|  |
| --- |
|  |
|  |

|  |  |
| --- | --- |
| Security Enhancements for Network Segregation | |
| How to prepare a production network for attack | |
| **Bachelor thesis** | |
| Degree programme: | Bachelor of Science Computer Science |
| Author: | Henrik Ekholm |
| Thesis advisor: | Dr. Bruce Nikkel |
| Expert: | Dr. Igor Metz |
| Date: | 20.01.2022 |

# Management Summary

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 proprietary communication protocols which can be affected simply be monitoring them, and their function is usually specialized in a manner where other tools cannot 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?

Contents

[1 Management Summary 2](#_Toc94061218)

[2 Introduction 4](#_Toc94061219)

[3 Project Steps 5](#_Toc94061220)

[4 Journal 7](#_Toc94061221)

[5 Conclusion 8](#_Toc94061222)

[6 List of illustrations 9](#_Toc94061223)

[7 Contents of the table 9](#_Toc94061224)

[8 Glossary 9](#_Toc94061225)

[9 References 9](#_Toc94061226)

[10 Appendix A: Handbook for integration 9](#_Toc94061227)

[11 Declaration of Authorship 10](#_Toc94061228)

# Introduction

## 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 proprietary communication protocols which can be affected simply be monitoring them, and their function is usually specialized 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 specifically for the network Sinkholing realized 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.

# Project Steps

## Problem/Threat Review

### Internal works and their ramifications

"Mastering the Fourth Industrial Revolution" was the 2016 theme of the World Economic Forum, in the same year, Ecolab decided to implement the core ideas in its strategy for the future of plant development. Since then, the amount of integrated or smart systems in our plants have grown significantly, but with very limited oversight from IT.

These new OT systems whereas much of our infrastructure at the time, neither properly managed nor did we have a proper inventory, as the procurement, installation and maintenance were done on the authority of the plants.

Late 2018 we invested in a vulnerability scan solution from Qualys, which we ran to get a full overview of our current Inventory and security posture.

This brought down one of our production lines, which lead to the plants moving their production equipment to separate VLANS or at least gave us a rough overview of the inventory.

### Threats

Before we can start to work on solutions, we need to understand the threats that we face. Working with both the plants, supply chain and external security partners, we established a few main concerns which can be broadly stated as two categories:

Ransomware where the plan is to take our systems or our production data ransom for money, and IP loss where the plan would be to steal our data to sell if for financial gain.

In addition to these two general issues, we also need to keep in mind a potential state funded disruption attack, as we are considered an essential service by the US government.

### Foundation

Back in 1990 the Purdue University released an architecture diagram to be used for segmenting plant networks. The main idea being to separate the whole network into 5 levels, clearly making a cut between Manufacturing and enterprise systems.[[1]](#footnote-1)

In 2019 Cisco released a paper in collaboration with Rockwell which outlines the current problem with securing OT systems in an IT environment, and a few design proposals on how to secure such a system the model plant uses both Rockwell and Cisco devices, it seems like a good starting point[[2]](#footnote-2)

## Plan of action

### Segmentation

To be able to protect the OT network form the IT, first a segmentation is needed.

This is best accomplished by Firewall, and as already mentioned, this part is underway.

### Control Data flow

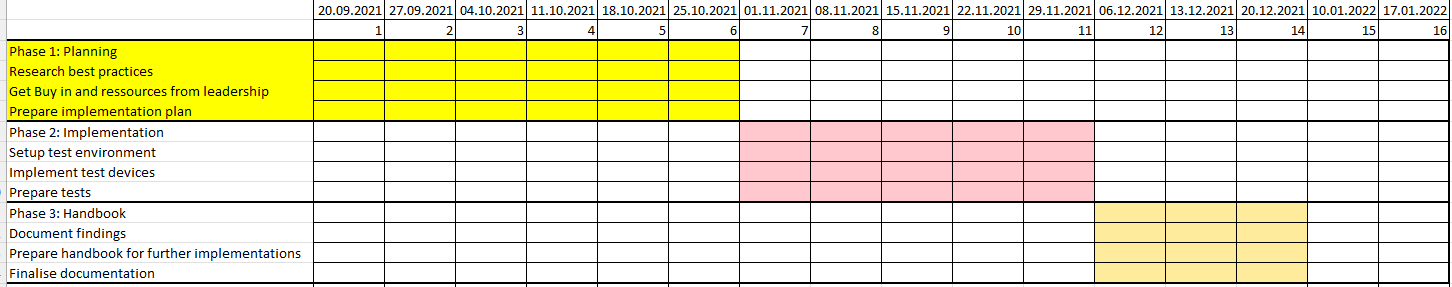
Monitor what data comes in, and what data leaves the OT network.

### Get visibility

See what goes on inside the segmented part.

## Project Plan

Time planning is in three phases as seen below



First phase is to come up with a plan on what is needed for the improvements to happen.

Second phase is the implementation in a test environment.

