Appendix D

Initial project proposal

D.1 Title

Designing a Cyber-Secure Infrastructure for Accounting Firms in Belgium: A Modular Approach Using EaC, TDD, and CI/CD Aligned with the CyFun Framework

D.2 Proposal summary

This project aims to design a secure IT infrastructure tailored to the needs of small and medium enterprises (SMEs) using modern paradigms such as Everything as Code (EaC), Test-Driven Development (TDD), and Continuous Integration/Continuous Deployment (CI/CD). The infrastructure will align with the CyFun cybersecurity framework established by the Belgian Cybersecurity Centre (CCB), focusing on compliance with the NIS2 directive's initial level. By implementing a flexible, reusable infrastructure design, this project will facilitate streamlined cybersecurity practices for SMEs.

D.2.1 Participants

Project Director/Owner: Jêrome Dossogne
Researchers(s):

- Querinjean Arnaud

D.2.2 Background

Small and Medium sized enterprises (SMEs) are very important to the global economy. Representing a significant portion of businesses and 60 per cent of employment. [11] Despite their importance, SMEs often lack the resources and expertise to implement robust cybersecurity measures [2] (This vulnerability is particularly critical in the accounting sector, where companies process sensitive financial data and are subject to strict regulatory requirements.) The CyFun framework developed by the Belgian Cybersecurity Centre (CCB) provides a structured cybersecurity approach that aligns with the NIS2 Directive for critical infrastructure protection. The NIS2 directive sets cybersecurity standards for essential and digital services providers, including SMEs in regulated sectors.

D.2.3 Objectives

The goal of this project is to develop a secure IT infrastructure for SMEs that complies with CCB standards by following these steps:

- **Needs Analysis**: Conduct a study of IT security requirements for accountancy firms in Belgium. This will include a literature review and interviews with at least 3 accountancy firms to gather data.

- **Establish a Sector Profile**: Build a generic profile that represents the common characteristics and requirements of accountancy firms in terms of cybersecurity. This will involve using statistical analysis of the firms' responses to identify common characteristics and validate our hypothesis.

- **Develop a Secure, Modular Infrastructure**: Utilize tools such as Ansible for automated deployment, Docker for containerisation, and Github for CI/CD.

D.2.4 Expected Outcome

The project will produce a number of deliverables:

- **A Sector Profile Report**: A study of the cybersecurity needs of Belgian accountancy firms, focusing on the common characteristics of SMEs in this sector.

- **A Prototype Secure Infrastructure**: A modular and secure infrastructure prototype developed based on the established sector profile.

- **A Master Thesis**: A comprehensive document that details the research, implementation, and analysis conducted throughout the project.

- **A Draft of a White Paper**: A draft document that can be further modified and improved upon for the research lab to consider publishing at a later date (with or without the student's further collaboration, upon their preference).

D.3 Proposal description (max. 4 pages, ref's included)

D.3.1 Aim of the study and relevance for designated target group

The aim of this study is to develop a modular and secure IT infrastructure tailored to the cybersecurity needs of accounting firms in Belgium, aligning with the CCB's standards. This infrastructure will address the unique challenges faced by SMEs in the accounting sector, providing a scalable and resource-efficient solution. According to recent findings [3], SMEs, especially in financial sectors, are increasingly targeted by cyber threats due to limited resources in cybersecurity. But they also face a lack of awareness and therefore a lack of adequate protection [2] for critical and sensitive information, which makes the implementation of secure infrastructures even more crucial.

D.3.2 State of the art

-Cybersecurity Challenges for SMEs in Belgium (challenges for the accounting sector)
SMEs often lack the resources and expertise to implement robust cybersecurity measures, making them prime targets for cyber-attacks [2]
-CyFun Framework (BASIC) (Analyze the role of compliance standards and regulatory frameworks) The CyFun framework is designed to help Belgian organizations, including SMEs, achieve a baseline level of cybersecurity
- key infrastructure paradigms: Everything as Code (EaC), Test-Driven Development (TDD), and CI/CD

D.3.3 Global research context

D.3.4 Research strategy

The research will begin with a literature review to understand the cybersecurity needs of accountancy firms. Following this, a needs analysis will be conducted through structured interviews with five accountancy firms to gather specific data. The collected data will then be analyzed statistically to identify and confirm common cybersecurity requirements. Based on these findings, a secure infrastructure will be developed using tools such as Ansible for automated deployment, Github for CI/CD.

