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

Bern University of Applied Sciences

Department
Division

1 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

2 Introduction

2.1 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?

2.2 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.

2.3 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.

2.4 Learning

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

2.5 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.

3 Meeting Notes

3.1 14.07.2021 - First meeting (Remote)

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

3.2 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

3.3 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

4 Threat Review

4.1 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.

In 2019 Cisco released a paper in collaboration with Rockwell which outlines the current problem with securing OT systems in an IT environment called Currently we employ the (Cisco Systems, Inc.,Rockwell Automation, 2019)/

5 Conclusion

6 List of illustrations

No table of figures entries found.

7 Contents of the table

No table of figures entries found.

8 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.

9 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

10 Appendix A: Handbook for integration

11 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: