Windows Hardening recommendation

Windows 10 sowie andere Microsoft Betriebssysteme sollten immer einer Systemhärtung unterzogen werden. Das Ziel eines Hardenings, ist die Reduktion von Möglichkeiten der Ausnutzung von Verwundbarkeiten.

Verwundbarkeiten werden z.B. für einen Identitätsdiebstahl ausgenutzt, resultierend daraus für die anstehende Erpressung oder Betriebsspionage. Aus diesem Grund sollten nicht genutzte Funktionen/Komponenten deaktiviert und Schutzmaßnahmen aktiviert werden.

Hier mal ein kleiner Überblick was gehärtet werden kann und welcher nutzen dahintersteht:

Was	**Wieso**
Benutzer Konfiguration	Zum Schutz der Anmeldedaten
Netzwerk Konfiguration	Standard Netzwerkkommunikation einrichten
Funktion- und Rollen- Konfiguration	Aktiviere was du brauchst und deaktiviere was du nicht brauchst
Update Konfiguration	Schwachstellen patchen
Zeitsynchronisation	Verhindern von Zeitverschiebung (Kerberos)
Firewall Konfiguration	Schutz vor Einbruch oder Ausbruch
Remotezugriff Konfiguration	Verhindern von fremden Zugriff
Dienste Konfiguration	Angriffsfläche minimieren
Allgemeine Konfigurations Härtung	Zum Schutz von OS und Applikationen
Logging und Monitoring	Wissen was auf dem System passiert

Des Weiteren sollte stets darauf geachtet werden, das bei der Vergabe von Berechtigungen, sei es für Mensch oder Maschine, immer Sicherheitsgruppen eingesetzt werden und keine Einzelberechtigung stattfindet, denn diese sind weder administrierbar noch hilft es einem bei der Einführung von Transparenz und Struktur.

Weiter sollte das Prinzip von Least Privilege bekannt sein und auch eingehend gelebt werden. Was bedeutet das im Detail?

Das LPP schreibt vor, dass einem Benutzer, einer Software oder anderen Einheit nur die absolut notwendigen Berechtigungen eingeräumt werden, die zur Ausführung der Aufgabe notwendig sind.

Erstellt von Jörn Walter **30.12.2017**

Windows Hardening recommendation

Hardening Checkliste for Windows 10:

Bit Locker

==========

[ ] Enable Bit Locker

Antivirus

=========

[ ] Enable Windows Defender

EMET

====

[ ] Install EMET

Group Policies

==========

CIS Microsoft Windows 10 Enterprise RTM (Release 1507) Benchmark

https://benchmarks.cisecurity.org/tools2/windows/CIS_Microsoft_Windows_10_Enterprise_RTM_Release_1507_Benchmark_v1.0.0.pdf

Account Policies

[ ] Set 'Account lockout duration' to '15 or more minute(s)'

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout duration

[ ] Set 'Account lockout threshold' to '10 or fewer invalid logon attempt(s), but not 0

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold

[ ] Set 'Reset account lockout counter after' to '15 or more minute(s)

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Reset account lockout counter after

Windows Hardening recommendation

Local Policies

[ ] Audit Policy

--- Audit account logon events: Failure

--- Audit account management: Success, Failure

--- Audit directory service access : No auditing

--- Audit logon events: Failure

--- Audit object access: Failure

--- Audit policy change: Success, Failure

--- Audit privilege use: Success, Failure

--- Audit process tracking: No auditing

--- Audit system events: Success Failure

[ ] Set 'Access this computer from the network' to 'Administrators'

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Access this computer from the network

[ ] Set 'Allow log on locally' to 'Administrators, Users'

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on locally

[ ] Set 'Deny log on as a batch job' to include 'Guests'

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a batch job

[ ] Set 'Deny log on as a service' to include 'Guests'

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a service

[ ] Set 'Accounts: Block Microsoft accounts' to 'Users can't add or log on with Microsoft accounts'

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Block Microsoft accounts

[ ] Set 'Interactive logon: Do not display last user name' to 'Enabled'

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not display last user name

[ ] Set 'Interactive logon: Do not require CTRL+ALT+DEL' to 'Disabled'

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not require CTRL+ALT+DEL

[ ] Set 'Microsoft network client: Digitally sign communications (always)' to 'Enabled'

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (always)

[ ] Set 'Microsoft network client: Digitally sign communications (if server agrees)' to 'Enabled'

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (if server agrees)

[ ] Set 'Microsoft network server: Digitally sign communications (always)' to 'Enabled'

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (always)

[ ] Set 'Microsoft network server: Digitally sign communications (if client agrees)' to 'Enabled'

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (if client agrees)

[ ] Set 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled'

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares

[ ] Set 'Network access: Do not allow storage of passwords and credentials for network authentication' to 'Enabled'

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow storage of passwords and credentials for network authentication

Windows Hardening recommendation

[ ] Set 'Network security: LAN Manager authentication level' to 'Send NTLMv2 response only. Refuse LM & NTLM'

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: LAN Manager authentication level

[ ] Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' to 'Require NTLMv2 session security, Require 128-bit encryption'

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) clients

[ ] Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' to 'Require NTLMv2 session security, Require 128-bit encryption'

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) servers

[ ] Set 'Shutdown: Allow system to be shut down without having to log on' to disabled

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Shutdown: Allow system to be shut down without having to log on

[ ] Set 'User Account Control: Admin Approval Mode for the Built-in Administrator account' to 'Enabled'

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Admin Approval Mode for the Built-in Administrator account

Windows Firewall With Advanced Security

[ ] Set 'Windows Firewall: Domain: Firewall state' to 'On (recommended)'

Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties*\Firewall state

[ ] Set 'Windows Firewall: Domain: Inbound connections' to 'Block (default)'

Windows Hardening recommendation

Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties*\Inbound connections

Control Panel

[ ] Set 'Prevent enabling lock screen camera' to 'Enabled'

Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization\Prevent enabling lock screen camera

[ ] Set 'Turn off the Windows Messenger Customer Experience Improvement Program' to 'Enabled'

Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off the Windows Messenger Customer Experience Improvement Program

[ ] Set 'Turn off Windows Customer Experience Improvement Program' to 'Enabled'

Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Windows Customer Experience Improvement Program

[ ] Set 'Turn off Windows Error Reporting' to 'Enabled'

Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Windows Error Reporting

[ ] Set 'Do not display network selection UI' to 'Enabled'

Computer Configuration\Policies\Administrative Templates\System\Logon\Do not display network selection UI

[ ] Set 'Turn off app notifications on the lock screen' to 'Enabled'

Computer Configuration\Policies\Administrative Templates\System\Logon\Turn off app notifications on the lock screen

[ ] Set 'Untrusted Font Blocking' to 'Enabled: Block untrusted fonts and log events'

Computer Configuration\Policies\Administrative Templates\System\Mitigation Options\Untrusted Font Blocking

Windows Hardening recommendation

[ ] Set 'Allow standby states (S1-S3) when sleeping (on battery)' to 'Disabled'

Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Allow standby states (S1-S3) when sleeping (on battery)

[ ] Set 'Allow standby states (S1-S3) when sleeping (plugged in)' to 'Disabled'

Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Allow standby states (S1-S3) when sleeping (plugged in)

[ ] Set 'Require a password when a computer wakes (on battery)' to 'Enabled'

Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Require a password when a computer wakes (on battery)

[ ] Set 'Require a password when a computer wakes (plugged in)' to 'Enabled'

Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Require a password when a computer wakes (plugged in)

[ ] Set 'Configure Offer Remote Assistance' to 'Disabled'

Computer Configuration\Policies\Administrative Templates\System\Remote Assistance\Configure Offer Remote Assistance

[ ] Set 'Configure Solicited Remote Assistance' to 'Disabled'

Computer Configuration\Policies\Administrative Templates\System\Remote Assistance\Configure Solicited Remote Assistance

[ ] Set 'Enable RPC Endpoint Mapper Client Authentication' to 'Enabled'

Computer Configuration\Policies\Administrative Templates\System\Remote Procedure Call\Enable RPC Endpoint Mapper Client Authentication

[ ] Set 'Restrict Unauthenticated RPC clients' to 'Enabled: Authenticated'

Computer Configuration\Policies\Administrative Templates\System\Remote Procedure Call\Restrict Unauthenticated RPC clients

[ ] Set 'Enable/Disable PerfTrack' to 'Disabled'

Computer Configuration\Policies\Administrative Templates\System\Troubleshooting and Diagnostics\Windows Performance PerfTrack\Enable/Disable PerfTrack

Windows Hardening recommendation

[ ] Set 'Enable Windows NTP Client' to 'Enabled'

Computer Configuration\Policies\Administrative Templates\System\Windows Time Service\Time Providers\Enable Windows NTP Client

[ ] Set 'Enable Windows NTP Server' to 'Disabled'

Computer Configuration\Policies\Administrative Templates\System\Windows Time Service\Time Providers\Enable Windows NTP Server

[ ] Set 'Allow a Windows app to share application data between users' to 'Disabled'

Computer Configuration\Policies\Administrative Templates\Windows Components\App Package Deployment\Allow a Windows app to share application data between users

[ ] Set 'Block launching Windows Store apps with Windows Runtime API access from hosted content.' to 'Enabled'

Computer Configuration\Policies\Administrative Templates\Windows Components\App runtime\Block launching Windows Store apps with Windows Runtime API access from hosted content.

