UNIVERSITÄT LIECHTENSTEIN

Bachelor Thesis

Cybersecurity of the Power Grid

Interview questions

Instructions:

This presentation contains the questions (30 in total) that will be asked during the “live” interview.

The first 27 are ‘closed’ and general questions, potentially leading to short follow-up comments. The remaining 3 are ‘open’ questions, which should be tailored for your specific company.

The estimated length of the live interview is of 45 minutes.

Jacqueline Meyer

Experiences with cyber-attacks

1. How many cyber-attacks have you suffered *since 2012* at your company?

None | 1-5 | More than 5

→ If no, are you certain? / If yes, were they a cause of concern?

2. Do you use *penetration testing* as a means to perform vulnerability assessment of your systems?

No | No, but we are planning to do so | Yes

→ If no, why ? Do you apply similar methods?

3. Do you implement *security-by-design* principles?

No | No, but we are planning to do so | Yes

4. Do you implement any *security standards* (e.g. NISTIR 7628) at your company?

No | No, but we are planning to do so | Yes

General questions on security landscape

5. How is cybersecurity *managed* in your company?

- Everything is done completely in-house
- Mostly in-house, minority oustourced
- Mostly outsourced, minority in-house
- Completely outsourced

6. Do you apply *back-up* strategies at your company?

- No
- Yes, we have *local* back-up
- Yes, we have back-ups in the *cloud*
- Yes, we have back-ups both locally and in the cloud

7. Do you apply *data-replication* strategies as well?

8. In general, do you use *cloud*-based solutions for your IT systems (not necessarily for cybersecurity)?

- No, not at all
- No, but we are planning to do so
- Yes, we do

→ If yes, are there any additional risks arising from that? If no, why not?

→ Based on which national regulations are the deployed cloud solutions organised? E.g. EU regulations, US regulations, etc.

9. On a scale from 1 to 10, how problematic is *data confidentiality* for your company?

1 — Not problematic at all, we do not deal with sensitive customer data

5 — Problematic, but not major concern

10 — Highly problematic

Risk assessment

10. Do you use *qualitative* or *quantitative* approaches for risk-assessment?

- Only quantitative approaches
- Only quantitative approaches
- Both

11. Of the three steps of the security life cycle (*prevention, detection, reaction*) which one do you consider to be the **most** challenging?

12. Between *physical*-security (e.g. resilience against earthquakes) and *cyber*-security, which one do you think is more important to your company?

- Physical security is more important
- Both are equally important
- Cyber-security is more important

13. During your **risk assessment**, do you analyse past incidents that happened at *your* company?

- No
- No, but we are planning to do so
- Yes

14. During your **risk assessment**, do you analyse past incidents that happened at *other similar* companies?

- No
- No, but we are planning to do so
- Yes

→ If you use detailed historical data to analyse past incidents, is it *costly* to obtain and manage such data?

Risk assessment

15. Cyber-resilience is often associated with *cyber-security education* --- spanning from low level employees to mid-and top-level management. Do you think that your company is well-equipped to deal with that aspect?

Mid-/Top-level management:

- ○ They are aware of the risks and put cyber-security among their *priorities*
- ○ They are aware of the risks, but cyber-security is *overlooked* in favor of other more important areas for production
- ○ They are *not aware* of the risks, but the company is actively promoting educational activities focused on this specific aspect

Employees:

- ○ They are aware of the risks and of the *best practices* to avoid such risks and such education is periodically evaluated
- ○ They are not aware of the risks, but the company is *actively promoting* educational activities focused on this specific aspect
- ○ They are not aware of the risks, and *unlikely to improve* their education in the short-term future

→ If you have training measures in place, how do they look like?

Attack scenarios

16. Consider an attacker that could **access *individual* consumer data** (e.g. energy consumption) in your systems. How *threatening* would that be for your company ?

○ Not threatening ○ Midly threatening ○ Highly threatening

→ Why?

17. Is your company threatened by **Denial of Service** attacks?

○ Not threatening ○ Midly threatening ○ Highly threatening

→ Which of your systems are especially at risk to be a target of DOS?

18. Do you use **smart meters** at your company and if yes, which percentage of meters has already been replaced by smart meters?

Attack scenarios

19. 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 relistically feasible in your company?

- ○ It's unrealistic and/or impossible in our company
- ○ It's a possible, but very unlikely scenario
- ○ It's a concrete and very likely threat

20. How likely is it for attackers to cause *malfunction* of your equipment (e.g. by having PLC or breaker misbehave)?

- ○ Very unlikely
- ○ It's likely, but not a cause for major concern
- ○ Very likely

21. How much are you endangered by *Advanced Persistent Threat*?

- ○ We are not endangered
- ○ There is some risk, but not major
- ○ We are at a high-risk to be attacked by APT

Attack scenarios

22. How likely are *False Data Injection* attacks to your systems?

○ Very unlikely ○ It's likely, but it's not a cause for major concern ○ Very likely

23. How likely are *man-in-the-middle* attacks to occur in your IT systems?

○ Very unlikely ○ It's likely, but it's not a cause for major concern ○ Very likely

24. Is your company at risk from *spoofing* attacks?

○ No ○ Yes, but they are not very significant ○ Yes, they are a major cause of concern

→ Are any *countermeasures* in place to defend agains such threats?

New technologies

25. Do you think that *blockchain* will be used in the future by your or related companies?

- ○ No
- ○ Unlikely to be ever used
- ○ Yes, it will provide some benefit, but only in the long term
- ○ Yes, it will be a crucial technology

26. Do you use *artificial intelligence* tools for securing your systems?

- ○ No
- ○ No, but we plan to do so
- ○ Yes, but not for critical applications
- ○ Yes, for a lot of tasks

→ If no, why not? If yes, are there any additional challenges arising from that?

27. Do you leverage *IOT (Internet of Things) devices* in your company?

- ○ No
- ○ No, but we plan to do so
- ○ Yes, but not for critical applications
- ○ Yes, for a lot of tasks

→ If no, why not? If yes, are you aware of the security risks arising from these devices?

Open questions

- Individual questions for each company.

Appendix

- Qualitative approaches for risk assessment: evaluate probabilities and consequences of risks with methods like brainstorming or workshops and not using formulas.
- Quantitative approaches for risk assessment: calculate probabilities of risks using formulas and mathematical simulation techniques, e.g. Monte Carlo simulations.