Research Proposal Outline

Project Title:

Threat modelling framework for small businesses

Significance/Contribution to the discipline/Research Problem:

Existing threat modelling frameworks assume that the threat modeler has a significant level of understanding of cybersecurity concepts. However, this is not the case in small businesses, where it is rarely possible to employ a cybersecurity expert due to budget constraints. Although there are some commercial tools tailored for SMEs, they are either still too complicated for non-technical stakeholders, or they are just suggestion tools that lack a framework that provides a theoretical background to help stakeholders develop a security-focused way of thinking. The new framework aims to help SME stakeholders develop a proactive, cybersecurity-oriented mindset.

Research Question:

How can existing threat modelling frameworks can be incorporated into a non-technical framework so that small businesses can model the cybersecurity threats they face in the absence of a cybersecurity expert?

Aims and Objectives:

- Explore how small businesses approach cybersecurity.
- Identify the pitfalls small businesses face in their cybersecurity efforts.
- Design a non-technical threat modelling framework that can be easily used by small business stakeholders without a computer/cybersecurity background.

- Develop a web-based application to help small business stakeholders identify potential cybersecurity risks and mitigations.

Key literature related to the project:

TBD

Methodology/Development strategy/Research Design:

Research and development will be conducted in 7 steps:

1. Literature review on the current state of research on cybersecurity in small and medium-sized enterprises.
2. An initial qualitative survey to explore how cybersecurity is handled in small businesses and the pitfalls they encounter.
3. Analysis of the initial survey results and identification of the problem areas.
4. Identification of threat modelling frameworks that are relevant to small businesses.
5. Incorporating identified threat modelling frameworks into a non-technical framework.
6. Implementation of a threat-modelling framework into a web-based suggestion tool.
7. Follow-up survey on how small businesses perceive the new tool and assess its impact on business cybersecurity.

Ethical considerations and risk assessment:

Small business stakeholders (i.e. business owners, managers, etc.) will be approached by using their publicly available contact details (i.e. those available on their website) and their consent to participate in the initial survey will be sought.

Consent to participate in the follow-up survey will be sought during the initial survey, and those who do not give explicit consent will not be contacted for the follow-up survey.

The results will be presented in an unbiased, objective manner, regardless of whether they support or refute the main objective of the research.

Description of artefact(s) that will be created:

As a result of the research, two artifacts will be created:

1. Threat Modelling Framework for Small Businesses:

A threat modelling framework specifically designed for small businesses that lack cybersecurity knowledge and expertise. The framework will incorporate widely accepted threat modelling frameworks such as STRIDE or DREAD, as well as the MITRE ATT&CK framework. Of possible, the new framework will follow an easy to remember mnemonic. The main objectives are (1) to design a framework that is compliant with industry standards, (2) to provide small business stakeholders without a computer/cybersecurity background with an easy-to-use framework that will help them identify the cybersecurity threats to their business and mitigate against them.

2. Threat Modelling Application:

A web-based application that will be based on the framework designed. It will have an intuitive and easy to use GUI that will help users to identify the threats that their organisation faces. The application will also provide a visual attack tree, calculate an overall cybersecurity rating and suggest mitigation measures for the identified threats.

Timeline of proposed activities:

(Gnatt Chart)

1. Literature review (3 weeks)

2. Preparation of initial survey and application for ethical approval (1 week)

3. Contact small businesses and collect survey results (4 weeks)

4. Analysis of initial survey results (1 week)

5. Research industry accepted threat modelling frameworks and identify those applicable to small businesses (2 weeks, overlapping with previous steps)

6. Design of the new threat modelling framework (2 weeks, overlapping with previous steps)

7. Develop, deploy and test the web application (10 weeks)

8. Contact small businesses for follow-up survey and collect results (4 weeks)

9. Analysis of follow-up survey results (1 week)

10. Writing the final report (4 weeks, overlapping with previous steps)