APRIL 2018

Hardening Microsoft Office 2016

Introduction

1. Workstations are often targeted by adversaries using malicious web pages, malicious email attachments and removable media with malicious content in an attempt to extract sensitive information. Hardening applications on workstations is an important part of reducing this risk.
2. This document provides guidance on hardening Microsoft Office 2016 – specifically Microsoft Excel 2016, Microsoft PowerPoint 2016 and Microsoft Word 2016. Before implementing the recommendations in this document, testing should be undertaken to ensure the potential for unintended negative impacts on business processes is reduced as much as possible.
3. This document is intended for information technology and information security professionals within organisations looking to undertake risk assessments or vulnerability assessments as well as those wishing to develop a hardened Standard Operating Environment for workstations.
4. The Group Policy Administrative Templates for Microsoft Office 2016 referenced in this document can be obtained from Microsoft[1]. Once downloaded, the ADMX and associated ADML files can be placed in *C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions* on the Domain Controller and they will automatically be loaded in the Group Policy Management Editor. As Group Policy Administrative Templates for Microsoft Office are periodically updated by Microsoft, care should be taken to ensure the latest version is always used.

High priorities

5. The following security controls, listed in alphabetical order, are considered to have an excellent effectiveness and should be treated as high priorities when hardening Microsoft Office deployments.

Attack Surface Reduction

6. Attack Surface Reduction (ASR)[2] is a new security feature introduced in Microsoft Windows 10, version 1709 as part of Windows Defender Exploit Guard. It is designed to combat the threat of

[1] https://www.microsoft.com/en-au/download/details.aspx?id=49030

[2] https://docs.microsoft.com/en-au/windows/security/threat-protection/windows-defender-exploit-guard/attack-surface-reduction-exploit-guard

malware exploiting legitimate functionality in Microsoft Office applications. In order to use ASR, Windows Defender Antivirus must be configured as the primary real-time antivirus scanning engine on workstations.

7. ASR offers a number of attack surface reduction rules, these include:
   a. block executable content from email client and webmail:
      BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46550
   b. block Office applications from creating child processes:
      D4F940AB-401B-4EFC-AADC-AD5F3C50688A
   c. block Office applications from creating executable content:
      3B576869-A4EC-4529-8536-B80A7769E899
   d. block Office applications from injecting code into other processes:
      75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84
   e. block JavaScript and VBScript from launching downloaded executable content:
      D3E037E1-3EB8-44C8-A917-57927947596D
   f. block execution of potentially obfuscated scripts:
      5BEB7EFE-FD9A-4556-801D-275E5FFC04CC
   g. block Win32 API calls from Office macro:
      92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B.
8. Organisations should either implement ASR using Windows Defender Antivirus or use third party antivirus solutions that offer similar functionality to those provided by ASR. For older versions of Microsoft Windows, alternative measures will need to be implemented to mitigate certain threats addressed by ASR, such as the likes of Dynamic Data Exchange (DDE) attacks[3].
9. For organisations using Windows Defender Antivirus, the following Group Policy settings can be implemented to enforce the above ASR rules.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Antivirus\Windows Defender Exploit Guard\Attack Surface Reduction	
Configure Attack Surface Reduction rules	Enabled Set the state for each ASR rule: 75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84 1 3b576869-a4ec-4529-8536-b80a7769e899 1

[3] https://technet.microsoft.com/en-au/library/security/4053440

	d4f940ab-401b-4efc-aadc-ad5f3c50688a	1
	92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B	1
	5beb7efe-fd9a-4556-801d-275e5ffc04cc	1
	d3e037e1-3eb8-44c8-a917-57927947596d	1
	be9ba2d9-53ea-4cdc-84e5-9b1eeee46550	1

Macros

10. Microsoft Office files can contain embedded code (known as a macro) written in the Visual Basic for Applications (VBA) programming language.

11. A macro can contain a series of commands that can be coded or recorded, and replayed at a later time to automate repetitive tasks. Macros are powerful tools that can be easily created by novice users to greatly improve their productivity. However, an adversary can also create macros to perform a variety of malicious activities, such as assisting to compromise workstations in order to exfiltrate or deny access to sensitive information. To reduce this risk, organisations should either disable or secure their use of Microsoft Office macros.

12. For information on securing the use of Microsoft Office macros see the *Microsoft Office Macro Security* publication[4].

Patching

13. To address security vulnerabilities identified in Microsoft Office, Microsoft regularly releases patches. If patches are not applied in an appropriate timeframe it can allow an adversary to easily compromise workstations. To reduce this risk, patches should be applied in an appropriate timeframe as determined by the severity of security vulnerabilities they address and any mitigating measures already in place.

14. For more information on determining the severity of security vulnerabilities and appropriate timeframes for applying patches see the *Assessing Security Vulnerabilities and Applying Patches* publication[5].

Medium priorities

15. The following security controls, listed in alphabetical order, are considered to have a very good effectiveness and should be treated as medium priorities when hardening Microsoft Office deployments.

ActiveX

16. While ActiveX controls can be used for legitimate business purposes to provide additional functionality for Microsoft Office, they can also be used by an adversary to gain unauthorised

[4] https://www.asd.gov.au/publications/protect/Microsoft_Office_Macro_Security.pdf

[5] https://www.asd.gov.au/publications/protect/Assessing_Security_Vulnerabilities_and_Applying_Patches.pdf

access to sensitive information or to execute malicious code. To reduce this risk, ActiveX controls should be disabled for Microsoft Office.

17. The following Group Policy setting can be implemented to disable the use of ActiveX controls in Microsoft Office.

Group Policy Setting	Recommended Option
…\Microsoft Office 2016\Security Settings	
Disable All ActiveX	Enabled

Add-ins

18. While add-ins can be used for legitimate business purposes to provide additional functionality for Microsoft Office, they can also be used by an adversary to gain unauthorised access to sensitive information or to execute malicious code. To reduce this risk, add-in use should be managed.

19. The following Group Policy settings can be implemented to manage add-ins in Microsoft Excel, Microsoft PowerPoint and Microsoft Word.

Group Policy Setting	Recommended Option
…\Microsoft Excel 2016\Miscellaneous	
Block all unmanaged add-ins	Enabled
List of managed add-ins	Enabled List of managed add-ins: *<organisation defined>*
…\Microsoft PowerPoint 2016\Miscellaneous	
Block all unmanaged add-ins	Enabled
List of managed add-ins	Enabled List of managed add-ins: *<organisation defined>*
…\Microsoft Word 2016\Miscellaneous	
Block all unmanaged add-ins	Enabled
List of managed add-ins	Enabled List of managed add-ins: *<organisation defined>*

Extension Handling

20. Extension Hardening mitigates a number of scenarios whereby an adversary would deceive users into opening malicious Microsoft Excel files. By default, users will be warned when file content or MIME type doesn't match the file extension; however, users can still allow such files to open. As such, it is important that only Microsoft Excel files that pass integrity checks are allowed to be opened. To reduce this risk, Extension Hardening functionality should be enabled for Microsoft Excel.

21. The following Group Policy setting can be implemented to enable Extension Hardening functionality in Microsoft Excel.

Group Policy Setting	Recommended Option
…\Microsoft Excel 2016\Excel Options\Security	
Force file extension to match file type	Enabled Always match file type

File Type Blocking

22. File Type Blocking can be used to block insecure file types such as legacy, binary and beta file types from opening in Microsoft Office. By failing to block such file types, an adversary can exploit vulnerabilities in these file types to execute malicious code on workstations. To reduce this risk, insecure file types should be prevented from opening in Microsoft Office.

23. The following Group Policy settings can be implemented to block specified file types in Microsoft Excel, Microsoft PowerPoint and Microsoft Word.

