UNIVERSITÄT LIECHTENSTEIN

Bachelor Thesis

Cybersecurity of the Power Grid

Interview questions

Instructions:

This presentation contains the questions (10 in total) that will be asked during the “live” interview.

The estimated length of the live interview is of 25 minutes.

Thank you very much for your participation!

Jacqueline Meyer

Risk assessment

1. How would you evaluate the current capabilities of the electricity sector to **prevent** cyber-incidents?

Not satisfactory — Satisfactory-good — Good-excellent

2. How would you evaluate the current capabilities of the electricity sector to **detect** cyber-incidents?

Not satisfactory — Satisfactory-good — Good-excellent

3. How would you evaluate the current capabilities of the electricity sector to **react** to cyber-incidents?

Not satisfactory — Satisfactory-good — Good-excellent

→ Which of the above mentioned phases of the security life cycle do you consider to be the most challenging for the companies handling power grids?

4. On a scale from 1-10, what *overall score* would you give to the cyber-security of the current national power grids?

1 Not satisfactory at all

5 Satisfactory, but there is room for improvement

10 Excellent

Risk assessment

5. Which of these measures do you think are the **three most suitable** approaches to improve the capabilities of private companies in the previously mentioned aspects of cyber-resilience (prevention, detection, reaction), please choose three?

- ○ The use of *penetration testing* for vulnerability assessment
- ○ Implementing security *standards*
- ○ *Outsourcing* of cyber-security tasks to specialized companies
- ○ Deploying *back-ups*
- ○ Using *data-replication* strategies
- ○ Promoting *educational activities* for management and employees
- ○ Analyzing past incidents that happened at the *own company*
- ○ *Sharing information* about previously happened incidents
- ○ Using *Artificial Intelligence* to secure systems
- ○ Implementing *Security-by-Design* approaches
- ○ Leveraging adequate *risk-assessment* approaches

6. For more detail on information sharing: On a scale from 1-10; how *willing* do you think are companies to share information about cyber-incidents?

a) Sharing information with you as *public authority*
b) Sharing information with *other private companies*
c) Sharing information with *academia* to elaborate new solutions

1	5	10
Cooperation is very difficult, companies reluctantly share information	Cooperation is generally satisfactory	Cooperation is excellent, companies willingly share all relevant information timely

Attack scenarios

7. Which of these attacks do you think represent both a feasible and severe threat to power grids?

- ○ Denial of Service
- ○ Malware (e.g. ransomware)
- ○ Advanced Persistent Threats
- ○ Man-in-the-Middle
- ○ Spoofing
- ○ Data breaches of individual *customer data*
- ○ False Data Injection
- ○ Others, please specify:

→ Why?

8. According to a 2021 report by Gartner, «Future malware will be able to *kill* or *harm* humans» by controlling physical equipment. Is a similar attack scenario realistically feasible in power grid contexts in your opinion?

○ It's unrealistic and/or impossible in power grids

○ It's a possible, but very unlikely scenario

○ It's a concrete and very likely threat

→ Can public authorities take action against such scenario? If so, what can be done exactly?

New technologies and trends

9. Which of the following future developments do you think has/will have the *largest impact* on cyber-security in power grids and the electricity sector within the next five years?

- ○ The use of *blockchain* technologies
- ○ The deployment of *Artificial Intelligence*
- ○ The widespread use of *cloud*-based solutions
- ○ The deployment of *IOT* devices
- ○ Others, please specify:

→ How do you take into account the above chosen topic when elaborating new policies/regulations?

10. How likely is it that private companies use their customer data in order to increase their profits?

○ Very unlikely

○ It's unlikely yet, but the probability of this is increasing

○ Very likely

→ If «Very likely» or «It's unlikely yet, but the probability of this is increasing»:
On a scale from 1 to 10, do you think that customers are *truly* aware of this?

1
They are not aware of this at all

5
They are aware of it, but it's not of major importance to them

10
They are aware of it and data confidentiality is crucial to them