2 Deaktivierung und Reduktion

Dieses Kapitel beschreibt die unterschiedlichen Varianten zur Deaktivierung der Erhebung von Telemetrie-

Daten. Es werden nur System-basierte Maßnahmen vorgestellt. Netzwerk-basierte Maßnahmen werden in

(ERNW_WP4.1) dargestellt, sie bedienen sich der Funktionalita t typischer zentraler Netzwerkkomponenten

wie beispielsweise Proxy- und Domain Name System (DNS)-Servern.

2.1 Deaktivierung von Telemetrie-Dienst und ETW Session

Der Telemetrie-Dienst ist die Kernkomponente der Telemetrie. Der Dienst ist sowohl verantwortlich für

das Sammeln der Telemetrie-Daten wie auch für das Senden dieser Daten. Eine ausführliche Beschreibung

des Telemetrie-Diensts für Windows 10, Version 1607, 64 Bit, deutsche Sprache aus dem Long-Term

Servicing Branch (LTSB) findet sich in (ERNW_WP4). Im Folgenden werden nur Änderungen beschrieben,

die einen Einfluss auf die Deaktivierung des Dienstes haben. Die primäre Datensammlung geschieht über

die ETW-Session DiagTrack-Listener. Diese ETW-Session ist die Quelle der primären Telemetrie-

Daten. Diese ETW-Session sammelt Daten unabhängig davon, ob der Telemetrie-Dienst ausgeführt wird

oder nicht. Um den Telemetrie-Dienst und die primäre Datensammlung zu deaktivieren, sind die folgenden

Schritte notwendig:

1. Der Telemetrie-Dienst Benutzererfahrung und Telemetrie im verbundenen Modus

(Connected User Experience and Telemetry) muss deaktiviert werden.

2. Es muss die DiagTrack-Listener Session deaktiviert werden. Die Deaktivierung des

Autologgers kann in der Registry vorgenommen werden; dazu muss der Wert des entsprechenden

Registrierungsschlüssels auf 0 gesetzt werden.

3. Löschen der Logdatei(en) des Autologgers unter

%systemroot%\System32\LogFiles\WMI\Diagtrack-Listener.etl<id>, falls diese

vorhanden sind.

1

4. Neustarten des Systems.

Schnittstelle Pfad/Befehl

services.msc Benutzererfahrung und Telemetrie im verbundenen Modus →

Eigenschaften →

Starttyp → Deaktiviert

Registry HKLM\SYSTEM\CurrentControlSet\Services\DiagTrack\Start = 4

PowerShell Get-Service -Name "DiagTrack" | Stop-Service -PassThru |

Set-Service -StartupType Disabled -PassThru

oder

Set-ItemProperty -Path

HKLM:\SYSTEM\CurrentControlSet\Services\DiagTrack\ -Name

Start -Value 4

Tabelle 1: Schritt 1: Deaktivierung der Benutzererfahrung und Telemetrie im Verbund Modus

Schnittstelle Pfad/Befehl

Registry HKLM\SYSTEM\CurentControlSet\Control\

WMI\Autologger\Diagtrack-Listener\Start = 0

PowerShell Get-AutologgerConfig -Name "Diagtrack-Listener" | Set-

AutologgerConfig -Start 0 -PassThru

oder

Set-ItemProperty -Path

HKLM:\SYSTEM\CurrentControlSet\Control\WMI\Autologger\Di

agtrack-Listener\ -Name Start -Value 0

Perfmon.exe Datensammlersätze →

Startereignis-Ablaufverfolgunssitzungen →

Diagtrack-Listener →

Eigenschaften →

Ablaufverfolgungssitzung →

Haken bei Aktiviert entfernen

Tabelle 2: Schritt 2: Deaktivierung der Diagtrack-Autologger Session

Schnittstelle Pfad/Befehl

Explorer.exe Löschen von %systemroot%\System32\LogFiles\WMI\Diagtrack-

Listener.etl

PowerShell Remove-Item "LogFiles\WMI\Diagtrack-Listener.etl*"

Tabelle 3: Schritt 3: Löschen der Autologger Logdatei falls vorhanden

Im Vergleich zu (ERNW_WP4.1) gibt es nur noch eine ETW-Session. Diese ETW-Session wird nicht mehr

durch Stoppen des Dienstes deaktiviert, aus diesem Grund muss der Autologger Registry Key zwingend

gesetzt werden, um die primäre Datensammlung zu unterbinden. In dieser ETW-Session werden nun die

Daten erhoben, die früher in der vom Telemetrie-Dienst gestarteten Diagtrack-Listener ETW-Session

sowie in der Autologger-Diagtrack-Listener Session erhoben wurden.