Group Policy Settings	Recommended Option
…\Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block Settings	
dBase III / IV files	Enabled File block setting: Block
Dif and Sylk files	Enabled File block setting: Block
Excel 2 macrosheets and add-in files	Enabled File block setting: Block
Excel 2 worksheets	Enabled File block setting: Block
Excel 2007 and later add-in files	Enabled File block setting: Block
Excel 2007 and later binary workbooks	Enabled File block setting: Block
Excel 2007 and later macro-enabled workbooks and templates	Enabled File block setting: Block
Excel 3 macrosheets and add-in files	Enabled File block setting: Block
Excel 3 worksheets	Enabled File block setting: Block
Excel 4 macrosheets and add-in files	Enabled File block setting: Block
Excel 4 workbooks	Enabled File block setting: Block
Excel 4 worksheets	Enabled File block setting: Block

Excel 95 workbooks	Enabled File block setting: Block
Excel 95-97 workbooks and templates	Enabled File block setting: Block
Excel 97-2003 add-in files	Enabled File block setting: Block
Excel 97-2003 workbooks and templates	Enabled File block setting: Block
Set default file block behavior	Enabled Blocked files are not opened
…\Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center\File Block Settings	
PowerPoint 97-2003 presentations, shows, templates and add-in files	Enabled File block setting: Block
PowerPoint beta files	Enabled File block setting: Block
Set default file block behavior	Enabled Blocked files are not opened
…\Microsoft Word 2016\Word Options\Security\Trust Center\File Block Settings	
Set default file block behavior	Enabled Blocked files are not opened
Word 2 and earlier binary documents and templates	Enabled File block setting: Block
Word 2000 binary documents and templates	Enabled File block setting: Block
Word 2003 binary documents and templates	Enabled File block setting: Block
Word 2007 binary and later binary documents and templates	Enabled File block setting: Block
Word 6.0 binary documents and templates	Enabled File block setting: Block
Word 95 binary documents and templates	Enabled File block setting: Block
Word 97 binary documents and templates	Enabled File block setting: Block
Word XP binary documents and templates	Enabled File block setting: Block

Hidden markup

24. To assist users in collaborating on the development of Microsoft Office files, Microsoft Office allows users to track changes relating to insertions, deletions and formatting of content, as well as providing the ability to make comments. Users may choose to either view or hide these markups. If markup content is hidden, users may be unaware that sensitive changes or comments may still be included when Microsoft Office files are distributed to external parties or released into the public domain. To reduce this risk, users should be made aware of hidden markup in Microsoft Office files.

25. The following Group Policy settings can be implemented to make users aware of hidden markup in Microsoft PowerPoint and Microsoft Word files.

Group Policy Settings	Recommended Option
…\Microsoft PowerPoint 2016\PowerPoint Options\Security	
Make hidden markup visible	Enabled
…\Microsoft Word 2016\Word Options\Security	
Make hidden markup visible	Enabled

Office File Validation

26. Office File Validation (OFV) checks that the format of a Microsoft Office file conforms to an expected standard. By default, Microsoft Office files that fail OFV checking will be opened in Protected View, with users given the option to enable editing. Alternatively, OFV can be configured to open Microsoft Office files in Protected View in an enforced read-only state or simply block them from opening. If Microsoft Office is configured to disable OFV, users may be unaware that they are opening a Microsoft Office file that may be malicious in nature. To reduce this risk, OFV functionality should be enabled for Microsoft Office.

27. The following Group Policy settings can be implemented to enable OFV functionality in Microsoft Excel, Microsoft PowerPoint and Microsoft Word.

Group Policy Settings	Recommended Option
…\Microsoft Office 2016\Security Settings	
Turn off error reporting for files that fail file validation	Enabled
…\Microsoft Excel 2016\Excel Options\Security	
Turn off file validation	Disabled
…\Microsoft PowerPoint 2016\PowerPoint Options\Security	
Turn off file validation	Disabled
…\Microsoft Word 2016\Word Options\Security	
Turn off file validation	Disabled

Protected View

28. Protected View can be used to open Microsoft Office files from untrusted locations in a sandboxed environment. By default, Protected View is enabled for Microsoft Office files that have been downloaded from the Internet, opened from a defined unsafe location or opened as an attachment from Microsoft Outlook. However, organisations can choose to disable Protected

View for any or all of these scenarios. If so, an adversary could exploit any of these avenues to deliver a malicious Microsoft Office file to a user's workstation. To reduce this risk, Protected View should be enabled for Microsoft Office.

29. The following Group Policy settings can be implemented to enable Protected View functionality in Microsoft Excel, Microsoft PowerPoint and Microsoft Word.

Group Policy Settings	Recommended Option
…\Microsoft Excel 2016\Excel Options\Security\Trust Center\Protected View	
Do not open files from the Internet zone in Protected View	Disabled
Do not open files in unsafe locations in Protected View	Disabled
Set document behaviour if file validation fails	Enabled Block files
Turn off Protected View for attachments opened from Outlook	Disabled
…\Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center\Protected View	
Do not open files from the Internet zone in Protected View	Disabled
Do not open files in unsafe locations in Protected View	Disabled
Set document behaviour if file validation fails	Enabled Block files
Turn off Protected View for attachments opened from Outlook	Disabled
…\Microsoft Word 2016\Word Options\Security\Trust Center\Protected View	
Do not open files from the Internet zone in Protected View	Disabled
Do not open files in unsafe locations in Protected View	Disabled
Set document behaviour if file validation fails	Enabled Block files
Turn off Protected View for attachments opened from Outlook	Disabled

Trusted documents

30. Macros, ActiveX controls and other active content in trusted documents are assumed to be safe by Microsoft Office. An adversary can exploit this trust by modifying trusted documents to contain malicious code. To reduce this risk, trusted documents should be disabled for Microsoft Office.

31. The following Group Policy settings can be implemented to disable the use of trusted documents in Microsoft Excel, Microsoft PowerPoint and Microsoft Word.

Group Policy Settings	Recommended Option
…\Microsoft Excel 2016\Excel Options\Security\Trust Center	
Turn off trusted documents	Enabled
Turn off Trusted Documents on the network	Enabled
…\Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center	
Turn off trusted documents	Enabled

Turn off Trusted Documents on the network	Enabled
…\Microsoft Word 2016\Word Options\Security\Trust Center	
Turn off trusted documents	Enabled
Turn off Trusted Documents on the network	Enabled

Low priorities

32. The following security controls, listed in alphabetical order, are recommended for consideration when hardening Microsoft Office deployments.

Reporting information

33. Microsoft Office contains in-built functionality, namely the Office Feedback Tool, which allows users to provide feedback, including screenshots, to Microsoft. This information if captured by an adversary could expose sensitive information on workstations such as file names, directory names, versions of installed applications or content open in other applications. This information could subsequently be used by an adversary to tailor malicious code to target specific workstations or users. To reduce this risk, functionality in Microsoft Office that allows reporting of information to Microsoft should be disabled.

34. The following Group Policy settings can be implemented to prevent users reporting information to Microsoft.

Group Policy Setting	Recommended Option
…\Microsoft Office 2016\Privacy\Trust Center	
Allow including screenshot with Office Feedback	Disabled
Automatically receive small updates to improve reliability	Disabled
Disable Opt-in Wizard on first run	Enabled
Enable Customer Experience Improvement Program	Disabled
Send Office Feedback	Disabled
Send personal information	Disabled

Further information

35. The *Australian Government Information Security Manual* (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. This publication can be found at https://www.asd.gov.au/infosec/ism/.

36. The *Strategies to Mitigate Cyber Security Incidents* complements the advice in the ISM. The complete list of mitigation strategies and supporting publications can be found at https://www.asd.gov.au/infosec/mitigationstrategies.htm.

Contact details

37. Organisations or individuals with questions regarding this advice can contact the ACSC by emailing asd.assist@defence.gov.au or calling 1300 CYBER1 (1300 292 371).