|  |  |
| --- | --- |
|  | **I-ISMS Implementation Revision** 1 |

**NP Factory, Ltd.**

**Factory Floor**

**Industrial Information Security Management System**

Guide to conducting Windows O/S hardening

Nathan Pocock

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

|  |  |
| --- | --- |
| **I-ISMS Implementation Revision** 1 (93) | **Industrial Information Security Management System**  Guide to conducting Windows O/S hardening  Editor: *Nathan Pocock*  Authors: *Nathan Pocock* |

**IISMS**

PRIVATE

|  |  |
| --- | --- |
| Do - 07 -- Guide To Windows Hardening.Docx  Version: 1 Revision 93  Pages: 23 | Path: C:\Users\nathan pocock\OneDrive\wgu-capstone\templates\Do - 07 -- Guide to Windows Hardening.docx  Keywords: windows, o/s, hardening, vulnerability, mitigate, remote  Last Saved by Nathan Pocock on 9/22/2016 9:54 AM |
|  | **NP Factory, Ltd.**  [Company Address]  Factory Floor  I-ISMS Implementation  704-491-5840  Manager Pocock |

Executive Summary

Provides high-level guidance on how to configure the Windows desktop computers to provide a greater level of security from attack of local and remote users.

Revision History

|  |  |  |
| --- | --- | --- |
| Revision | Author | Date |
| Initial creation | Nathan Pocock | 13-Sep-16 |
|  |  |  |
|  |  |  |
|  |  |  |

Contents

[1 Instructions 7](#_Toc462301421)

[2 Overview 8](#_Toc462301422)

[1.1 Documentation 8](#_Toc462301423)

[1.2 Backups 8](#_Toc462301424)

[3 Computer System (Hardware) 9](#_Toc462301425)

[4 Windows Operating System 9](#_Toc462301426)

[1.3 Install anti-virus / endpoint-protection 9](#_Toc462301427)

[1.4 Enable firewall 9](#_Toc462301428)

[1.5 Windows Updates 10](#_Toc462301429)

[1.6 NTFS File System 10](#_Toc462301430)

[1.7 Disable Hardware 11](#_Toc462301431)

[5 Windows Features 11](#_Toc462301432)

[1.8 Disable file and print sharing 11](#_Toc462301433)

[1.9 Disable unneeded network adapter services and protocols 12](#_Toc462301434)

[1.10 Disable remote desktop 13](#_Toc462301435)

[1.11 Enable DEP 13](#_Toc462301436)

[1.12 Enable auditing 13](#_Toc462301437)

[1.13 Disable any unnecessary scheduled tasks 14](#_Toc462301438)

[1.14 Uninstall unnecessary applications and windows components 14](#_Toc462301439)

[1.15 Required services automatically restart 15](#_Toc462301440)

[1.16 Disable unnecessary services (peer-networking, remote registry, search, etc.) 15](#_Toc462301441)

[6 User settings 15](#_Toc462301442)

[1.17 Enable UAC 15](#_Toc462301443)

[1.18 Display legal notice on logon attempt 16](#_Toc462301444)

[1.19 Disable automatic login 16](#_Toc462301445)

[1.20 Setup user accounts 16](#_Toc462301446)

[1.20.1 Require each user to have own account 16](#_Toc462301447)

[1.20.2 Limit administrators 17](#_Toc462301448)

[1.20.3 Rename administrator account 17](#_Toc462301449)

[1.20.4 Remove unused user accounts 17](#_Toc462301450)

[1.20.5 Disable guest accounts 17](#_Toc462301451)

[1.21 Disable anonymous access to named-pipes and shares 17](#_Toc462301452)

[1.22 Verify user-access to file system 18](#_Toc462301453)

[1.23 Verify user-access to applications 19](#_Toc462301454)

[1.24 Restrict logon attempts 19](#_Toc462301455)

[1.25 Set password policy 20](#_Toc462301456)

[1.26 Prevent users from sharing 20](#_Toc462301457)

[7 Desktop preferences 20](#_Toc462301458)

[1.27 Password protected screensaver 20](#_Toc462301459)

[1.28 Disable autorun 20](#_Toc462301460)

[1.29 NTP “time.windows.com” 21](#_Toc462301461)

[8 Shared resources 21](#_Toc462301462)

[1.30 Disable any unnecessary folders and/or printers 21](#_Toc462301463)

