Infosec & Quality [ITA] - Apr. 2023

Newsletter mensile su sicurezza delle informazioni e qualità.

17 APR 2023

Share

Temperanza, Fortezza e Prudenza. Cappella Portinari. Milano. Aprile 2023. Foto mia.

Indice

****

01- Rapporto Clusit 2023

E' stato pubblicato il rapporto Clusit 2023: https://clusit.it/rapporto-clusit/.

Un altro, che ringrazio, mi ha segnalato le cose per lui più interessanti. Ne approfitto e le segnalo:

- Pag. 157: "Nel 2021 le organizzazioni che hanno pagato il riscatto hanno recuperato mediamente solo il 61% dei propri dati, rispetto al 65% del 2020, mentre solo il 4% è riuscita a recuperare l'intera quantità di risorse inficiate. (fonte: Sophos "The State of Ransomware 2022")
- Pag. 159: [traduco io, Cesare, il testo] Il gruppo cyber-criminale Lockbit ha specificatamente richiesto ai propri affiliati di non cifrare i dati quando sono attaccati i settori maggiormente critici, come quello sanitario. Vedi anche il codice di condotta del gruppo DarkSide
- https://krebsonsecurity.com/2021/05/a-closer-look-at-the-darkside-ransomware-gang/.
- Pag. 180: Indagine ironica "Quanto potrebbe essere devastante la violazione laddove si verificasse nel loro archivio dati cloud": Il 29% ha risposto "Ci sarebbe l'armageddon", il 15% "Mi darei malato quel giorno", il 9% "Darei la colpa ad un tirocinante" [...]
- Pag. 184: "Il modo più risoluto di proteggere i dati nel cloud è quello di rimuoverli dal cloud."
- Pag. 191: "Negli anni le disposizioni normative ed extra-normative hanno sopperito parzialmente alla carenza culturale delle organizzazioni, suggerendo o imponendo l'introduzione di sistemi di sicurezza, processi e tecnologie col fine di evitare il verificarsi di incidenti con potenziali ripercussioni anche a livello sociale." --> Mi piace questa prospettiva della legge come aiuto e non come imposizione.
- Pag. 195: Il 35% delle grandi organizzazioni ha sviluppato un proprio framework ad-hoc; il 6% usa la metodologia FAIR con analisi quantitativa del rischio.
- Pag. 251-258: Direttiva NIS2 spiegata molto bene [qui mi dice che non sapeva che crittografia e cifratura fossero concetti diversi, ma penso che ci sia un errorino nel testo della Direttiva].
- Pag. 313-329: Enumera bene i rischi della IA, tra l'altro fa riferimento a Microsoft Failure Modes: https://learn.microsoft.com/en-us/security/engineering/failure-modes-in-machine-learning.

****

02- Nuovo direttore di ACN

L'Agenzia per la cybersicurezza nazionale ha cambiato direttore. E' uscito Roberto Baldoni, è arrivato Bruno Frattasi.

Andrea Maria Tacchi di DNV mi diede la notizia a inizio marzo e mi segnalò questo articolo: https://www.wired.it/article/baldoni-agenzia-cybersicurezza-dimissioni-soldi-pnrr/.

A qualcuno interessa il mio parere? Quasi sicuramente no e quindi lo riassumo: a) non ho apprezzato molte scelte di Baldoni, a partire dalla promozione del NIST CSF per fare il "Framework Nazionale per la Cybersecurity e la Data Protection", ma non ne ho seguito le gesta

e quindi non ho altre critiche da fare; b) criticai all'epoca le richieste eccessive per i profili professionali richiesti, ma ancora una volta si tratta di poche cose; c) vedo che ACN pubblica bollettini e raccomandazioni, come tutte le cose sono migliorabili, ma mi sembrano buone iniziative; d) il resto sono lotte di potere e spero che ACN continui a lavorare e migliorare.

PS: dimenticavo un'altra critica a Baldoni: l'uso del termine "sicurezza cibernetica" (come se in inglese esistesse la cybernetics security).

PPS: un'altra è la pubblicazione di documenti (https://innovazione.gov.it/notizie/articoli/cloud-pa-online-gli-atti-per-classificare-dati-e-servizi-e-qualificare-i-servizi/) con ampie parti che non è possibile copi-incollare.

****

03- Le norme tecniche avanzano (e ISO/IEC 27005)

Il 16 marzo 2023, al Security summit di Milano, ho parlato nella sessione "Le norme tecniche avanzano". Io mi sono concentrato sulle novità della ISO/IEC 27005. La presentazione è qui: https://securitysummit.it/eventi/milano-2023/sessioni/le-norme-tecniche-avanzano.

Entro fine aprile dovrebbe uscire un articolo in cui approfondisco i concetti (anche se, in realtà, li ho espressi anche in altre occasioni).

****

04- Schemi di certificazione europei

Copio direttamente dalla newsletter Project:IN Avvocati (sempre ottima) questa notizia: L'ENISA (Agenzia per la Cybersicurezza dell'UE) ha annunciato lo scorso 19 marzo il lancio di una nuova piattaforma il cui obiettivo è promuovere e diffondere informazioni sui sistemi di certificazione UE in materia di cybersicurezza. Più in particolare, la piattaforma consentirà agli utenti di condividere informazioni sugli schemi di certificazioni attualmente in fase di sviluppo, tra cui anche l'EUCS (Cybersecurity Certification Scheme for Cloud Servies).

Aggiungo il link alla piattaforma, che è in realtà una pagina web con le informazioni relative alle certificazioni (che sono ancora in fase di sviluppo e quindi, per ora, dobbiamo solo monitorarne l'avanzamento): https://certification.enisa.europa.eu/.

****

05- Zero Trust Maturity Model Version 2 del CISA

Il CISA (Cybersecurity & infrastructure security agency degli USA) pubblica cose interessanti. Recentemente, Aprile 2023, ha pubblicato la versione 2 del "Zero Trust Maturity Model": https://www.cisa.gov/zero-trust-maturity-model.

Le misure sono illustrate in modo molto sintetico e confesso che non tutto mi è chiaro. Per esempio, non capisco perché nel livello "tradizionale" (ossia il più basso) si parli di identity store centralizzati all'interno di un'agenzia senza accennare a quelli esterni, presenti invece nel livello "iniziale", come se nel tradizionale non si possa immaginare l'uso di sistemi esterni.

Rimane un documento che, a mio avviso, vale la pena studiare.

****

06- Sicurezza informatica di base

Pierluigi Stefli di Datapro Srl mi ha segnalato due iniziative per fornire indicazioni sulla sicurezza informatica. Si tratta di materiale di base, destinato soprattutto ai "non professionisti della sicurezza".

Il primo è Barry: https://www.ibarry.ch/it/. Trovo interessante la parte relativa ai controlli di sicurezza, che mette a disposizione strumenti utili.

Il secondo è S-U-P-E-R: https://www.s-u-p-e-r.ch/it/. In questo c'è anche un quiz per verificare il proprio livello di comprensione.

****

07- Qualità: ISO 9001 Auditing Practices Group

L'ISO 9001 Auditing Practices Group esiste da 20 anni e io non avevo proprio idea che potesse esistere. Il suo sito è: https://committee.iso.org/home/tc176/iso-9001-auditing-practices-group.html.

Si tratta di un gruppo informale ma ufficiale all'interno dell'ISO.

Sul sito si trovano interessanti linee guida su come condurre audit e su cosa verificare nell'ambito della ISO 9001.

****

08- Novità legali: NIS 2 e frammentazione normativa

Segnalo questo articolo dal titolo "Nel labirinto delle norme Ue sulla cybersicurezza: come districarsi nella Direttiva NIS2": https://www.agendadigitale.eu/sicurezza/nel-labirinto-delle-norme-ue-sulla-cybersicurezza-criticita-attuali-e-scenari-futuri/.

Questo articolo mi conforta perché conferma le difficoltà di lettura della NIS2 e non solo.

Per ora, in attesa di implementing acts, recepimenti italiani, chiarimenti europei e italiani (inclusi quelli di ACN), io suggerisco di iniziare a ragionare sui controlli dell'Allegato B del DPCM 81 del 14 aprile 2021. Alcuni di questi controlli richiedono un certo tempo per essere realizzati e anche costi elevati. E' vero che c'è tempo, ma sicuramente partirei ad analizzare questi controlli, in modo da potersi attivare prontamente nel caso venissero confermati (è vero che sono orginati dal Framework Nazionale, di cui era responsabile Baldoni, ora non più Direttore di ACN, però al momento questo è quello che abbiamo).

Poi comincerei a ragionare sulla procedura di gestione degli incidenti per recepire le richieste normative.

Alla valutazione del rischio penserò solo quando usciranno indicazioni precise. Spero proprio che non promuovano un approccio basato sui singoli asset perché sarebbe una cosa assurda (ricordo che è un'impostazione degli anni Ottanta, tratta dal CRAMM, software stand-alone usato dalle grandi società di consulenza che lo facevano popolare dai ragazzini per fatturare giornate di consulenza; il CRAMM adesso non è neanche più mantenuto). Spero che qualcuno

con competenze pratiche si renda conto che è un approccio dispendioso che non dà risultati utili.

Altra cosa è invece verificare l'implementazione delle misure su ciascun asset, ma, appunto, non è valutazione del rischio.

Io qui ho fornito la mia idea. Mi piacerebbe sapere cosa ne pensano gli altri.