D.3.5 Collaboration

This project will involve collaboration with Ilyas Bakhat, who is focusing on user behavior simulation ?

D.3.6 Expected outcome

The expected outcomes include a sector profile report, a prototype infrastructure, a master thesis and a white paper. These will help SMEs and accountancy firms in the field of cybersecurity.

D.3.7 Feasibility & risks

Feasibility

As far as the feasibility of the project is concerned, I've got the cybersecurity and DevSecOps skills from my background. I also have the resources to be in contact with SME companies, and the collaboration with my supervisor. The project is scheduled for an academic year, which will give me time to research, develop and test part of the infrastructure and write my master's thesis.

Risk

The risks could be that I don't have enough data from the companies I have contacted. But also the risk that implementing and ensuring compliance with Cyfun may prove difficult.

D.3.8 References

D.4 Phasing of the Project (max. 4 pages)

D.4.1 Workpackage 1: Integration and Initial Planning

Start date: Mid-October 2024
End date: End of October 2024

Description

This first work package focuses on joining the research group and setting up initial plans for the project, including meetings and defining project goals.

S.M.A.R.T. Objectives

- Join research group channels and access necessary resources.
- Schedule project meetings and create a project timeline.
- Review and adjust project goals based on feedback.

Deliverables and K.P.I.s

- IPP approved by the supervisor.
- Document summarizing initial goals and communication plan.

—

D.4.2 Workpackage 2: Technology Research and Literature Review

Start date: Early November 2024
End date: End of November 2024

Description

This phase involves gathering information on cybersecurity for SMEs and setting up tools to track relevant technology updates.

S.M.A.R.T. Objectives

- Find and organize key literature on cybersecurity, EaC, TDD, and CI/CD.
- Set up a system (e.g., Zotero) to track relevant publications.
- Identify and document at least 20 useful sources.

Deliverables and K.P.I.s

- Annotated bibliography with key sources.
- Technology tracking system set up in Zotero.

—

D.4.3 Workpackage 3: State of the Art and Requirements Analysis

Start date: Early December 2024
End date: End of December 2024

Description

This package is about reviewing current technologies and defining the specific security needs for accounting firms.

S.M.A.R.T. Objectives

- List and classify at least 10 tools and technologies.
- Document specific security needs for accounting firms.
- Analyze and compare available solutions to project needs.

Deliverables and K.P.I.s

- Draft of the State of the Art chapter.
- Document detailing security requirements.

—

D.4.4 Workpackage 4: Roadmap and Project Design

Start date: Early January 2025
End date: End of January 2025

Description

This phase involves finalizing the project roadmap and designing the secure infrastructure layout.

S.M.A.R.T. Objectives

- Develop a complete roadmap with clear tasks and deadlines.
- Design the main components of the secure infrastructure.
- Adjust the roadmap based on feedback from the supervisor.

Deliverables and K.P.I.s

- Approved project roadmap.
- Initial infrastructure design document.

—

D.4.5 Workpackage 5: Prototype Development and Testing

Start date: Early February 2025
End date: End of March 2025

Description

This package focuses on creating the first working version of the infrastructure and testing its basic functions.

S.M.A.R.T. Objectives

- Build the prototype using Ansible, Docker, and GitLab.
- Run at least three test cycles to ensure functionality.
- Adjust prototype based on test results.

Deliverables and K.P.I.s

- Working prototype that passes initial tests.
- Document showing test results and adjustments made.

—

D.4.6 Workpackage 6: Validation and Security Improvements

Start date: Early April 2025
End date: End of April 2025

Description

This phase includes validating the prototype's security and making necessary adjustments to meet compliance standards.

