|  |  |
| --- | --- |
|  | **IISMS Implementation Revision** 1 |

**NP Factory, Ltd.**

**Plant floor**

**Industrial Information Security Management System**

Guide to Networked Industrial Equipment Hardening

Nathan Pocock

https://our.intranet/path/to/document.docx

|  |  |
| --- | --- |
| **IISMS Implementation Revision** 1 (12) | **Industrial Information Security Management System**  Guide to Networked Industrial Equipment Hardening  Editor: *Nathan Pocock*  Authors: *Nathan Pocock* |

**Hardening**

PRIVATE

|  |  |
| --- | --- |
| 05e - Guide To Device Hardening.Docx  Version: 1 Revision 12  Pages: 8 | Path: C:\Users\nathan pocock\OneDrive\wgu-capstone\templates\05e - Guide to Device Hardening.docx  Keywords: iisms, hardening, lockdown, restricting, access, security, prevent  Last Saved by Nathan Pocock on 9/18/2016 4:15 PM |
|  | **NP Factory, Ltd.**  [Company Address]  Plant floor  IISMS Implementation  704-491-5840  Manager Pocock |

Executive Summary

A guide to help facilitate locking-down an Ethernet connected industrial networked device.

Revision History

|  |  |  |
| --- | --- | --- |
| Revision | Author | Date |
| Initial creation | Nathan Pocock | 18-Sep-16 |
|  |  |  |
|  |  |  |
|  |  |  |

Contents

[1 Instructions 6](#_Toc461979435)

[2 Introduction 7](#_Toc461979436)

[3 Security Considerations 7](#_Toc461979437)

[4 Restricting Access to Insecure Devices 8](#_Toc461979438)

[1.1 Firewall appliance 8](#_Toc461979439)

[1.2 Intrustion Detection/Prevention Device 8](#_Toc461979440)

Figures

# 

# Instructions

Please complete this document as follows:

1. Read the introduction
2. Use this document as a starting-point to identify the options available for each device
3. Add more sections to this document with specific instructions that specifically apply to your needs, equipment, and environment
4. Go to each device and implement the security that is available
5. Document the changes made to each device
6. Save each document to a secure location

Lastly, delete this page and then save the document.

# Introduction

Networked industrial equipment/devices will vary greatly in their function and capabilities. Indeed, some devices will provide significant security capabilities whereas others may provide literally none. For this reason, this document is a guideline only, not a set of instructions.

The following assumptions are made:

* Each device has different security capabilities, if any
* The operating manual and vendor are the best source for security-related information

# Security Considerations

The following list contains a series of questions that you should ask when sat in front of the device:

* User-access:
  + Can you restrict user access, e.g. login, card-swipe, pin number?
  + Can you create individual user-level access?
  + Can you define user-access levels per user, e.g. user vs. admin?
  + Are there capabilities to determine policies, e.g. password/pin; change frequency, etc.?
* Behavior:
  + Does the device allow behaviors/capabilities to be enabled/disabled?
  + Can behavior be configured on a per-user basis?
  + Are there settings to control safety parameters?
* Networking:
  + Can you define the IP settings to be fixed/dynamic?
  + Can you restrict the IP addresses that can communicate with the device?
  + Are there any settings to enable VPN?
  + Are there any settings to harden to the TCP/IP stack?
* Logging:
  + Can you enable audit logs?
  + Can you configure what is stored in the audit logs?
  + Can you configure where the logs are stored?
  + Can you send copies of the logs to a location on the network?
  + Can you integrate the auditing with other networked systems? (e.g. SNMP, Syslog)

# Restricting Access to Insecure Devices

If a networked device is identified as being “at risk” of cyber-attack, perhaps it has known vulnerabilities or weaknesses (denial of service, no login requirements, etc.) then protection will be required.

## Firewall appliance

The simplest method of protecting an Ethernet-connected insecure-device is to simply put a firewall appliance in front of it. The appliance should be capable of being used in an industrial environment, so consider the following:

* Exposure to heat, dust, noise/audio, noise/radio, liquid, chemicals, fire, etc.
* Prolonged periods of activity, i.e. months or years without downtime (reliability)
* Resistance to attack, such as denial of service

With a firewall appliance in place, consider the following:

* Allow the device-specific protocol to traverse the firewall only (inbound and outbound?)
* Block all other traffic

## Intrusion Detection/Prevention Device

An alternative method of a firewall is to use an IDS/IPS in an embedded control such, perhaps even a Raspberry Pi. An IDS/IPS can be configured with specific rule-sets that permit ONLY the device-specific protocol traffic. Furthermore, the rules could be tailored to only permit specific protocol activities to eliminate any potential of configuration change, and restrict capabilities to simply acquiring data only.

Unfortunately, this is outside the scope of this document and is something that should be left to the experts. This will be a time-consuming exercise compared to simply installed a *Firewall appliance*, above.