****

09- Novità legali: D. Lgs. 24 del 2023 sul whistleblowing

E' stato approvato il D. Lgs. 24 del 2023 sul whistleblowing. Per saperne di più, preferisco rimandare direttamente a un articolo di Agenda digitale: https://www.agendadigitale.eu/documenti/whistleblowing-ce-la-legge-tutto-cio-che-aziende-e-pa-devono-fare-per-adeguarsi/.

Il cosiddetto whistleblowing riguarda le segnalazioni di violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità di un'amministrazione pubblica o di un ente privato. La normativa disciplina la protezione delle persone che segnalano queste violazioni nel caso in cui ne siano venute a conoscenza in un contesto lavorativo pubblico o privato.

Si interseca con privacy e sicurezza delle informazioni, anche se la materia mi sembra, in generale, molto poco tecnica. Però è bene sapere che c'è.

Su Normattiva il testo sarà disponibile dal 1 aprile.

****

10- Novità legali: D. Lgs. 26 del 2023 sul Codice del consumo

Il D. Lgs. 26 del 2023 recepisce la Direttiva (UE) 2019/2161 e modifica il Codice al consumo.

Mi sembra che tratti di attività commerciali online, ma non di sicurezza delle informazioni. Ci sono anche richiami al GDPR e al D. Lgs. 196, ma non mi sembrano significativi. Comunque sia, segnalo un articolo in merito: https://www.altalex.com/documents/2023/03/20/codice-consumo-rinnova-raccogliere-sfide-mercati-digitali.

Su www.normattiva.it il D.Lgs. 26 e il Codice del Consumo (D. Lgs. 206 del 2005) saranno disponibili dal 2 aprile, data di entrata in vigore del D. Lgs. 26.

****

11- EN 17799 e certificazioni privacy

Fabio Guasconi ha tenuto un interessantissimo webinar per il Clusit dal titolo "EN 17799, impatto e nuove prospettive sulle certificazioni GDPR" (https://clusit.it/webinar/). Per accedere a slide e video bisogna essere soci Clusit (cosa che continuo a raccomandare).

Chi non fosse socio Clusit può studiarsi le slide (senza video!) presentate da Luciano Quartarone, sempre sullo stesso tema, nell'ambito dell'incontro "Le norme tecniche avanzano": https://securitysummit.it/eventi/milano-2023/sessioni/le-norme-tecniche-avanzano.

Le slide contengono anche un mio intervento sulla ISO/IEC 27005, di cui ho già parlato altrove, e l'intervento, molto interessante, anche se molto tecnico, di Stefano Ramacciotti sulla recente versione 4 dei Common Criteria.

****

12- Il blocco di ChatGPT

Io so qualcosa di privacy e so molto poco di intelligenza artificiale (tutto quello che so viene da un bel libro, "Intelligenza artificiale e sicurezza: opportunità, rischi e raccomandazioni", gratuito, della Clusit community for security, che si trova su https://iasecurity.clusit.it/).

Per questo non ho niente da dire sull'argomento, ma posso segnalare articoli sulle persone che ho apprezzo molto in questi due campi.

Intanto la notizia in brevissimo la si trova sulla newsletter #13/2023 di Project:IN Avvocati: https://www.linkedin.com/pulse/132023-italia-chiude-durgenza-chatgpt-mentre-arriva.

Per quanto riguarda l'intelligenza artificiale, segnalo questo, dal titolo "Non è possibile fermare l'AI, solo rincorrerla" da Notizie.ai di Luca Sambucci: https://www.notizie.ai/non-e-possibile-fermare-lai-solo-rincorrerla/.

Per la privacy, vorrei segnalare un'intervista a Elia Barbujani su Repubblica.it, ma c'è il cookie wall e non mi rimane che segnalare invece un suo post su LinkedIn: https://www.linkedin.com/posts/elia-barbujani_chatgpt-i-dubbi-dellesperto-lo-stop-activity-7048302886803386368-Eazv.

Infine, imperdibile il commento di Not Boring Privacy: https://t.me/notboringprivacy/531.

****

13- Gli uomini possono fare tutto (Aprile 2023)

"BUCATO. Ingiustamente considerato lavoro pesante, malinconico, riservato alle donne, e in special modo alle donne di servizio. In realtà ogni uomo, aiutato dalle conquiste della scienza (nailon e saponi schiumosi), dovrebbe lavare la sera quanto indossò di giorno. E ogni donna dovrebbe consacrare le sue economie all'acquisto, rateale, di una lavatrice elettrica, liberandosi, una volta per sempre, dalla tirannia delle lavandaie".

Pochi giorni fa lessi questa voce del "Dizionario del successo dell'insuccesso e dei luoghi comuni" di Irene Brin (del 1986, ma i brani sono del 1954 e 1965).

Mi venne in mente che pochi mesi fa, "l'informatico" di un mio cliente mi raccontava che rifiuta la lavatrice, ma provvede a lavarsi, in autonomia e quotidianamente come vuole la Brin, i vestiti usati durante la giornata.

****

Comments

Write a comment...