http://www.dirittoegiustizia.it/news/23/0000098319/Website_Evidence_Collector_il_tool_gratuito_del_Garante_Europeo_per_la_Protezione_dei_dati_personali.html.

La pagina per scaricare lo strumento è questa:
- https://joinup.ec.europa.eu/solution/website-evidence-collector/releases.

****
EONL