[1.31 Share any applicable folders/printers with specific individuals 22](#_Toc462301464)

[9 Enabling System Protections 22](#_Toc462301465)

[1.32 System backups 22](#_Toc462301466)

[1.33 Enable restore points 23](#_Toc462301467)

[10 \*DCOM Permissions for OPC 23](#_Toc462301468)

Figures

**No table of figures entries found.**

# 

# Instructions

This page provides quick instructions for using this guide:

1. Carefully read through the Overview on page 8
2. Plan your desired workstation capabilities and limits first!
3. For each PC on your network, do the following:
   1. Prepare a document to record the configuration changes
   2. Backup the PC before making any changes
   3. Proceed through this document configuring Windows settings
   4. Test the PC is in good working order
   5. Backup the PC
4. Add more instructions for further restrictions as necessary.

Finally, delete this page.

# 

# Overview

The windows operating system is a gigantic framework of various services, components, and applications. Collectively, all of these capabilities make a significant attack surface. The best way to defend from attacks is to reduce the attack-surface and then harden those services that we do want to use.

Talk to your IT dept. to see if they have existing policies that you can implement, or use as a baseline for your own policies. This could save an immense amount of time.

**IMPORTANT** This guide will cover only a portion of the Windows capabilities that should be more tightly controlled.

More thorough hardening instructions can be found in the United States Department of Defense STIG Windows 7 Security Technical Implementation Guide (Department of Defense, 2016)

This document assumes Windows 7.

## Documentation

It is ESSENTIAL that you record the changes you make to a computer.

If you do not have a computer change configuration system, then you could utilize the [06 - Computer Vulnerability and Risk Analysis.dotx](06%20-%20Computer%20Vulnerability%20and%20Risk%20Analysis.dotx) template with some minor modifications to store the changes made to the computer.

## Backups

Conduct a complete system backup before making ANY changes to the computer system.

At the end of the re-configuration process, conduct a thorough system test and then perform another backup.

Once complete, assure that automatic system backups are configured and verified as running..

# Computer System (Hardware)

While the operating system is the focus of this paper, it is extremely important to assure the BIOS is configured to:

* Require a password to enter into the BIOS configuration
* Safe-boot into Windows directly; and without an option to boot to an alternate operating system

Lastly, conduct a visual inspection of the computer and then disconnect and remove any unnecessary devices/components that may be attached.

# Windows Operating System

This section will focus on Windows itself.

## Install anti-virus / endpoint-protection

Anti-virus, or Endpoint-protection is a form of defense from known malware and attack-signatures. Some generalized recommendations include:

* Enable real-time scanning
* Enable scheduling whole-system scanning to occur over the weekend or periods of down-time / minimal use
* Enable automatic updates of virus signatures and allow them to update at least daily
* Enable application monitoring, to determine which applications are trying to use the network
* Enable file signature analysis to help detect if/when key system files change

Most modern security suites consist of anti-virus, firewall, and host intrusion detection and prevention. Be sure to review the documentation and enable all of those features.

## Enable firewall

A firewall is required, whether it is the Windows Firewall (see [05b - Guide to Windows Firewall Hardening.docx](05b%20-%20Guide%20to%20Windows%20Firewall%20Hardening.docx)) or a firewall provided by a security suite (see *Install anti-virus / endpoint-protection*, above)

## Windows Updates

First, upgrade the O/S to the latest service pack and patches. This is extremely important.

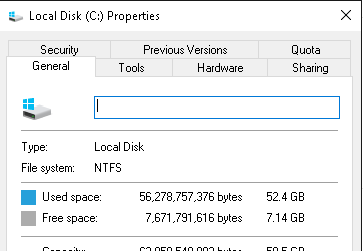
Second, disable windows update to prevent unplanned reboots which could affect production:

Third, disable Windows Anytime Upgrade to prevent the automatic installation of next-generation operating systems:

1. Click START > RUN and then enter “REGEDIT” and press ENTER
2. When the registry editor opens, expand the HKEY\_LOCAL\_MACHINE node
3. Navigate to \Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\WAU\; if the “WAU” folder does not exist then right-click and create a new KEY called “WAU”
4. Locate the setting called “Disabled”, if it does not exist then create a new DWORD called “Disabled” and set the value to “1”.

