Windows 10 Telemetrie-Prüfung mit Nutzerinteraktion

Verantwortliche Durchführung für Tests und Dokumentation:	LfD Niedersachsen, Referat 3 - IT-Labor
Abschlussdatum der Tests:	14.05.2020
Finalisierung und Freigabe der Dokumentation:	17.06.2020

1 Zielsetzung des Tests

Microsoft gibt an, dass keine Übermittlung von Telemetriedaten an Microsoft erfolgt, wenn das Betriebssystem Windows 10 Enterprise sowie das von Microsoft zur Verfügung gestellte „Windows Restricted Traffic Limited Functionality Baseline“ (V1903)[1] installiert wurde.

Ende letzten Jahres wurde bereits ein Telemetrie-Test ohne Nutzerinteraktion am Windows 10 Enterprise System (durch die *Landesbeauftragte für den Datenschutz Niedersachsen (LfD Niedersachsen*) und das *Bayerische Landesamt für Datenschutz Aufsicht (BayLDA*)) durchgeführt.

Bei diesem Test wurde festgestellt, dass die datenschutzrechtlich kontrovers diskutierten Telemetriedaten bei Einsatz der Enterprise Version im überprüften Szenario deaktivierbar sind.[2]

Da Telemetriedaten ggf. erst bei Nutzeraktivität übertragen werden, soll dieser Aspekt nun in dem vorliegenden Test berücksichtigt werden.

Dazu werden die auftretenden Datenübertragungen protokolliert (Wireshark[3]-Protokolle).

Anschließend wird untersucht, ob sich in den Protokollen Verbindungen an die von Microsoft angegebenen Endpunkte („Telemetrie-Verbindungen“) finden.

Diese Endpunkte werden von Microsoft wie folgt angegeben[4]:

[1] Windows Restricted Traffic Limited Functionality Baseline: https://docs.microsoft.com/de-de/windows/privacy/manage-connections-from-windows-operating-system-components-to-microsoft-services, downloadlink: https://go.microsoft.com/fwlink/?linkid=828887, herunter geladen am 8.1.2020
[2] Siehe 9. Tätigkeitsbericht des BayLDA 2019: https://www.lda.bayern.de/media/baylda_report_09.pdf, Seite 22
[3] https://www.wireshark.org/
[4] https://docs.microsoft.com/de-de/windows/privacy/configure-windows-diagnostic-data-in-your-organization

Windows-Version	Endpunkt
Windows 10, Version 1703 oder höher, mit installiertem kumulativen Update 2018-09	**Diagnosedaten:** v10c.vortex-win.data.microsoft.com
	Funktional: v20.vortex-win.data.microsoft.com
	Microsoft Defender Advanced Threat Protection ist länderspezifisch; das Präfix ändert sich je nach Land,
	z.B.: **de**.vortex-win.data.microsoft.com
	Einstellungen: settings-win.data.microsoft.com
Windows 10, Version 1803 oder höher, ohne kumulatives 2018-09-Update installiert	**Diagnosedaten:** v10.events.data.microsoft.com
	Funktional: v20.vortex-win.data.microsoft.com
	Microsoft Defender Advanced Threat Protection ist länderspezifisch; das Präfix ändert sich je nach Land,
	z.B.: **de**.vortex-win.data.microsoft.com
	Einstellungen: settings-win.data.microsoft.com
Windows 10, Version 1709 oder früher	**Diagnosedaten:** v10.vortex-win.data.microsoft.com
	Funktional: v20.vortex-win.data.microsoft.com
	Microsoft Defender Advanced Threat Protection ist länderspezifisch; das Präfix ändert sich je nach Land,
	z.B.: **de**.vortex-win.data.microsoft.com
	Einstellungen: settings-win.data.microsoft.com

Verbindungen zu anderen Microsoft-Diensten, wie z. B. Windows Update Diensten, Windows Aktivierungsdienten oder Zertifikatsdiensten können ebenfalls im Wireshark Protokoll auftauchen, stellen aber keine „Telemetrie-Verbindungen“ im Sinne der Definition dieses Tests dar.

Es gilt somit, herauszufinden, ob im Wireshark Protokoll Verbindungen zu den in der Tabelle aufgelisteten Microsoft Endpunkten auftauchen.

Der Test beinhaltet drei unterschiedliche Prüfszenarien:

Prüfszenario 1 (Windows Restricted Traffic Limited Functionality Baseline, Telemetrielevel = 0):

- Installation des „Windows Restricted Traffic Limited Functionality Baseline“. Dadurch wird u.a. der Telemetrielevel des Systems auf „0“ gesetzt.
- 72 Stunden Betrieb eines Windows 10 Enterprise Systems, mit installiertem Microsoft „Windows Restricted Traffic Limited Functionality Baseline“ (V1903) und verschiedenen, teilweise automatisiert ablaufenden, Benutzeraktivitäten (mit systemnahen Programmen, jeweils nach Zeitplan) innerhalb der 72 Stunden des Tests.
- Mitschnitt des dabei aufgetretenen Netzwerkverkehrs.
- Auswertung des Wireshark Protokolls auf Vorhandensein von Verbindungen zu relevanten Microsoft Endpunkten (s.o.).

Prüfszenario 2 (Windows Restricted Traffic Limited Functionality Baseline, Telemetrielevel = 1):
Laut Aussage von Microsoft ist für die tatsächliche Unterbindung der Telemetriedaten-Übermittlung das Setzen des Telemetrielevels auf „0“ ausreichend.

Mit dem Prüfszenario 2 soll überprüft werden, ob bei einem Telemetrielevel größer als „0“ Netzwerkverbindungen zu den von Microsoft benannten Endpunkten in den Protokollen zu finden sind.

Der Telemetrielevel kann durch folgende Registry-Einträge geändert werden:

- **`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DataCollection`**
- **`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Policies\DataCollection`**
- **`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\default\System\AllowTelemetry`**

Der dort jeweils wiederzufindende Parameter *„AllowTelemetry“* bzw. *„Value“*
(in **`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\default\System\AllowTelemetry`**)
stellt mit den möglichen Werten 0-3 die Intensität der Microsoft-seitigen Telemetriedaten-Übermittlung dar:

- 0 = „security“ = Keine Telemetriedaten Erfassung und Übermittlung bis
- 3 = „full“ = Vollständige Telemetriedaten Erfassung und Übermittlung

Anmerkung: der Telemetrielevel „0“ kann in den Windows Home und Pro-Versionen von Windows 10 nicht gesetzt werden.

Der Versuchsaufbau in Prüfszenario 2 wird zum Prüfszenario 1 daher nur in einem Punkt (ceteris paribus) wie folgt abgeändert:

- Der Parameter-Wert *„AllowTelemetry“* (bzw. „Value“) wird manuell in den dazu verfügbaren Registrierungsvariablen auf „1“ (= „einfach“ bzw. „basic“) gesetzt.
- Laufzeit des Tests: 30 Minuten.
    - Die verkürzte Laufzeit ist damit begründet, dass zu erwarten ist, dass in Telemetrielevel 1 bereits nach kurzer Zeit Verbindungen zu den in der o.g. Tabelle angegebenen Endpunkten (insbesondere zu *v10.events.data.microsoft.com*) stattfinden.
    - Folgende Benutzeraktivitäten am Windows 10 System werden in den 30 Testminuten durchgeführt:
        - Einstecken eines beliebigen USB Sticks.
        - Erstellen einer Notepad Datei.
        - Abspeichern der Datei auf dem USB Stick.
        - Manuelles Starten des Browsers und Aufruf der Website www.rki.de mit anschließendem Aufruf von drei Links derselben Website.
        - Schließen des Browsers.
        - Start des *Invoke User Simulators* (automatisiertes Webbrowsen).

Prüfszenario 3 (Standard-Windows-Installation, Telemetrielevel = 0):

Das in Prüfszenario 1 und 2 installierte Microsoft „Windows Restricted Traffic Limited Functionality Baseline“ unterbindet nicht nur den Telemetrie-Verkehr. Es werden auch viele von Microsoft standardmäßig installierte „Zusatzprodukte“ deinstalliert. Dadurch werden die Netzwerkverbindungen an Microsoftsysteme deutlich reduziert.
In manchen Fällen möchte ein Verantwortlicher aber diese „Zusatzfunktionalitäten“ nutzen.

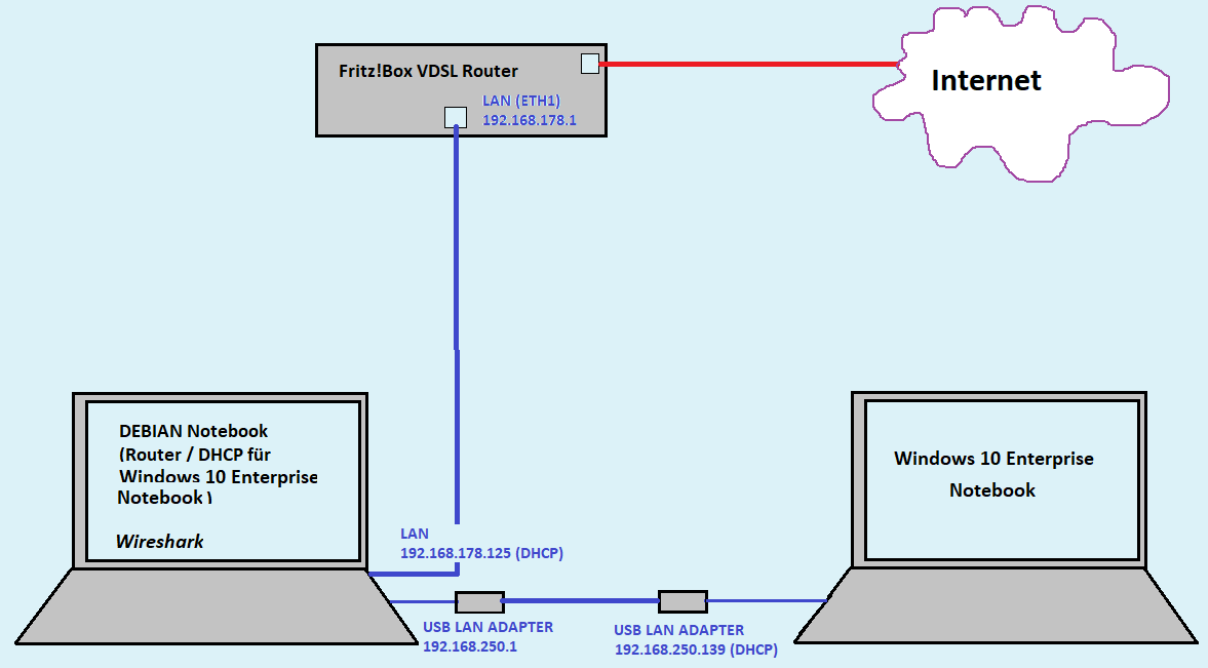
Für den Verantwortlichen wäre es also relevant zu wissen, ob die Unterbindung der Telemetrie-Datenübermittlung nur durch Setzen des Telemetrielevels auf „0“ möglich ist, ohne das „Windows Restricted Traffic Limited Functionality Baseline“ zu installieren und somit andere (ggf. im Unternehmensumfeld benötigte) Microsoft Dienste zu nutzen, die durch die Installation des Paketes nicht zur Verfügung stehen würden.

Um dies zu prüfen, wird folgender Test durchgeführt:

- Standard Installation von Windows 10 Enterprise.
- Manuelles Setzen des Telemetrielevel des Systems auf „0“.
- 72 Stunden Benutzeraktivitäten am Windows 10 System, nach Zeitplan.
- Mitschnitt des dabei aufgetretenen Netzwerkverkehrs.
- Auswertung des Wireshark Protokolls auf Vorhandensein von Verbindungen zu relevanten Microsoft Endpunkten (s.o.).

2 Beschreibung des Laboraufbaus

2.1 Grafische Darstellung des Laboraufbaus



2.2 Folgende Hardware Komponenten und Konfigurationen werden verwendet:

2.2.1 Notebook Lenovo Typ 20KE-S9020

Konfiguration:

- Windows 10 Enterprise V1909.
  Workgroup Installation ohne Anbindung an eine Domäne.
- Alle zum Testzeitpunkt vorhandenen Microsoft Updates werden installiert.
- Microsoft „ Windows Restricted Traffic Limited Functionality Baseline" (V1903) wird installiert (Prüfszenario 1 und 2).
- Kommandozeile: *ipconfig /flushdns* wird vor Durchführung jedes Prüfszenarios ausgeführt.
- Es werden darüber hinaus keine weiteren Veränderungen am Windows 10 Enterprise System vorgenommen.
- Das System wird vor jedem Test neu gestartet.

2.2.2 Notebook Fujitsu Typ E734 mit Betriebssystem Debian 10

Konfiguration:

- Nutzung der integrierten ETH NW Schnittstelle als Verbindung zur Fritz!Box.
- IP Adresse (192.168.178.x Bereich) wird per DHCP von der Fritz!Box an das Debian Notebook verteilt.
- Eine zusätzlich angeschlossene USB Netzwerkkarte dient als Netzwerk- Schnittstelle zum Windows 10 Enterprise Notebook.

- Das Debian Notebook fungiert als Router durch Nutzung des LINUX Dienstes *dnsmasq* für das Windows 10 Enterprise Testnotebook.
- DHCP Router Dienst läuft auf Debian Notebook und vergibt IP (im Adressbereich 192.168.250.x) an das Windows 10 Enterprise Notebook.

2.2.3 Fritz!Box 7590

- Dient als Netzwerk-Router für das Debian Notebook mit V-DSL Verbindung zum Internet.
- Vor jedem Prüfszenario wird der DNS Cache der Fritz!Box geleert.

3 Beschreibung des Testablaufs

Der Test simuliert einen 72 stündigen Betrieb des Windows 10 Enterprise Notebooks.
Es werden in unterschiedlichen Zeitabständen (die minutengenau in einer Tabelle erfasst sind), am Windows 10 Enterprise Notebook manuelle Tätigkeiten mit unterschiedlichen Softwarekomponenten sowie durch ein Skript gesteuerte Browseraktivitäten vorgenommen, um Anwendertätigkeiten zu simulieren.

Dazu wird eine Teilkomponente eines automatisch ablaufenden Power-Shell Skripts verwendet. Das Skript mit dem Namen *„Invoke-UserSimulator“* wurde zur automatisierten Simulation von auf dem PC ablaufenden Vorgängen entwickelt. Es ist über *Github*[5] frei verfügbar.
Verwendet wird in diesem Test nur die Web-Browsings Funktion des Skripts.

Folgende Benutzeraktionen werden durchgeführt:

3.1 Automatisiertes Web-Browsing

Das GitHub Tool *„Invoke-UserSimulator“* startet automatisch den Browser und „klickt“ skriptgesteuert automatisch in bestimmten, festgelegten Intervallen, zufällig auf Links vorgegebener (d.h. ebenfalls im Skript eingetragener) Websites, um von dort aus dann (wieder zufallsgesteuert) weiter zu browsen.
Um die im Wireshark Auswertungs-Protokoll zu erwartende Menge an IP Adressanfragen durch das automatisierte Webbrowsen nicht unnötig zu vergrößern (und so die Auswertung des Wireshark-Protokolls zu erschweren) wurde für den Test nur eine Website ausgesucht und auf dieser durch das Tool automatisiert „gesurft“.
Folgende Website wurde für das automatisierte Browsen ausgewählt und verwendet, da diese Website beim Start keine Verbindungen zu anderen Host Adressen (IP Adressen) herstellt: https://www.rki.de.
Während des Testverlaufs muss zusätzlich mit dem (zufälligen) Aufruf weiterer Websites gerechnet werden, die von der Ausgangswebsite erreichbar sind.

[5] https://github.com/ubeeri/Invoke-UserSimulator

3.2 Manuelle durchgeführte Tätigkeiten am Testsystem während des 72 Stunden Tests

Zusätzlich zum automatisierten Web-Browsing werden nach einem vorab festgelegten (und für spätere Erleichterung der Auswertung in einer Excel Tabelle erfassten) Zeitplan über 72 Stunden hinweg manuell folgende Aktivitäten am System durchgeführt:

- *Notepad* Datei erstellen, speichern, verändern und kopieren.
- *Systemsteuerung→ Ereignisanzeige „System" Events* zufällig auswählen und ansehen.
- *Paint Datei* (Zeichnung) erstellen, speichern, verändern und kopieren.
- Dateien mehrfach von und zu einem angeschlossenen *USB Stick* kopieren und ersetzen.

Hinweis:
Es wurden bewusst keine Dritthersteller-Produkte oder Teile des Microsoft Office Pakets installiert und für die Simulation benutzt, da hier von weiterem Telemetrie-Verkehr zum Software-Hersteller auszugehen ist.

4 Auswertung der Wireshark Protokolle

Das jeweils aufgezeichnete Wireshark Protokoll des Prüfszenarios wird mittels Klartextsuche („Zeichenkette") auf das Vorhandensein der Strings

- v10c *(.vortex-win.data.microsoft.com)*
- v10. *(events.data.microsoft.com)*
- v20 (.vortex-win.data.microsoft.com)
- settings-win.data.microsoft.com

durchsucht.

Laut Microsoft wird der zu erwartende Kontakt zu den Endpunkten durch DNS-Anfragen gekennzeichnet sein (die erst außerhalb des Laborsystems bzw. des Internets, aufgelöst werden), da Microsoft die IP Adressen hinter diesen Verbindungen stetig ändert.

Im Wireshark Protokoll ist somit nur das Auffinden der oben genannten Adressen (im Klartext) entscheidend.

5 Prüfergebnis

5.1 Prüfszenario 1

Im Testzeitraum von 72 Stunden konnten mit regelmäßiger Benutzeraktivität auf dem System (inkl. Web-Browsing) keine Verbindungen zu den in Kapitel 4 genannten Adressen festgestellt werden.
Eine Übermittlung von Telemetriedaten fand in diesem Szenario somit nicht statt.

5.2 Prüfszenario 2

Im Testzeitraum von nur 30 Minuten konnten mit regelmäßiger Benutzeraktivität auf dem System (inkl. Web-Browsing) bereits Verbindungen zu v10.events.data.microsoft.com und Verbindungen zu settings-win.data.microsoft.com festgestellt werden. Diese Verbindungen konnten sogar in einem zusätzlichen 30 Minuten Test ohne jegliche Benutzeraktivität festgestellt werden.
Eine Übermittlung von Telemetriedaten fand somit erwartungsgemäß statt.

5.3 Prüfszenario 3

Im Testzeitraum von 72 Stunden konnten, mit Benutzeraktivität, auf dem System (inkl. Web-Browsing) nur Verbindungen zu settings-win.data.microsoft.com festgestellt werden.
Eine Übermittlung von Telemetriedaten, insbesondere von an v10 übermittelten Diagnosedaten, hat somit nicht stattgefunden.

6 Fazit

Durch diese Tests konnten die Aussagen der Firma Microsoft nicht widerlegt werden, dass in der oben beschriebenen Konfiguration keine Telemetriedaten übermittelt werden. Hieraus kann jedoch nicht der Schluss gezogen werden, dass eine Telemetrie-Datenübermittlung grundsätzlich nicht stattfindet. Daher sind Verantwortliche stets in der Pflicht zu prüfen, ob der Einsatz von Windows 10 auch in ihrer individuellen System- und Verarbeitungssituation datenschutzrechtlich zulässig ist.

Ein besonderes Augenmerk ist auf Verbindungen zu settings-win.data.microsoft.com zu legen, da die Möglichkeit besteht, dass über diese Verbindung Konfigurationsdaten heruntergeladen werden, durch die Änderungen am Verhalten des Telemetriedienstes bewirkt werden könnten.

Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstraße 5
30159 Hannover
Telefon 0511 120-4500
Fax 0511 120-4599
E-Mail poststelle@lfd.niedersachsen.de