Infosec & Quality [ENG]- Jun. 2023

19 Jun 2023

Certosa di Pavia - June 2023 - Photo by me

Table of contents

****

01- NIST SP 800-124 on mobile device security

I recommend the publication of the SP 800-124 rev. 2 "Guidelines for Managing the Security of Mobile Devices in the Enterprise" of NIST: https://csrc.nist.gov/publications/detail/sp/800-124/re-2/final.

Excellent.

****

02- Draft of the Artificial Intelligence Act approved by the EU Parliament

I have not yet dealt with the regulatory proposals on artificial intelligence. The main reason is that these regulations are still in draft. Now the situation has advanced further and an article in Guerre di Rete allows us to understand the current situation (in Italian): https///guerredirete.substack.comnetwork-to-act-leuroparliament.

****

03- Threats and attacks: bug programmed in sports goggles

I recommend this article (in Italian) by Valeria Lazzaroli: https://www.linkedin.com/posts/valeria-lazzaroli_supplychain-cybersecurity-ip-activity-7059467324990341122-tIlx.

In a few words: a sports headset crashed (users were delighted) because the software license (by SWARG) was not updated by the hardware manufacturer (ORQA).

My comment (on LinkedIn): first of all you should understand if it is a bug or a feature. That is: the deadline was it stipulated in the contract between ORQA and SWARG or not? Certainly it was a bug for ORQA that seems to fall out of surprise.

I also wonder about the fact that now the software is sold "as a service", not "as a product" and that's a problem. Let me explain.

Software-as-a-service updates itself, whenever the manufacturer wants (you can always ask them not to, but this leads to other problems) and as the manufacturer wants. This generates availability risks (at least because usually updates happen without previous warning and block the system). This allows manufacturers to introduce licensing control systems, as in the ORQA case.

I repeat: there are pros and cons in this approach. We must be careful.

It is certain that SWARG could issue some warning that the license was about to expire.

****

04- Operation "Ghost money"

Enos D'Andrea told me the news (in Italian) about Operation "Ghost money": https://www.commissariatodips.it/notizie/articolo/operazione-ghost-money/index.html.

In short: the police arrested a gang that was stealing money simply by presenting fake SEPA warrants to banks. The credit institution provided the money before verifying the genuineness of the deposited documentation (for efficiency issues) and, of course, the criminals rushed to transfer the funds to other current accounts.

Interesting therefore to observe as mechanisms designed to speed up the operations can be exploited for thefts.

****

05- Update of ISO/IEC 29134:2023 Guidelines for privacy impact assessment

In May 2023, was issued the second edition of ISO/IEC 29134:2023 "Guidelines for privacy impact assessment": https://www.iso.org/standard/86012.htmlwaspublished.

I repeat for the last time what I already wrote about the drafts of this second edition: updates are not significant compared to the previous edition. I think that is a pity, since the standard would require a significant update, based on the experience gained in recent years.

****

06- Men can do everything (June 2023)

This time, unfortunately, I report a failure. On June 5 at 14 a son of mine had the class party at school. The program included a children's performance of some songs with ukulele (Yellow submarine and others) and then snacks brought by families.

I already had an appointment for that afternoon and the client was very kind and we were able to agree on a reduction in my commitment. However, since it would have an audit after a few days, we did not completely cancel the meeting. So I showed up at school at 15, at the end of the concert (but before the snack).

My son scolded me and, frankly, I was sorry not to have arrived in time.

Then I saw a 10-second recording of the concert and... well... the sorrow diminished a bit ;-)

****

EONL