## NTFS File System

Assure that all connected hard drives are formatted with NTFS, which is a secure file system providing the ability to specify which users/groups can access files/folders, and provides auditing to show which users accessed files/folders:

1. Check the file type for each drive by simply opening Windows Explorer, and then right-click > Properties, on a drive and look for the NTFS file system:   
   
2. If the drive says FAT or FAT32 then you must convert it by running the following sequence:
   1. Click START, and then navigate to All Programs > System, and then right-click on Command Prompt and choose “Run as administrator”.
   2. A command prompt will open
   3. Enter the following command, which assumes the C: drive will change; replace the drive letter as appropriate:   
      convert c: /FS:NTFS
   4. A system reboot will be required for the conversion to take place.

## Disable Hardware

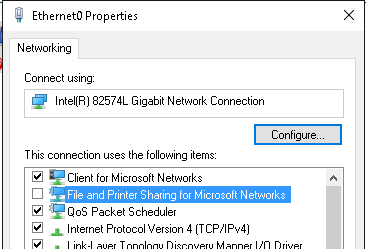
Disable any unused modems, network adapters, USB ports, printers, scanners, or any other type of device that is not required:

1. Open the Control Panel and then choose Device Manager.
2. A list of device categories will be presented.
3. Expand a section that contains a device that can be disabled, for example if disabling a floppy disk drive then expand the “Floppy disk drives” category.
4. Right-click on the device and choose “Disable” from the context menu.
5. Repeat for other devices that are not necessary.

# Windows Features

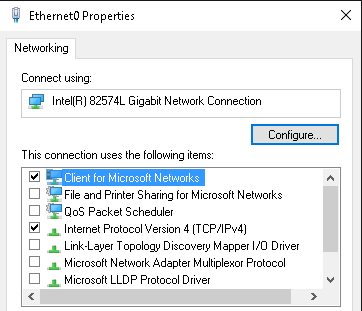
## Disable file and print sharing

If file and print sharing is not required, then it should be disabled:

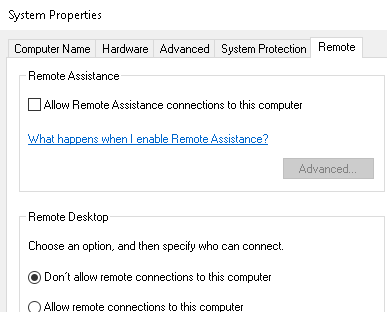
1. Right-click the “network” icon in the taskbar (beside the system clock) and choose “Open Network and Sharing Center”
2. For each network adapter displayed, do the following:
   1. Right-click on the adapter and then choose “Properties”
   2. Deselect the “File and Printer Sharing for Microsoft Networks”:   
      
   3. Click OK to save and close the window.

## Disable unneeded network adapter services and protocols

Remove unnecessary protocols and bindings from the network adapter by:

1. Right-click the “network” icon in the taskbar (beside the system clock) and choose “Open Network and Sharing Center”
2. For each network adapter displayed, do the following:
   1. Right-click on the adapter and then choose “Properties”
   2. Deselect each protocol and component that is not necessary, for example:   
      
   3. Click OK to save and close the window.

## Disable remote desktop

1. Click the START menu and then right-click on the Computer and choose Properties
2. Click the “Advanced system settings” option
3. Click the “Remote” tab
4. Clear the settings on-screen to disable remote assistance and remote desktop:   
   
5. Click OK to save and close the window.

## Enable DEP

1. Click the START menu and then right-click on the Computer and choose Properties
2. Click the “Advanced system settings” option
3. Click the “Advanced” tab
4. Click “Settings” beside the “Performance” section
5. Click “Data Execution Tab” and ensure the “Turn on DEP” option is selected.
6. Click OK to save and close the window.

## Enable auditing

Auditing will record all computer activities, which can be essential for forensic investigations after a breach has occurred.

1. Click START > Control Panel > Administrative Tools > Local Security Policy
2. Navigate to Local Policies > Audit Policy
3. A number of settings will be displayed, for each setting do the following:
   1. Double-click on a setting
   2. Check the box for both “Success” and “Failure”
   3. Click OK to save and close the dialog.
4. Close the app.

## Disable any unnecessary scheduled tasks

Windows contains a large quantity of tasks that are executed on a schedule. Many tasks pre-configured by Windows are not necessary and should be disabled. There may be other tasks that should be disabled too.

