WORKSHOP SCENARIO part 2

CONTEXT

It’s 2028, and you are working for a company called PODcorp. PODcorp has recently launched a device that allows near-instant transportation of people. The TELO-pod is a one-person capsule that can convert the user to data, transport them across the internet to a TELO-pod in their network, and rematerialize there. The person gets scanned on a quantum level. This information is stored locally until transmission is successfully verified by the receiving device and the person has rematerialized on the other side.

As this is a product with digital elements, PODcorp needs to comply with the CRA (amongst other legislation). Your job is to specifically, for the CRA, figure out what kind of activities the company needs to do in order to comply with the *vulnerability handling requirements* of the CRA. The technology of the TELO-pod is not our concern. Our concern is the safety of the user from the cybersecurity perspective of the product.

For the sake of this exercise, we will assume that whatever is needed to comply with the *vulnerability handling requirements* is available.

OBJECTIVE

Two months after the TELO-pod was launched on the EU market, a security researcher discovered a vulnerability. During the transmission of the user’s data across the internet, it is possible to manipulate the data via a man-in-the-middle attack.

The security researcher would now like to contact and inform you of the found vulnerability. As the product falls under the CRA, the vulnerability handling requirements must be fulfilled.

Your task is to check whether all activities are in place to handle that vulnerability.

Consider what activities a company like PODcorp needs to do in order to ensure that the vulnerability handling requirements are fulfilled.

Consider at least the following vulnerability handling stages:

- Sharing
- Preparation
- Discovery
- Validation and Triage
- Remediation
- Gaining Awareness
- Promote Deployment
- Post Release