Infosec & Quality [ENG] - Jul. 2023

24 Jul 2023

Levanzo. July 2023. Photo by me.

Table of contents

00- Editorial

01- Kevin Mitnick died

02- Enisa - Good Practices for Supply Chain Cybersecurity

03- New Privacy shield, i.e. "EU-US Data Privacy Framework"

04- Men can do everything (July 2023)

****

00- Editorial

As always, the newsletter comes out a bit late in July and stays on holiday in August. See you in September.

I wish you all a good summer.

****

01- Kevin Mitnick died

Kevin Mitnick, one of the most skilled hackers, has died. Not a great technician, but one with the ability to invent techniques to trick people into revealing passwords and other secrets.

I advise anyone involved in information security to read his first book, "The Art of Deception": https://en.wikipedia.org/wiki/The_Art_of_Deception. Although it is from 2002, so with obsolete technological references, it is still fundamental because technology is not so important.

I learned the news from Not Boring Privacy: https://www.instagram.com/p/Cu6GaqXtYnj/?igshid=MTc4MmM1YmI2Ng.

****

02- Enisa - Good Practices for Supply Chain Cybersecurity

Davide Giribaldi of Swiss Cyber Com recommended the Enisa's guide "Good Practices for Supply Chain Cybersecurity", released at the end of May: https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity.

I report the considerations of David and I thank him:

"The Guide is only about the operators of essential services (according to NIS Directive, that is going to be replaced by NIS2).

It highlights the organizational and cultural (not technical) difficulties in making third parties responsible (see fig. 6 p. 12 of the report) where a certification (e.g. ISO/IEC 27001) is an assurance tool (correct, but unfortunately too many companies see it as “another piece of paper”), but many companies have problems in auditing suppliers on the field.

In the report there are also interesting considerations about the approaches used for the supply chain IT risk assessment. Among these, I point out that the third most important item is the "expense" made towards the supplier.

Let's be clear: the more I spend on a supplier, the more I trust their products and services, but I don't think it's a meaningful element for evaluating cybersecurity".

****

03- New Privacy shield, i.e. "EU-US Data Privacy Framework"

Short recap: Privacy Shield, i.e. the agreement that regulated the transfer of personal data from Europe to the USA, was invalidated in July 2020. In July 2023, after exactly 3 years (minus a few days) the "EU-US Data Privacy Framework (DPF)" was approved: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721.

The website of the US DoC where you can find the requirements to join the program and the list of participants: https://www.dataprivacyframework.gov/.

Google is already on the list (as Not Boring Privacy tells us in Italian): https://www.instagram.com/p/Cu1vPbCNAJs/.

The new agreement has already been criticized: https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu.

I will suggest to my customers to continue to work as they have been doing for some years after the invalidation of the Privacy Shield. That is, maintaining IT systems in Europe or, at worst, using suppliers who adopt SCCs.

****

04- Men can do everything (July 2023)

Three of my clients I assisted in the preparation, had audits in the second half of June and first half of July. Unfortunately, the certification bodies changed dates and I have not been able to witnessed to all the days.

On the days I could, on the other hand, I always arrived a little later and always went out a little earlier to take the children to or pick up the children from summer camps. A struggle. I thank the auditors who did not ask philosophical questions in my absence and the clients who allowed me to do so.

****

Translated with the help of Microsoft Translator X.

EONL