Assignment H1

Read / watch / listen and summarize (This subtask x does not require tests with a computer. Some bullets per article is enough for your summary, feel free to write more if you like. Add some question or idea of your own.)

Threat modelling

Threat modelling is defined as the analysis possible issues with security and privacy of a system. The article in its entirety showcases the reasons behind the threat modelling manifesto, highlighting its values and principles. It also specifies patterns that benefit the modelling, such as using a systematic approach, allowing for informed creativity from a diversified team that uses specific toolkits created for these specific purposes. Patterns that do not align with the vision of the manifesto are also explained, like loosing the overall picture of the system by focusing of some specific parts of it or not creating multiple threat modelling representations.

The second source is a YouTube playlist of multiple short videos, where the concept of threat modelling is presented. Some of the covered topics are similar to the ones present in the previously mentioned manifesto, but it also highlights possible common issues that might arise while analysing possible threats.

The third source is another introduction to the threat modelling concept, and it covers the concepts already present in the manifesto. It also highlights possible advantages of using this model, like increasing security awareness. After explaining the benefits of this model, common techniques are briefly described, and common challenges and possible solutions to said challenges are presented.

Security hygiene

Some of the basic security practices that I think everyone should follow are the following:

- Having strong passwords that are not re-used for multiples services
- Enabling two factor authentication
- Pay attention when receiving email, since fake ones can be quite deceiving
- Have multiple and regular backups

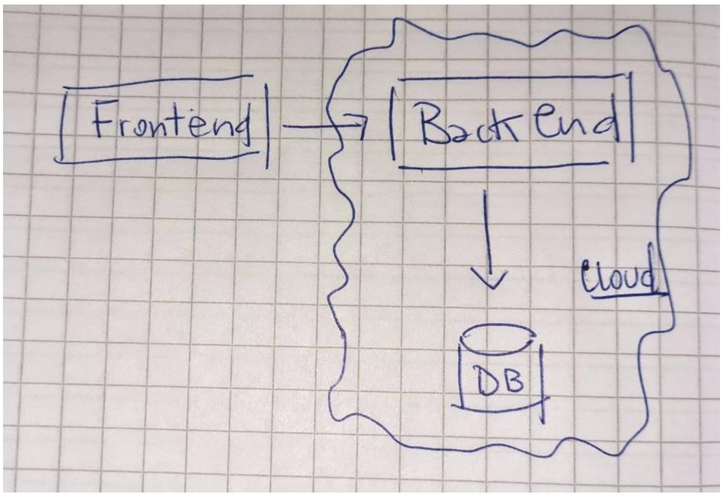
Make belief boogie man

1) What are we working on?

Imagining an imaginary tech company leading in a specific field, one needs to recognize their assets. Personally I identiefied the following:

- User personal informations
- Company's secrets on current and future projects
- Payment methods and company's funding and accounting

Company systems diagram



2) What can go wrong

Using the STRIDE model, what I was able to identiy the following poossible issues:

- Spoofing: social engineering to enter our systems from the “main door”
- Tampering: possible ransomware attacks
- Repudiation: unauthorized data deletion
- Information disclosure: interception of private data that is not correctly encrypted
- Denial of service: malicious interruption of our services
- Elevation of privileges: correlated to spoofing, where a compromised employee gains new privileges.

3) What are we going to do about it

- Regular employees security trainings
- Constant monitoring of the whole system
- Creation of an incidfdent response plan
- Better overall security related to the current codebase of the company

4) Did we do good enough job?

Especially when working in companies that offer online services, one cannot ever be satisifed with their security work since the attacks have to be considered continuing and constant. Keeping the employees aware of the possible risks is crucial to avoiding possible breaches.