# Infosec & Quality [ITA] - Giu. 2023

19 JUN 2023



Certosa di Pavia - Giugno 2023 - Foto mia

**Indice**



**********

**01- NIST SP 800-124 sulla sicurezza dei dispositivi mobili**

Segnalo la pubblicazione della rev. 2 della SP 800-124 "Guidelines for Managing the Security of Mobile Devices in the Enterprise" del NIST: https://csrc.nist.gov/publications/detail/sp/800-124

**********

**02- Bozza dell'Artificial intelligence Act approvata dal Parlamento UE**

Non mi sono occupato finora delle proposte normative di intelligenza artificiale. Il motivo principale è che si tratta di normative ancora in fase di elaborazione. Adesso la situazione è avanzata ulteriormente e un articolo di Guerre di rete dal titolo "Intelligenza artificiale - AI Act, l'Europarlamento tiene" permette di capire bene la situazione attuale e gli elementi in discussione: https://guerredirete.substack.com/p/guerre-di-rete-ai-act-leuroparlamento.

Per capire qualcosa di intelligenza artificiale, anche se in modo non approfondito, ricordo la pubblicazione (gratuita) del Clusit dal titolo "Intelligenza artificiale e sicurezza: opportunità, rischi e raccomandazioni": https://iasecurity.clusit.it/. E' di inizio 2021, ma gli argomenti ci sono quasi tutti.

**********

**03- Regolamento DORA**

Del Regolamento DORA avevo accennato in precedenza. Nel titolo la R sta per "resilienza" e l'ambito di applicazione è il settore finance. A ben vedere, questa resilienza richiede di occuparsi di sicurezza informatica (reti e sistemi informatici).

Per una prima idea del DORA, segnalo questo articolo di novembre 2022: https://www.cybersecurity360.it/legal/regolamento-dora-cosi-leuropa-garantira-la-resilienza-operativa-digitale-per-il-settore-finanziario/.

L'articolo è di Giancarlo Butti che ha recentemente pubblicato il libro "Manuale di resilienza" (https://www.iter.it/prodotto/manuale-di-resilienza/). Non ho letto il libro e quindi non posso dirne alcunché. Conosco Giancarlo e quindi so che sicuramente è molto interessante.

**********

**04- Minacce e attacchi: bug programmato in visori sportivi**

Segnalo questo articolo di Valeria Lazzaroli: https://www.linkedin.com/posts/valeria-lazzaroli_supplychain-cybersecurity-ip-activity-7059467324990341122-tIlx.

In pochissime parole: un visore sportivo si è bloccato (con gioia degli utilizzatori) da un momento all'altro perché non risultava aggiornata la licenza del software (di SWARG) da parte del produttore dell'hardware (ORQA).

Il mio commento (su LinkedIn): intanto bisognerebbe capire se si tratta di un bug o di una funzionalità. Cioè: era previsto dal contratto tra ORQA e SWARG o no? Certamente era un bug per ORQA che sembra caduta essersi sorpresa della cosa.

Ho pensato anche al fatto che adesso il software lo vendono "as a service", non più "as a product" e questo è un problema. Mi spiego meglio.

Questi software si aggiornano da soli, quando vuole il produttore (puoi sempre chiedere che non lo facciano, ma questo comporta altri problemi) e come vuole il produttore. Questo genera rischi di disponibilità (come minimo perché si aggiorna senza preavvisare, bloccando il sistema). Questo modo di fare consente ai produttori di introdurre sistemi di controllo delle licenze come

nel caso segnalato.

Ripeto: ci sono pro e contro in questo approccio. Bisogna starci attenti.

Certo è che SWARG poteva lanciare qualche avvertimento che la licenza stava per scadere.

**********

**05- Operazione "Ghost money"**

Enos D'Andrea mi ha segnalato la notizia sull'Operazione "Ghost money": https://www.commissariatodips.it/notizie/articolo/operazione-ghost-money/index.html.

In brevissimo: hanno arrestato una gang che rubava soldi semplicemente presentando falsi mandati SEPA alle banche. L'istituto di credito dava disponibilità di una somma prima di verificare la non genuinità della documentazione depositata e, ovviamente, i criminali si affrettavano a bonificare i fondi su altri conti correnti.

Interessante quindi osservare come meccanismi progettati per velocizzare le operazioni possono essere sfruttati per furti.

**********

**06- Errata corrige: Romania ed Europa**

La Romania è in Europa e lo so anche molto bene.

Però in un mio precedente post (http://blog.cesaregallotti.it/2023/05/accreditamento-ukas-non-piu-valido-per.html) l'ho indicata come esempio di Paese extra europeo. Volevo scrivere Albania.

Mi scuso con tutti e ringrazio Toto Zammataro per avermelo segnalato.

Il post l'ho corretto dove ho potuto.

**********

**07- Aggiornamento della ISO/IEC 29134:2023 Guidelines for privacy impact assessment**

A maggio 2023 è stata pubblicata la seconda edizione della ISO/IEC 29134:2023 "Guidelines for privacy impact assessment": https://www.iso.org/standard/86012.html.

Ripeto per l'ultima volta quanto già scritto altre volte quando parlavo delle bozze di questa seconda edizione: riporta solo aggiornamenti non significativi rispetto all'edizione precedente. Penso che sia è un peccato, visto che la norma richiederebbe un aggiornamento significativo, basato sull'esperienza maturata in questi anni.

**********

**08- Privacy: DL 48 e semplificazioni in materia di trasparenza**

Segnalo che è stato approvato il DL 48 del 2023: https://www.normattiva.it/eli/id/2023/05/04/23G00057/ORIGINAL.

Nell'articolo 26 riporta alcune semplificazioni nelle informazioni da fornire al personale,

introdotte dal D. Lgs. 104 del 2022 che a sua volta modificava il D. Lgs. 152 del 1997 (sulle informazioni da fornire ai lavoratori).

Poche cose, ma interessanti:

1- non è necessario copiare le norme, ma è sufficiente citarle; ritengo sia una buona cosa, purché le stesse norme siano facilmente comprensibili, e già il capoverso precedente segnala che spesso non è così;

2- "il datore di lavoro è tenuto a consegnare o a mettere a disposizione del personale, anche mediante pubblicazione sul sito web, i contratti collettivi nazionali, territoriali e aziendali, nonché gli eventuali regolamenti aziendali applicabili al rapporto di lavoro";

3- il datore di lavoro è tenuto a informare il lavoratore dell'utilizzo di sistemi decisionali o di monitoraggio.

Notizia appresa dalla circolare di B&C tax.

**********

**09- Gli uomini possono fare tutto (Giugno 2023)**

Questa volta, purtroppo, segnalo un insuccesso. Il 5 giugno alle 14 un mio figlio aveva la festicciola di classe a scuola. Il programma prevedeva un'esecuzione dei bambini di qualche canzone con l'ukulele (Yellow submarine e altre) e poi merenda con le cose portate da ciascuno.

Avevo già un appuntamento per quel pomeriggio e il cliente è stato molto gentile e riuscimmo a concordare una bella riduzione del mio impegno. Però, visto che avrebbe avuto un audit dopo qualche giorno, non annullammo completamente l'incontro. Così mi presentai a scuola alle 15, a concerto finito (ma a merenda ancora da cominciare).

Mio figlio mi fece un bel musone (ci tiene alla mia presenza, nonostante pensi ci siano papà sicuramente migliori di me) e, sinceramente, mi spiacque non essere arrivato per tempo.

Poi ho visto una registrazione di 10 secondi del concerto ed era anche carino. Però il dispiacere è un po' diminuito ;-)

**********

EONL

## Comments

Write a comment...