1. Click START > Control Panel > Administrative Tools > Task Scheduler
2. The left-side navigation tree shows a folder structure. Expand each layer and for each folder, do the following:
   1. Select a folder on the left and the list of tasks will be visible on the right
   2. For each task, you can open its properties to review it if you wish
   3. Right-click on the task and either (a) delete it, or (b) disable it.

Warning: newer operating systems contain a SIGNIFICANT number of scheduled tasks for spying on user activities and reporting metrics and usage to Microsoft, and should be deleted.

## Uninstall unnecessary applications and windows components

1. Click START > Control Panel > Add/Remove Programs
2. Review the list of installed software and remove any applications that are not needed
3. Click the “Turn Windows features on or off” in the left-side navigation
4. A list of windows “features” will be presented, clear any checkboxes for components that are not needed, such as, for example:
   1. Hyper-V
   2. Internet explorer
   3. Internet information services
   4. Legacy components
   5. Media features
   6. MSMQ
   7. Print and document services
   8. RAS
   9. Remote differential
   10. XPS, etc., etc.

## Required services automatically restart

1. Click START > Control Panel > Administrative Tools > Services
2. For each service that is listed as “running’ verify if it should be; if not, then disable it.
3. For each service that is listed with startup as “automatic”, verify if it is needed or not, and if not, then open its properties and change it to startup “manual’ or “disabled”.
4. For each service that you know is critically important, such as a SCADA service, then open its properties and click the “Recovery” tab
5. Configure the settings as appropriate
6. Click OK to save and close the window.

## Disable unnecessary services (peer-networking, remote registry, search, etc.)

1. Click START > Control Panel > Administrative Tools > Services
2. Review the list of services and for each service that is identified as not necessary, such as “peer networking, remote registry, search, etc.) you should do the following:
   1. Right-click on the service and choose “Properties”
   2. Set the startup mode to “Disabled” (preferred) or “Manual”
   3. Click “OK” to save and close the window.

# User settings

## Enable UAC

User Account Control is a feature that can prevent applications from conducting administrative tasks even when used by an administrator, by forcing the user to acknowledge the request with an administrative login. This feature can prevent unauthorized or accidental changes to the system.

1. Click START > Control Panel > Users
2. Click the “Change User Account Control settings” link
3. Adjust the slider to the top and then click OK to save and close the window.

## Display legal notice on logon attempt

Force users to acknowledge the computer is for official work operations and authorized personnel only:

1. Click START > Control Panel > Administrative Tools > Local Security Policy
2. Expand Local Policies > Security Options
3. Double-click setting “Interactive logon: Message title for users attempting to log on” and set the value to something like “WARNING! Prosecution Alert!”; and then click OK to save and close the window
4. Double-click setting “Interactive logon: Message text for users attempting to logon” and set the value to something like “This computer system is for official authorized personnel conducting official company business only. All activities are monitored. Violators will be prosecuted.”

## Disable automatic login

If the computer currently automatically boots-up straight to the desktop without requiring a user to login, then automatic login is enabled and must be disabled as follows:

1. Click START > Run, and then enter the command “REGEDIT” and press enter
2. Expand HKEY\_LCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
3. Double-click value “AutoAdminLogon” and set the value to “0”.

## Setup user accounts

### Require each user to have own account

Do not share user accounts as this will not help investigations in the event of a breach requiring forensic analysis of the system. Create a user account per worker:

1. Click START > Control Panel > User Accounts
2. Click “Manager another account”
3. In the “Manage Accounts” screen you can manage existing accounts as well as add new accounts
4. When adding a new account be sure to choose “Standard user”; do not use “Administrator” accounts for normal operations, reserve these accounts exclusively for conducting administrative tasks.

### Limit administrators

While in the user accounts window, review the administrative user accounts and prune them where necessary.

Avoid using accounts with administrative privileges. Use administrative accounts exclusively for performing administrative tasks only.

### Rename administrator account

Renaming administrator accounts that have a default name of “admin” or “administrator” can significantly reduce an attackers chance of brute-force guessing login credentials, as follows:

1. Click START > Control Panel > Administrative Tools > Computer Management
2. Navigate to and select System Tools > Local User and Groups > Users
3. Highlight the administrator account and then right-click and choose “Rename”; provide the new name and hit Enter.

### Remove unused user accounts

While in the *advanced* user accounts window, prune the database to remove user accounts that should not be there.

### Disable guest accounts

While in the *advanced* user accounts window, prune the database to disable all guest accounts:

* Highlight a guest account
* Right-click and choose “Properties”
* Check the “Account is Disabled” box and then click OK.

