|  |
| --- |
|  |
| BA-Thesis:  Plant network priming  Task Definition  **Henrik Ekholm**  **V0.1 14.08.2021** |
| **Berner Fachhochschule**  Departement Technik und Informatik |

Index

[Task Definition 1](#_Toc79862493)

[Index 2](#_Toc79862494)

[1 General 3](#_Toc79862495)

[1.1 Purpose of Document 3](#_Toc79862496)

[1.2 Definitions and Abbreviations 3](#_Toc79862497)

[1.3 Version Control 3](#_Toc79862498)

[1.4 Confirmations 3](#_Toc79862499)

[1.5 References 3](#_Toc79862500)

[2 Task Definition 4](#_Toc79862501)

[2.1 Starting Position 4](#_Toc79862502)

[2.2 Goals and Deliverables 4](#_Toc79862503)

[2.2.1 Soll Ziele 4](#_Toc79862504)

[2.2.2 Kann-Ziele 4](#_Toc79862505)

[2.2.3 Qualitätsziele 4](#_Toc79862506)

[2.3 Learning 5](#_Toc79862507)

[2.4 Risk Analysis 5](#_Toc79862508)

[3 ORGANISATION 5](#_Toc79862509)

[3.1 Included Persons 5](#_Toc79862510)

[3.2 Dates 5](#_Toc79862511)

[4 Results 5](#_Toc79862512)

[4.1 Proof of Concept 5](#_Toc79862513)

[4.2 Dokumente 5](#_Toc79862514)

[4.3 Delivery 6](#_Toc79862515)

# General

## Purpose of Document

This document is to define and scope the Final Project Practical OT security.

## Definitions and Abbreviations

|  |  |
| --- | --- |
| **Abbreviation** | **Explanation** |
| POC | Proof of concept |
|  |  |

## Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Datum** | **Description** | **Autor** |
| 0.1 | 14.08.2021 | Document Creation | Henrik Ekholm |
| 0.2 | 18.08.2021 | First Draft completed | Henrik Ekholm |
| 0.3 | 12.10.2021 | Expert known details added |  |

## Confirmations

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Function** | **Datum** | **Signature** |
| Prof. Dr. Bruce Nikkel | Supervisor |  |  |
| Dr. Igor Metz | Expert |  |  |
| Herr Henrik Ekholm | Student |  |  |

## References

|  |  |  |
| --- | --- | --- |
| **Ref.** | **Author** | **Document** |
|  |  |  |
|  |  |  |
|  |  |  |

# Task Definition

## Introduction

Securing networks mainly used for modern computers has been the main concern in IT-Security for as long as it exists, and we therefore have many effective and good ways to protect and monitor these systems. What traditionally has been neglected are the production systems, systems standing in Plants, producing our everyday goods. These PLC machines, use properitary communication protocols which can be affected simply be monitoring them, and their function is usually specialised in a manner where other tools can not be installed on the same devices. This gives us the question, how do we protect these exceptionally fragile machines from malicious intent, especially now that many threat actors have switched their focus from the financial sectors to the producing ones?

## Starting Position

Currently the majority of the Companys manufacturing plants are on corporate network, the same network as our Laptops, servers other office equipment. There is currently a project underway to segment these networks off, but as they rely on outside data and connection to ERP systems on our servers some communication is required, so far less than a third has been segmented and of those none is segmented in a way that no attack vector remains.

There exists reference architecture that describes what devices need to be segmented, and into what VLANS behind the firewall they belong in, but no details on how outside communication needs to be handled except for the call for a Jump-Server. Additionally the document has not been updated to match our findings.

During the Segmentation Project, multiple exceptionally old devices were discovered to be in use, a second project has been started to renew this hardware. Kickoff was the 1.8.2021.

The Network is segmented with Palo alto firewalls, the logs are monitored.

## Goals and Deliverables

The goal of the project is to improve the security of the company’s plants. Especially in regards to the Network monitoring and Network forensic capabilities.

To this end, a POC will be created in one of the plants scheduled for segmentation. To make it possible to implement the same solutions for other plants, a handbook shall be created to guide the process. And to verify the setup, a reference architecture will be designed.

To design the layout, in minimum the following techniques shall be reviewed:

Honeypots and specificylly for the network Sinkholing realised by proxying

Jump Hosts for no direct access in or out of the protected network

Canary servers for early detection.

## Learning

This project will teach both design of a secure system as well as implementation in a business environment.

## Risk Analysis

This project relies for its practical part on support from a fortune 500 company with more than 50'000 employees. Funding for these projects come from Supply chain, Support from other teams such as networking, production and server are necessary. Should that support become unavailable, the possible scope of the POC will decrease.

# ORGANISATION

## Included Persons

|  |  |  |
| --- | --- | --- |
| **Name.** | **Funktion** | **E-mail** |
| Prof. Dr. Bruce Nikkel | Supervisor | bruce.nikkel@bfh.ch |
| Dr. Igor Metz | Expert | metz@glue.ch |
| Herr Henrik Ekholm | Student | Ekhoh1@bfh.ch |

# Results

## Proof of Concept

The proof of concept will be realized in a as of yet defined Plant in Europe. Access can not be granted, but a guided walkthrough of the concept is pending approval.

## Documents

A report of the project consisting of the following parts:

1. Tasks
2. Problem analysis
3. Design process
4. Implementation Process

A reference architecture to be used for further plants

An implementation Handbook

## Delivery

Delivery dates and form are as follows:

|  |  |  |
| --- | --- | --- |
| **Date** | **Was** | **Wo** |
| 30.8.2020 | Task Definitions | E-mail |
| 21.1.2021, 20:00 | Film | Moodle |

Additionally, a GitLab or SharePoint site will be set up where all the involved can review the current status.