2.2 Deaktivierung Telemetrie nach Microsoft Empfehlung

Microsoft stellt eigene Empfehlungen (ms_configdiag) bereit, um die Erhebung von Telemetrie-Daten zu

deaktivieren, beziehungsweise zu reduzieren. Um die Anzahl der ETW-Provider, die in die ETW-Session

Daten schreiben, zu reduzieren, kann der Telemetrie-Level konfiguriert werden. Unter Windows 10

Enterprise gibt es die Möglichkeit das Level auf “0 – Security” zu setzen2. Microsoft weist darauf hin,

dass diese Einstellung nicht gewählt werden soll, wenn Windows Updates benötigt werden, da im Falle

eines fehlgeschlagenen Updates keine Telemetrie-Daten gesendet werden, welche im Supportfall relevant

sein könnten. Wird das Telemetrie-Level auf “0 – Security” gesetzt, werden laut (ms_configdiag) keine

Telemetrie-Daten an Microsoft übertragen. Es wurde festgestellt, dass bei diesem Level weiterhin Daten in

der ETW-Session gesammelt und lokal gespeichert werden. In einer Testumgebung konnte innerhalb von

48 Stunden keine Netzwerkkommunikation des Telemetrie-Dienstes identifiziert werden, das heißt, es fand

keine Übertragung der lokal gespeicherten Telemetrie-Daten statt.

GPO (gpoedit.msc) In gpedit.msc:

Computerkonfiguration

→ Administrative Vorlagen

→ Windows-Komponenten

→ Datensammlung und Vorabversionen

Telemetrie zulassen öffnen,

Einstellung auf Aktiviert,

Optionen auf 0 – Sicherheit (Nur Enterprise).

(Falls die Einstellung auf „deaktiviert“ gesetzt wird, wird die

Nutzerkonfiguration übernommen und nicht Telemetrie allgemein

deaktiviert)

Registry Via regedit.exe den folgenden Pfad zu AllowTelemetry

(REG_DWORD) öffnen:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Polic

ies\DataCollection\AllowTelemetry

und auf 0 setzen.

PowerShell Set-ItemProperty -Path

HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Po

licies\DataCollection\ -name AllowTelemetry -Value

0

Tabelle 4: Konfiguration des niedrigst möglichen Telemetrie-Levels

Microsoft hat die Dokumentation (ms_configdiag) zur Konfiguration des Telemetrie-Levels angepasst. Die

in (ERNW_WP4.1) beschriebenen Schritte beziehen sich auf eine alte Version der Microsoft-

Dokumentation. Der Hauptunterschied ist, dass Microsoft die Definition des Telemetrie-Levels “0 –

Security” geändert hat. In der aktuellen Version der Dokumentation bedeutete dieses Level, dass keine

Daten an Microsoft übertragen werden. In der Vergangenheit hat dies nur zu einer Reduktion der

Messpunkte geführt, und weitere Dienste (z.B. Windows Update) mussten zusätzlich deaktiviert werden.

2.3 Lokale Firewall-Regeln

Mit der im Betriebssystem integrierten Funktion Windows Defender Firewall mit erweiterter

Sicherheit lassen sich unter anderem Netzwerkverbindungen von ausführbaren Dateien blockieren. Da

für die Übermittlung der DiagTrack-Dienst verantwortlich ist, soll dieser an der Ausführung gehindert

werden. Es existieren zwei Wege zum Blockieren der Telemetrie. Entweder kann eine vordefinierte Regel

verwendet werden oder der Netzwerkverkehr des Dienstes selbst blockiert werden. Tabelle 5 beschreibt

das Blockieren mithilfe einer vordefinierten Regel. Tabelle 6 beschreibt das Blockieren des DiagTrack

Dienstes.

Schnittstelle Pfad/Befehl

wf.msc Ausgehende Regel → Neue Regel → Vordefiniert → DiagTrack →

Benutzererfahrungen und Telemetrie im Verbund

auswählen→ Verbindung blockieren

Tabelle 5: Windows Defender Firewall Regel zum Blockieren der vordefinierten Verbindung

Schnittstelle Pfad/Befehl

wf.msc Ausgehende Regel → Neue Regel →Benutzerdefiniert→ Dienste Anpassen

→ Auf diesen Dienst anwenden → Benutzererfahrungen und Telemetrie

im Verbund → Weiter → (Protokolle und Ports) Weiter → (Bereich)

Weiter →Verbindung blockieren → Profile alle → Name angeben →

Fertigstellen

PowerShell New-NetFirewallRule -DisplayName

"BlockDiagTrackService" -Name

"BlockDiagTrackService" -Direction Outbound -Service

"DiagTrack" -Action Block

Tabelle 6: Windows Defender Firewall Regel zum Blockieren der Telemetrie

In (ERNW_WP4.1) wird ein alternativer Ansatz vorgestellt. Hierzu wird das ausführende Programm des

Dienstes blockiert. Viele Windows-Dienste, darunter auch der DiagTrack-Dienst, werden im Kontext des

Windows Dienst-Host Prozesses svchost.exe ausgeführt. Ein Blockieren von Netzwerkverbindungen

dieser ausführbaren Datei würde also nicht nur den DiagTrack-Dienst blockieren, sondern auch alle

anderen Dienste, die im Kontext von eines Windows Dienst-Host Prozesses (d.h. svchost.exe)

ausgeführt werden. Daher wurde eine Lösung vorgestellt, in der erst die ausführbare Datei des Windows

Dienst-Host Prozesses svchost.exe dupliziert und umbenannt wird. Dieses Duplikat wird genutzt, um

den DiagTrack-Dienst auf Grundlage des Dateinamens zu isolieren. Dieses Duplikat wird dann von der

Firewall auf Basis des Dateinamens blockiert. Dieser Ansatz funktioniert auch weiterhin.

Die nachfolgende schrittweise Erklärung ist (ERNW_WP4.1) entnommen und beschreibt, wie sich der

DiagTrack-Dienst (welcher im duplizierten Windows Dienst-Host Prozess ausgeführt wird) von den

anderen Diensten isolieren lässt, um nur diesen Dienst an der Initiierung von Netzwerkverbindungen zu

hindern.

1. Erstellung eines Hardlinks auf svchost.exe mit anderem Namen (in diesem Beispiel

utc_myhost.exe) in %SystemRoot%\System32\. Hierfür ist eine Anpassung der

Berechtigungen notwendig.

2. Änderung des Pfads der Ausführung in der Registrierungsdatenbank. Hierzu zum Pfad

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DiagTrack navigieren

und den Wert des Schlüssels ImagePath in %SystemRoot%\System32\utc_myhost.exe -k

utcsvc -p ändern. Damit wird der Dienst im Kontext des Duplikats ausgeführt.

3. Anlegen einer neuen ausgehenden Regel. Hierbei muss die ausführbare Datei (d.h. das Duplikat

%SystemRoot%\System32\utc_myhost.exe) angegeben werden, welche daran gehindert

werden soll Netzwerkverbindungen aufzubauen.

4. Neustarten des Systems.

Schnittstelle Pfad/Befehl

wf.msc Ausgehende Regel → Neue Regel → Programm →

%SystemRoot%\System32\utc_myhost.exe -k utcsvc -p →

Verbindung blockieren

PowerShell New-NetFirewallRule -DisplayName "BlockDiagTrack" -

Name "BlockDiagTrack" -Direction Outbound -Program

"%SystemRoot%\System32\utc_myhost.exe" -Action Block

Tabelle 7: Windows Defender Firewall Regel zum Blockieren des duplizierten Telemetrie-Dienst

Referenzen

ERNW_WP4. „SiSyPHuS Win10 (Studie zu Systemaufbau, Protokollierung, Härtung und

Sicherheitsfunktionen in Windows 10): Work Package 4.“ 2018.

ERNW_WP4.1. „SiSyPHuS Win10 (Studie zu Systemaufbau, Protokollierung, Härtung und

Sicherheitsfunktionen in Windows 10): Work Package 4.1.“ 2020.

ms_configdiag. Configure Windows diagnostic data in your organization. 2021. 13. 12 2021. <

https://docs.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-

organization>.

Eindeutige ID: #1016
Verfasser: n/a
Letzte Änderung: 2022-06-08 19:07