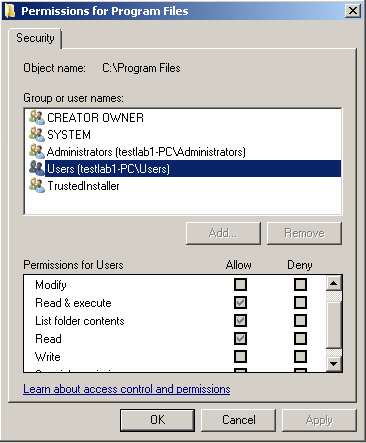
## Disable anonymous access to named-pipes and shares

We will prevent unauthorized user accounts from making application-to-application connections:

1. Click START > Control Panel > Administrative Tools > Local Security Policy
2. Navigate to and select Local Policies > Security Options
3. Double-click setting “Network access: Restrict anonymous access to named Pipes and Shares” and set the value to “Enabled”
4. Click OK to save and close the dialog.

## Verify user-access to file system

The best defense for the file system is to utilize the default windows security behavior:

1. Open Windows Explorer
2. Navigate to the root of the C: drive
3. The most important folders to protect are: Program Files, Program Files (x86), Users, and Windows. For each of these, conduct the following:
   1. Right-click the folder and choose PROPERTIES
   2. Click the “Security” tab
   3. Click the “Edit” button
   4. Make sure CREATOR OWNER, SYSTEM, and Administrators have “Full control”
   5. Make sure Users have Read & execute, List folder contents, and Read:   
      
   6. Click OK to save and close the dialog
   7. Now click the “Advanced” button for advanced security settings
   8. Click “Change Permissions…” button; this will open a more complex window
   9. Check the box ”Replace all child object permissions with inheritable permissions from this object”
   10. Click OK to save and close the window  
       Note: the change may require several minutes to complete
4. Repeat for the other folders.

## Verify user-access to applications

Are some applications off-limits for some users? If so then you can remove them:

1. Click START > Control Panel > Administrative Tools > Local Security Policy
2. Navigate to and click on Application Control Policies > AppLocker > Executable Rules
3. For each application and user you wish to define a rule for, do the following:
   1. Right-click and create a new rule, a wizard will start…
   2. Click “Next >” to bypass the welcome page
   3. Set the “Deny” action and then press the “Select…” button to choose the user(s) that you will block; click OK to close the dialog and return to the wizard and then click “Next”
   4. Select the “Path” option and click “Next >”
   5. Click the “Browse Files…” button and navigate to the executable, such as a SCADA application, an administrative application, or control application.
   6. Skip the exceptions screen by clicking “Next >”
   7. At the final page make sure a name and description are specified.  
      Tip: use the description field to justify the rule because you will forget at some point!
   8. Click “Create”

## Restrict logon attempts

To slow-down any attempt at brute-force guessing a password, we will instruct Windows to temporarily deactivate an account after so many failed attempts, in accordance with I-ISMs policy (see [01 - IISMS-CompanyPolicy.docx](01%20-%20IISMS-CompanyPolicy.docx)):

1. Click START > Control Panel > Administrative Tools > Local Security Policy
2. Navigate to and click on Account Policies > Account Lockout Policy
3. The setting in this screen are self-explanatory and should be set in accordance with the I-ISMS policy.

## Set password policy

In this section you should define password and account policies in accordance with the I-ISMS policy (see [01 - IISMS-CompanyPolicy.docx](01%20-%20IISMS-CompanyPolicy.docx)) as follows:

1. Click START > Control Panel > Administrative Tools > Local Security Policy
2. Navigate to and select Account Policies > Password Policy; the settings will appear to the right
3. The settings are self-explanatory; configure them as appropriate.

## Prevent users from sharing

If we do not want users to share resources from this computer, conduct the following:

1. Click START > Control Panel > Network and Sharing Center
2. Click “Change advanced sharing settings”
3. Click the radio “Turn off file and printer sharing”
4. While in this screen it would also be advisable to select “Turn off network discovery”
5. Click “Save changes” to save and close the window.

# Desktop preferences

## Password protected screensaver

If a screensaver is used then it should prompt for user-logon on resume:

1. Right-click on the Desktop and choose “Personalize”
2. Click the “Screen Saver” link
3. In the “Screen Saver Settings” dialog select your screensaver
4. Check the box “On resume, display logon screen”
5. Click OK to save and close the window.

## Disable autorun

Prevent any media from automatically executing if a CD is inserted or USB stick, etc.:

1. Click START > Run, and then enter “REGEDIT” and press enter.
2. Navigate to and click on HKEY\_LOCAL\_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer
3. Double-click on setting “NoDriveTypeAutoRun” and set the value to “FF” and click OK to save and close the dialog.

## NTP “time.windows.com”

It is essential that all computers maintain a synchronized clock. This is essential for accurate time-keeping and in the event that forensic analysis is needed in the event of a breach.

Ask your IT dept. if a Network Time Server is available on the network and obtain its IP address.

Note: the perimeter firewall may require a rule to be added to permit NTP to pass through:

1. Right-click on the system clock and choose “Adjust date/time”
2. Click the “Internet Time” tab
3. Click the “Change settings…” button
4. Check the box “Synchronize with an internet time server” and then specify either:
   1. The IP address provided by your IT dept.
   2. “time.windows.com”
   3. Click OK to save and close the window, twice.

# Shared resources

## Disable any unnecessary folders and/or printers

Remove any shared resources that should not be shared. Ideally, no resources will be shared:

1. Click START > Control Panel > Administrative Tools > Computer Management
2. Navigate to and select Shared Folders > Shares
3. For each shared resource right-click on the shared resource and choose “Stop Sharing”.

## Share any applicable folders/printers with specific individuals

If shared resources are required, then restrict access to the appropriate users only:

1. Click START > Control Panel > Administrative Tools > Computer Management
2. Navigate to and select Shared Folders > Shares
3. For each shared resource right-click on the shared resource and choose “Properties”
4. Click the “Share Permissions” tab and then modify the users/groups that have access to the resource
5. Click OK to save and close the window.

# Enabling System Protections

## System backups

There are 2 forms of backup that should be made:

* **Permanent**: a compete backup of the computer system that is then stored in a safe location. This type of backup is conducted annually or semi-annually in accordance with the I-ISMS policy (see [01 - IISMS-CompanyPolicy.docx](01%20-%20IISMS-CompanyPolicy.docx))
* **Ongoing**: automated backups that are scheduled to run frequently (weekly?) in accordance with the I-ISMS backup policy.

Attached backup drives should be physically secured to prevent any form of physical contact.

The use of the built-in Windows backup is effective when configured as follows:

1. Click START > Control Panel > Backup and Restore
2. Click the “Change settings” link to configure the backup activities; this will launch a wizard
3. First, specify the destination drive which will store the backup; click “Next”
4. Second, select “Let Windows choose (recommended)” as the backup policy; click “Next”
5. Make sure “Include a system image of drives: RECOVERY, OS (C:)” is selected
6. Click “Save settings and exit” to close the dialog.

With backup set, now conduct the initial backup by clicking the “Back up now” button.

## Enable restore points

1. Click the START menu and then right-click on the Computer and choose Properties
2. Click the “Advanced system settings” option
3. Click the “System Protection” tab
4. Ensure that the Local Disk (C:) is protected. If it is not, then select it and then press the “Configure” button
5. Click “Turn on system protection”
6. Click OK to save and close the dialog; and again.

# \*DCOM Permissions for OPC

OPC Classic applications use the COM/DCOM framework for Client/Server connectivity. This can be a difficult system to configure to allow these applications to successfully connect and share data with one another. Typically, software vendors provide DCOM instruction guides that remove all of the security safe-guards that protect a system from attack. While this shotgun approach will enable applications to work with each other, the engineers will typically stop right there instead of going back and gradually increasing the security back to a safe state.

There are MANY DCOM tutorials online which you can use with the DCOMCNFG.EXE application. However, consider following a tutorial that can help you to achieve the following results:

1. Create a dedicated user account for a specific OPC application; that user has limited access rights to the file system (e.g., the application’s binaries and any directory where configurations are saved)
2. The user is assigned to the application (application’s DCOM properties, IDENTITY tab)
3. The application’s Launch & Activation Permissions, Access Permissions and Configuration Permissions are locked-down such that only the specific user has the accesses it needs.

With this system in place, regardless of which user actually logs into the computer system, the dedicated user account will limit the capabilities of the application. If any vulnerabilities exist within the application then the potential impacts on the system are severely restricted, particularly if there are remote control capabilities etc.