S.M.A.R.T. Objectives

- Perform at least five security tests on the prototype.
- Improve the prototype based on test feedback.
- Ensure prototype meets CCB and GDPR standards.

Deliverables and K.P.I.s

- Security report showing test results.
- Updated prototype meeting security standards.

—

D.4.7 Workpackage 7: Documentation and Thesis Writing

Start date: Early May 2025
End date: End of May 2025

Description

This package involves documenting the project and completing the thesis draft.

S.M.A.R.T. Objectives

- Write the thesis draft covering all parts of the project.
- Organize detailed documentation of the prototype and processes.
- Submit draft by end of May 2025.

Deliverables and K.P.I.s

- Full thesis draft for supervisor review.
- Complete documentation of the project.

—

D.4.8 Workpackage 8: Final Presentation and Review

Start date: Early June 2025
End date: End of June 2025

Description

This final package focuses on preparing and presenting the project results and finalizing the thesis.

S.M.A.R.T. Objectives

- Prepare and practice a presentation summarizing project goals, methods, and results.
- Review and finalize the thesis with feedback.
- Submit final thesis and presentation materials.

Deliverables and K.P.I.s

- Final presentation ready for defense.
- Submitted and approved thesis.

D.4.9 Summary Timeline

- **Mid-Oct - Nov 2024**: Integration and initial planning.
- **Nov - Dec 2024**: Technology intelligence and literature review.
- **Dec 2024 - Jan 2025**: State of the Art and requirements analysis.
- **Jan - March 2025**: Prototype development and testing.
- **Apr - May 2025**: Validation and security evaluation.
- **May - June 2025**: Thesis writing and documentation.
- **June 2025**: Final presentation, review, and submission.
- **June 2025**: Preparation for publication and peer review.

D.5 Expertise of the project's research team (max. 2 pages)

D.5.1 Expertise

D.5.2 Publications & porfolio relevant to the project proposal

D.6 Requirement (equipment, skills, ...)

D.7 Proposal Summary Table (max. 2 pages)

Domain: Cybersecurity and IT infrastructure.

Study Director: Jerome Dossogne

Research Unit/Staff/Department: ?

Title: Designing a Secure IT Infrastructure for Accounting Firms.

Aim of the Study: To create a secure, reusable IT infrastructure that meets cybersecurity needs for small and medium accounting firms.

Research Strategy: Using Everything as Code (EaC), Test-Driven Development (TDD), and CI/CD to build, test, and improve the infrastructure.

Innovative Character: Focuses on a modular approach using automation and continuous testing, specifically tailored for accounting firms.

Target Group & Relevance for That Audience: Accounting firms and SMEs who need stronger cybersecurity with limited resources.

Partnerships: Collaboration with research group and Ilyas Bakhat's project.

D.8 Evaluation & Self-Evaluation

D.8.1 Self-Evaluation

- ... /10: Relevance and scope : Is the relevance of the proposed research well defined? Is the scope of project well described and delimited?

- ... /10: Efficiency : Are the required/allocated means means, i.e. personnel, infrastructure and equipment, consistent with the projected outcome of the project?

- ... /10: State of the Art : How is the state of the art, related to this proposal at a national and international level, described? Are the proposers aware of past and current similar research activities?

- ... /10: Research Strategy and Phasing : Are the phases of the project realistic, coherent and in line with the intended objectives? How realistic and well argumented are the objectives? Is the research team well organized and able to perform the planned research

- Remarks:

D.8.2 Evaluation

- ... /10: Relevance and scope

- ... /10: Efficiency

- ... /10: State of the Art

- ... /10: Research Strategy and Phasing
- Remarks:

Appendix E

Project management records / artifacts

E.1 Gantt charts

E.2 Pomodoro charts

E.3 Agile Methodology's User stories

E.4 Workpackages, Objectives and tasks

E.5 Diagrams & user produced artifacts: use cases, user stories, UML, ...