Third Phase is the Documentation and operationalisation of the system.

## Segmentation

Rockwell recommends that all systems in the plant, including the OT firewall and the entire production network are run by plant engineers, this would give them the autonomy they need to run it efficiently while not enforcing unexpected maintenance cycles during production times.

Proposing that idea met with some reservations: most of our plants do not have the technical know-how to do proper network maintenance or to configure a firewall. If they cannot run and maintain the full network, then what is to be done by the corporate teams, and what access is needed.

Proper implementation also requires 2 firewalls, one for the plant and one for enterprise IT to manage. As the plants lack the resources to manage their own firewall, and out of cost reasons, the compromise to only use one was reached.

Next, to manage and control the network itself certain firewall rules were created as standard. These can be found in the Handbook.

As the access to the AD-Server requires quite liberally open ports, it was decided that all devices in the OT network run with local accounts.

With the same argument, fixed IP addresses were used (with the option for the plants to use their own, internal DHCP servers).

The VLAN allocations were already done in an earlier project but left in the Handbook for reference.

## Remote access

Especially during the current times, the plants have relied heavily on remotely being able to monitor and manage their systems. As they are now segmented behind a firewall, a solution was needed.

The basic requirements were as follows:

* The access needs to be controlled by AD access groups
* Connection Brokered by PAM
* Every connection needs to be monitored and preferably recorded
* Access only through a jump server

I compared 4 of the industry leading ones:

CyberArk Privileged Access Security

BeyondTrust Privilege Management

ARCON Privileged Access Management

WALLIX Bastion

But the decision was made for me, as it turned out our server team had already been using BeyonTrust for a while, and it was just a question of extending the contract.

## Internet Access

As almost all systems are reliant on some form of internet connectivity, be it to update their systems or for Licensing purpose internet access is needed.

For this purpose a second DNS server was installed as Sinkhole. The idea of a sinkhole DNS is that all requests that are known to be bad are dropped. In our case, it was set up to drop all requests that were not specifically permitted.

In addition, for those cases where the need is for browser access, a HTTP proxy server needed to be set up to be able to monitor or block outbound server requests.

## Visibility

As we established early on in this work, an active probing of the network is not possible due to the sensitivity of devices running there. We also can not demand any special software be installed on the devices controlling production, therefore a Honeypot is the only viable option.

Now a full honeypot requires quite a few extra connections open in the firewall therefore I looked at maximal alertness for minimum maintenance and open ports.

# Journal

## 14.07.2021 - First meeting (Remote)

*Henrik Ekholm, Dr. Bruce Nikkel*

Introduction

Short explanation of the current situation/Background about Ecolab

•plant segmentation ongoing

•proper security architecture needed

Decision to do forensic readiness for production Network as project

* Deliverables:
  + POC - Henrik to verify support of project with leadership
  + Thesis with architecture
* In Preparation to investigate
  + Internal sink holes - Bruce to send slides of recent presentation
  + Proxy/Jump Hosts
  + Canary Server

Henrik to prepare Task Definition (Aufgabenstellung)

Next Meeting: 20.8.2021 at 11:00 in Wankdorf

## 20.08.2021 – (In Person)

Discussion about current Situation

* Reorganisation ongoing

Expert

* Henrik to set up contact as soon as expert known

Internal Project Proposal

* Henrik to e-mail Bruce Proposal or Executive summary of such

Task Definition was sent and viewed over

* Henrik to fill out missing parts when information known

Next Meeting 16.09.2021 in Wankdorf

## 16.09.2021 – (Remote)

Gitlab set up, but decided on e-mails for communication

Preparation before Kickoff

* Title and Description are done and registered
* Henrik to Prepare Project plan for next meeting
* At least steps, time is not necessary
* Henrik to create one thesis document for next meeting
  + Keep everything in one document
  + Put sinkholes and notes directly in there

Next Meeting 30.09.2021

Discussion with Security leadership – Segmentation/responsibilies

# Conclusion

# List of illustrations

**No table of figures entries found.**

# Contents of the table

**No table of figures entries found.**

# Glossary

|  |  |
| --- | --- |
| Term | Description |
|  |  |
| OT (Operation Technology) | Hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment. |

# References

Cisco Systems, Inc.,Rockwell Automation. (2019, 4). *Network Security within a Converged Plantwide Ethernet Architecture.* Retrieved from https://www.cisco.com: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/Network\_Security/WP/CPwE-5-1-NetworkSecurity-WP.pdf

# Appendix A: Handbook for integration

# Declaration of Authorship

I hereby certify that I composed this work completely unaided, and without the use of any other sources or resources other than those specified in the bibliography. All text sections not of my authorship are cited as quotations, and accompanied by an exact reference to their origin.

Place, date:

Signature:

1. (Williams, 1994) [↑](#footnote-ref-1)
2. (Cisco Systems, Inc.,Rockwell Automation, 2019) [↑](#footnote-ref-2)