[ ] Set 'Disallow Autoplay for non-volume devices' to 'Enabled'

Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies\Disallow Autoplay for non-volume devices

[ ] Set 'Set the default behavior for AutoRun' to 'Enabled: Do not execute any autorun commands'

Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies\Set the default behavior for AutoRun

[ ] Set 'Turn off Autoplay' to 'Enabled: All drives'

Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies\Turn off Autoplay

[ ] Set 'Allow Secure Boot for integrity validation' to 'Enabled'

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Allow Secure Boot for integrity validation

[ ] Set 'Configure use of hardware-based encryption for operating system drives' to 'Enabled'

Windows Hardening recommendation

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Configure use of hardware-based encryption for operating system drives

[ ] Configure use of hardware-based encryption for operating system drives: Use BitLocker software-based encryption when hardware encryption is not available'

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Configure use of hardware-based encryption for operating system drives: Use BitLocker software-based encryption when hardware encryption is not available

[ ] Set 'Require additional authentication at startup' to 'Enabled'

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Require additional authentication at startup

[ ] Set 'Require additional authentication at startup: Allow BitLocker without a compatible TPM' to 'Enabled: False'

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Require additional authentication at startup: Allow BitLocker without a compatible TPM

[ ] Set 'Require trusted path for credential entry' to 'Enabled'

Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface\Require trusted path for credential entry

[ ] Set 'Allow Telemetry' to 'Enabled: 0 - Security [Enterprise Only]'

Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Allow Telemetry

[ ] Set 'Download Mode' to 'Disabled'

Computer Configuration\Policies\Administrative Templates\Windows Components\Delivery Optimization\Download Mode

[ ] Set 'Application: Control Event Log behavior when the log file reaches its maximum size' to 'Disabled'

Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Application\Control Event Log behavior when the log file reaches its maximum size

Windows Hardening recommendation

[ ] Set 'Application: Specify the maximum log file size (KB)' to 'Enabled: 32,768 or greater'

Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Application\Specify the maximum log file size (KB)

[ ] Set 'Security: Control Event Log behavior when the log file reaches its maximum size' to 'Disabled'

Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security\Control Event Log behavior when the log file reaches its maximum size

[ ] Set 'Security: Specify the maximum log file size (KB)' to 'Enabled: 196,608 or greater'

Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security\Specify the maximum log file size (KB)

[ ] Set 'Setup: Control Event Log behavior when the log file reaches its maximum size' to 'Disabled'

Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Setup\Control Event Log behavior when the log file reaches its maximum size

[ ] Set 'Setup: Specify the maximum log file size (KB)' to 'Enabled: 32,768 or greater

Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Setup\Specify the maximum log file size (KB)

[ ] Set 'System: Control Event Log behavior when the log file reaches its maximum size' to 'Disabled'

Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\System\Control Event Log behavior when the log file reaches its maximum size

[ ] Set 'System: Specify the maximum log file size (KB)' to 'Enabled: 32,768 or greater'

Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\System\Specify the maximum log file size (KB)

[ ] Set 'Configure Windows SmartScreen' to 'Enabled: Require approval from an administrator before running downloaded unknown software'

Erstellt von Jörn Walter **30.12.2017**

Windows Hardening recommendation

Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer\Configure Windows SmartScreen

[ ] Set 'Turn off Data Execution Prevention for Explorer' to 'Disabled'

Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer\Turn off Data Execution Prevention for Explorer

[ ] Set 'Turn off heap termination on corruption' to 'Disabled'

Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer\Turn off heap termination on corruption

[ ] Set 'Turn off shell protocol protected mode' to 'Disabled'

Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer\Turn off shell protocol protected mode

[ ] Set 'Prevent the computer from joining a homegroup' to 'Enabled'

Computer Configuration\Policies\Administrative Templates\Windows Components\HomeGroup\Prevent the computer from joining a homegroup

[ ] Set 'Prevent the usage of OneDrive for file storage' to 'Enabled'

Computer Configuration\Policies\Administrative Templates\Windows Components\OneDrive\Prevent the usage of OneDrive for file storage

[ ] Set 'Allow users to connect remotely by using Remote Desktop Services' to 'Disabled'

Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections\Allow users to connect remotely by using Remote Desktop Services

[ ] Set 'Allow Cortana' to 'Disabled'

Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow Cortana

[ ] Set 'Allow indexing of encrypted files' to 'Disabled'

Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow indexing of encrypted files

[ ] Set 'Allow search and Cortana to use location' to 'Disabled'

Windows Hardening recommendation

Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow search and Cortana to use location

[ ] Set 'Set what information is shared in Search' to 'Enabled: Anonymous info'

Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Set what information is shared in Search

[ ] Set 'Join Microsoft MAPS' to 'Disabled'

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender\MAPS\Join Microsoft MAPS

[ ] Set 'Enables or disables Windows Game Recording and Broadcasting' to 'Disabled'

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Game Recording and Broadcasting\Enables or disables Windows Game Recording and Broadcasting

[ ] Set 'Prevent Internet Explorer security prompt for Windows Installer scripts' to 'Disabled'

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Prevent Internet Explorer security prompt for Windows Installer scripts

[ ] Set 'Configure Automatic Updates' to 'Enabled'

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates

[ ] Set 'Turn off toast notifications on the lock screen' to 'Enabled'

User Configuration\Policies\Administrative Templates\Start Menu and Taskbar\Notifications\Turn off toast notifications on the lock screen

[ ] Set 'Turn off Help Experience Improvement Program' to 'Enabled'

User Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication Settings\Turn off Help Experience Improvement Program

[ ] Set 'Always install with elevated privileges' to 'Disabled'

User Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges