[Nicholas Vollmer: Die Aufsichtsbehörden fordern dazu auf, die Telemetriedaten-Übertragung von MS-Windows zu stoppen und dafür einen Nachweis zu erbringen. Weil sich die Software ständig ändert, ist dies kaum zu gewährleisten. Es ist die Frage, inwieweit all dies nur dem Zweck dient MS unter Druck zu setzen.

Die Basis dafür wurde im November 2019 gelegt, als die DSK erstmals ausführliche Analysen durchführte.]

DATENSCHUTZKONFERENZ

Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

Telemetriefunktionen und Datenschutz beim Einsatz von Windows 10 Enterprise

Stand: 26.11.2020

In der 98. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) wurde ein Prüfschema zum datenschutzkonformen Einsatz von Windows 10 beschlossen und anschließend veröffentlicht[1]. Damit soll den Verantwortlichen die Überprüfung der Einhaltung der datenschutzrechtlichen Vorgaben beim Einsatz von Windows 10 erleichtert werden. Eine Arbeitsgruppe der DSK hat unter Beteiligung von LDA Bayern, BfDI, LfDI Mecklenburg-Vorpommern und LfD Niedersachsen seitdem ihre Untersuchung von Windows 10 in Hinblick auf die Telemetriestufe Security, die in der Enterprise-Edition verfügbar ist, fortgesetzt.

Unabhängig davon hat sich das an einer Laboruntersuchung der Arbeitsgruppe neben dem LfD Bayern als Gast beteiligte BSI selbst in einer umfangreichen Studie (SiSyPHuS-Studie) auch mit Fragstellungen der Windows-10-Telemetriefunktion beschäftigt.

Untersuchungsergebnisse der DSK-Arbeitsgruppe

Die Arbeitsgruppe hat die Telemetrie von Windows 10 einer Laboruntersuchung unterzogen, um festzustellen, ob sich die Telemetriedatenübermittlung durch Konfiguration unterbinden lässt. Microsoft hat gegenüber den Aufsichtsbehörden erklärt, dass bei der Nutzung der Telemetriestufe Security keine Telemetriedaten[2] übermittelt werden.

Es wurde Windows 10 Enterprise in der Version 1909 in drei Testszenarien untersucht. In allen drei Szenarien wurden Benutzeraktivitäten simuliert, um realistische Ergebnisse zu erzielen.

1. Anwendung des „Windows Restricted Traffic Limited Functionality Baseline“, Telemetriestufe „Security“, 72 Stunden Testzeitraum

2. Anwendung des „Windows Restricted Traffic Limited Functionality Baseline“, Telemetriestufe „Basic“, 30 Minuten Testzeitraum

3. Keine Anwendung des „Windows Restricted Traffic Limited Functionality Baseline“, Telemetriestufe „Security“, 72 Stunden Testzeitraum

[1] https://www.datenschutzkonferenz-online.de/media/ah/20191106_win10_pruefschema_dsk.pdf
[2] Zum Begriff siehe Bericht Windows 10 Telemetrie-Prüfung mit Nutzerinteraktion (Anlage 1)

Die Details der Untersuchung können dem Laborbericht (Anlage 1) entnommen werden.

Die Untersuchung hat bestätigt, dass im zweiten Prüfszenario die Übermittlung von Telemetriedaten festgestellt werden konnte. Im dritten Szenario wurde ein Verbindungsaufruf zum settings-win.data.microsoft.com Endpunkt festgestellt. Dieser Endpunkt wird laut Aussage von Microsoft von mehreren Windows-10-Systemkomponenten, auch von der Telemetriekomponente, angesteuert. Nutzt die Telemetriekomponente diesen Endpunkt, besteht die Möglichkeit, dass hierüber Konfigurationsdaten heruntergeladen werden, durch die Änderungen am Verhalten des Telemetriedienstes bewirkt werden könnten. Microsoft hat diesen Aufruf gegenüber den Datenschutzaufsichtsbehörden auf Basis eines Microsoft zur Verfügung gestellten Laborszenarios erläutert und erklärt diesen mit einer anderen Systemkomponente abseits der Telemetrie. Microsoft hat auf mündliche Nachfrage gegenüber den Datenschutzaufsichtsbehörden erklärt, dass trotz eines – möglicherweise aufgrund eines Softwarefehlers – unbeabsichtigten Aufrufs an den settings-win.data.microsoft.com Endpunkt von dem Telemetriedienst, bei einem Telemetrielevel „Security“ weiterhin keine Telemetriedatenübermittlung stattfinden würde.

Untersuchungsergebnisse des BSI

In einer den Labortest der Arbeitsgruppe ergänzenden Untersuchung des Windows-10-Enterprise-Datenverkehrs durch das BSI im Januar 2020 wurden Datenübertragungen zu „settings-win.data.microsoft.com“ festgestellt (siehe Anlage 2).

Dabei wurde ein Windows 10 Enterprise System Version 1803 mit Telemetrielevel Security und „Windows Restricted Traffic Limited Functionality Baseline“ genutzt. Es ist jedoch zu beachten, dass die Verbindungen zu „settings-win.data.microsoft.com“ nicht im Klartext analysiert werden konnten und somit die Möglichkeit besteht, dass Microsoft über diesen Kanal Daten exfiltriert oder in unerwünschter Weise Einfluss auf das System nimmt. Vor diesem Hintergrund hält das BSI aufgrund eines Defense-in-Depth-Ansatzes zur Stärkung der Sicherheit der IT-Systeme des Bundes an der Notwendigkeit einer Netztrennung von Windows-10-Clients der Bundesverwaltung, auch zur Abwehr von Schadcodes, fest.

Laut Microsoft wird über den Endpunkt „settings-win.data.microsoft.com“ auch die Konfiguration der Windows-Komponente „Benutzererfahrungen und Telemetrie im verbundenen Modus“ dynamisch aktualisiert.[3] Auch im BSI-Projekt „SiSyPHuS“ ist diese Adresse mehrfach im Zusammenhang mit der dynamischen Konfiguration der Windows-Telemetrie genannt.[4]

Den Feststellungen zur Folge könnte Microsoft darüber das Verhalten des Telemetriedienstes anpassen, Art und Umfang der Datenerhebung konfigurieren oder Kommandos zur Anreicherung der Daten ausführen, ohne dass der Nutzer dem zustimmen müsse oder das kontrollieren könne. Vor diesem Hintergrund sind Verbindungen zu diesem Endpunkt nach der Bewertung des BSI zumindest als bedenklich einzustufen.

3 https://docs.microsoft.com/de-de/windows/privacy/manage-windows-1803-endpoints
4 https://bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Workpackage4_Telemetry.pdf

Konsequenzen für Verantwortliche

Im veröffentlichten Prüfschema wird erläutert, dass Verantwortliche den Nachweis für die Rechtmäßigkeit etwaiger Übermittlungen personenbezogener Daten an Microsoft erbringen oder die Übermittlung personenbezogener Daten unterbinden müssen.

Zur Unterbindung der Übermittlung personenbezogener Telemetriedaten haben die Verantwortlichen beim Einsatz der Enterprise-Edition die Telemetriestufe Security zu nutzen und mittels vertraglicher, technischer oder organisatorischer Maßnahmen (z. B. durch eine Filterung der Internetzugriffe von Windows-10-Systemen über eine entsprechende Infrastruktur) sicherzustellen, dass nachweislich keine Übermittlung von Telemetriedaten an Microsoft stattfindet.

Angesichts ggf. weiterer offener Fragen, die z. B. mit dem Aufruf der „settings-win.data.microsoft.com“-Datenverbindung verbunden sind oder die auch die SiSyPHuS-Studie des BSI aufwirft, wie des Umstands, dass die vorliegenden Untersuchungen auf Grund laufender Fortentwicklungen der Software natürlich nur eine Momentaufnahme darstellen, können die bisherigen Untersuchungen Verantwortliche nicht abschließend von ihrer aus Art. 5 Abs. 2 DS-GVO abzuleitenden Prüf- und Nachweispflicht für den datenschutzkonformen Einsatz von Windows 10 hinsichtlich der Übermittlung von Telemetriedaten entlasten. Dies gilt erst Recht für Verantwortliche, die Windows 10 in der Pro- und Home-Edition einsetzen, in denen die Telemetriestufe derzeit nicht auf Security gesetzt werden kann. In diesen Fällen bleiben ohnehin andere Maßnahmen zur Unterbindung etwaiger Übermittlungen personenbezogener Telemetriedaten zu prüfen oder die Rechtmäßigkeit der Übermittlung nachzuweisen.

Deshalb sollte Windows 10 in allen angebotenen Editionen die Möglichkeit bieten, die Telemetriedatenverarbeitung durch Konfiguration zu deaktivieren. Dazu und zu den in den Labor-Untersuchungen der DSK und der SiSyPHus-Studie des BSI aufgezeigten verbliebenen Unwägbarkeiten werden die Datenschutzaufsichtsbehörden das weitere Gespräch mit Microsoft führen.

Die Landesbeauftragte für den Datenschutz Niedersachsen

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.

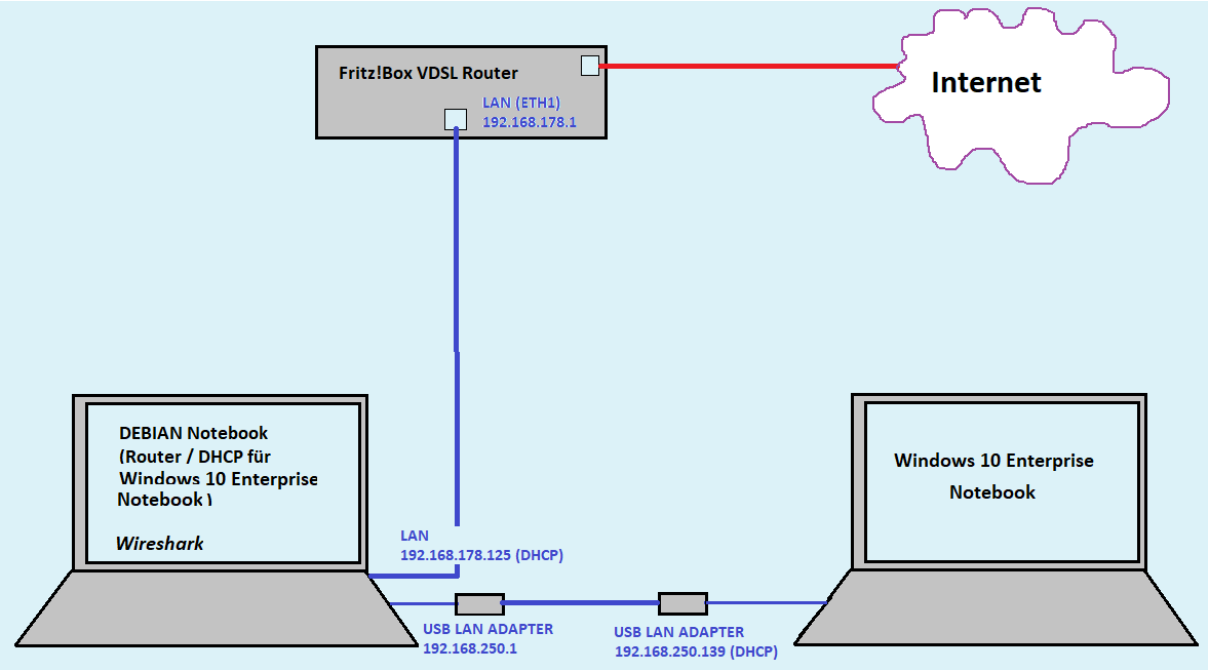
Für den Verantwortlichen wäre es also relevant zu wissen, ob die Unterbindung der Telemetrie-Datenübermittlung nur durch Setzen des Telemetrielevels auf „0“ möglich ist, ohne das „Windows Restricted Traffic Limited Functionality Baseline“ zu installieren und somit andere (ggf. im Unternehmensumfeld benötigte)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

Bundesamt
für Sicherheit in der
Informationstechnik

Anlage 2

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63, 53133 Bonn

Verteiler:

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
Referat 23

Bayerisches Landesamt für Datenschutzaufsicht
Bereichsleiter Cybersicherheit und Technischer Datenschutz

Die Landesbeauftragte für den Datenschutz Niedersachsen
Referat 3

Robert Krause

Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189
53175 Bonn

POSTANSCHRIFT
Postfach 20 03 63
53133 Bonn

TEL +49 228 99 9582 5697
FAX +49 228 9910 9582 5697

referat-tk12@bsi.bund.de

https://www.bsi.bund.de

Betreff: Untersuchung Windows 10 Enterprise Datenverkehr

Bezug: Windows 10 Prüfung beim BayLDA am 10./11.12.2019
Geschäftszeichen: TK 12 – 240 05 00
Datum: 28.01.2020

Sehr geehrte Damen und Herren,

die deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder befassen sich mit der Frage, ob und unter welchen Konfigurationsmöglichkeiten das Betriebssystem Windows 10 von Verantwortlichen in Deutschland eingesetzt werden kann. Ein besonderes Augenmerk liegt dabei auf den sogenannten Telemetriedaten, die Windows 10 automatisch an Microsoft überträgt.

Zu diesem Thema fand am 10./11.12.2019 beim Bayrischen Landesamt für Datenschutzaufsicht ein Treffen von Behördenvertretern mit Microsoft zu einem technischen Fachaustausch statt, an dem auch das BSI aus IT-Sicherheits-Perspektive teilgenommen hat. Ziel war es, zu einer Aussage zu gelangen, ob Windows 10 Enterprise datenschutzkonform betrieben werden kann. In einem Versuchsaufbau sollte zudem nachgewiesen werden, dass keine unerwünschten Daten, insbesondere keine Telemetriedaten, mehr an Microsoft übertragen werden.

Als Ergebnis konnte festgestellt werden, dass im beobachteten Zeitraum keine Daten an Microsoft übertragen wurden, bei denen von einem besonderen datenschutz- oder it-technischen Risiko auszugehen ist. Auf Grund dessen, dass im Versuchsaufbau keine Nutzerinteraktion und weitere technische Rahmenbedingungen (z.B. Domänenmitgliedschaft und Updates) nachgebildet werden konnten, wurde das Interesse geäußert, auch diese Teilaspekte nochmals zu beleuchten.

Dies hat das BSI in einem eigenen Versuchsaufbau mit Blick auf IT-Sicherheitsaspekte getan, der im Folgenden erläutert sowie die Ergebnisse vorgestellt werden sollen.

Versuchsaufbau

Über einen Untersuchungszeitraum von 72 Stunden wurden folgende Systeme in virtuellen Maschinen betrieben:

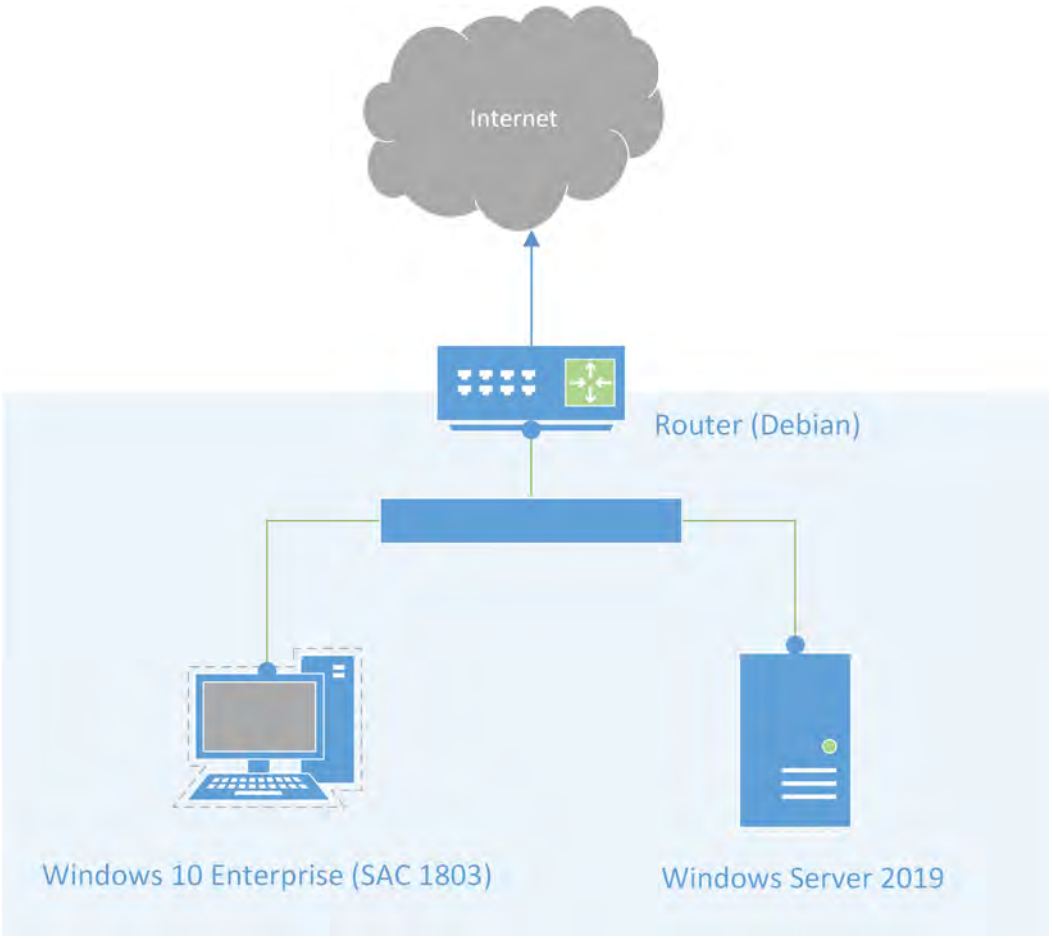
- Router (Debian 10)
  - Einsatz als Router, DHCP-Server, DNS-Server
  - Verwendung von tcpdump zur Aufzeichnung des Netzwerkverkehrs
  - Verwendung zur live-Darstellung der Datenverbindungen

- Windows 10 Server 2019
  - Einsatz als Domaincontroller, DNS-Server, WSUS-Server
  - Bereitstellung der Gruppenrichtlinie zur Verwendung eines WSUS-Servers
  - Bereitstellung von Updates für Windows 10 SAC 1803

- Windows 10 Enterprise (SAC 1803)
  - Einsatz als Workstation
  - Anwendung der Windows Restricted Traffic Limited Functionality Baseline[1] für Windows 10 SAC 1803
  - Domänen-Mitglied
  - Bezug von Updates über WSUS-Server der Domäne
  - Verwendung von Fiddler und procmon zur lokalen Systemüberwachung
  - Deaktivierung des Zertifikat-Pinnings durch Setzen des Schlüssels „SkipMicrosoftRootCertCheck“ in HKLM/SOFTWARE/Microsoft/Windows/CurrentVersion/Diagnostics/DiagTrack/TestHooks auf DWORD 0x1
  - Simulation von Nutzer- und Systemverhalten
    - Regelmäßige Prüfung auf Updates und deren Installation
    - Regelmäßige Neustarts
    - Simulation von Systemauslastung und Abstürzen (via Sysinternal Suite)
    - Starten und Verwenden von Programmen (ohne Internetfunktionen), z.B. Wordpad, Notepad, Powershell, Systemkommandos
    - De- und Installation weiterer Programme, Rekonfiguration der Einstellungen per GUI

1 https://docs.microsoft.com/de-de/windows/privacy/manage-connections-from-windows-operating-system-components-to-microsoft-services

Das Netzwerkdiagramm stellt sich wie folgt dar:



Ergebnis

Im gesamten Untersuchungszeitraum haben 2741 Pakete (1.919.128 Bytes) das Netzwerk über den Router hinaus zum Internet hin verlassen. Im Detail sind dabei folgende Endpunkte adressiert worden:

119 packets	26991 bytes	Microsoft Store Images (store-images.s-microsoft.com)	(23.210.254.117)
1931 packets	1594376 bytes	[u'www.fiddler2.com', u'fiddler2.com']	(50.56.19.116)
11 packets	2561 bytes	a2-22-119-98.deploy.static.akamaitechnologies.com	(2.22.119.98)
12 packets	2159 bytes	Microsoft.com Website (www.microsoft.com)	(23.210.253.93)
76 packets	11159 bytes	a2-22-119-33.deploy.static.akamaitechnologies.com	(2.22.119.33)
59 packets	13467 bytes	a2-22-89-31.deploy.static.akamaitechnologies.com	(2.22.89.31)
344 packets	123752 bytes	Windows Apps dynamic configuration update (settings-win.data.microsoft.com)	(40.74.35.71)
123 packets	126499 bytes	UNKNOWN	(52.155.217.156)
15 packets	3195 bytes	a2-22-94-250.deploy.static.akamaitechnologies.com	(2.22.94.250)
51 packets	14969 bytes	a2-19-241-220.deploy.static.akamaitechnologies.com	(2.19.241.220)

Diese sollen nun gesondert betrachtet werden.

50.56.19.116 – fiddler2.com – 1.6 MB / 1931 Pakete

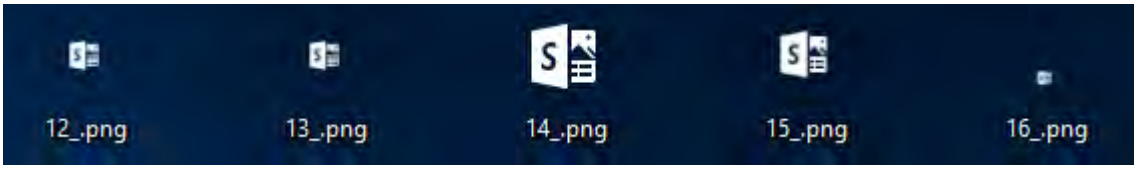
Diese IP wurde jeweils beim Starten der Anwendung „Fiddler2“ abgerufen und dient der Überprüfung und dem Bezug von Aktualisierungen. Es handelt sich um eine Verbindung, die nicht Microsoft Windows zuzurechnen ist und kann daher bei dieser Untersuchung unbeachtet bleiben.

23.210.254.117 – store-images.s-microsoft.com – 27 KB / 119 Pakete

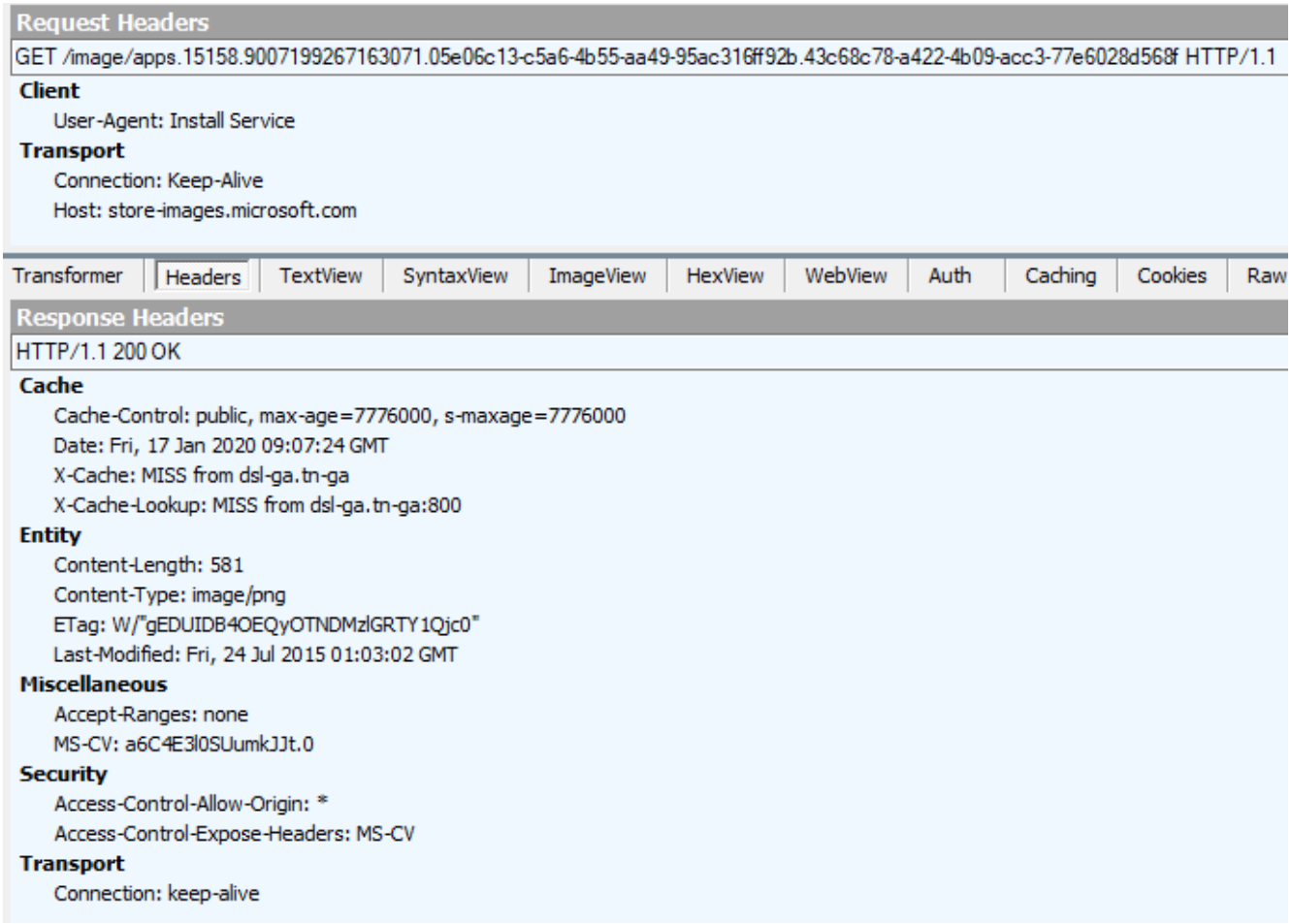
Über den gesamten Zeitraum sind Verbindungen zum Bildarchiv des Microsoft Stores zu verzeichnen.

15	200	HTTP	store-images.microsoft.com	/image/apps.15158.9007199267163071.05e06c13-c5a6-4b55-aa49-95ac316ff92b.43c68c78-a422-4b09-acc3-77e6028d568f
16	200	HTTP	store-images.microsoft.com	/image/apps.14793.9007199267163071.55f83110-ba62-4b6a-bc0a-8f12f27a5bb9.361cbfef-c19c-41d3-8a02-b1e3c8b2d188
17	200	HTTP	store-images.microsoft.com	/image/apps.63578.9007199267163071.f2756185-4638-47e0-9958-1ed9aa60f2a0.7480e404-ca1b-478b-846a-0b8514815b60
18	200	HTTP	store-images.s-microsoft.com	/image/apps.11611.9007199267163071.051d6f39-e04c-4c03-be99-103ab2771658.78beb32a-1635-487b-8355-2003309e37cf
19	200	HTTP	store-images.s-microsoft.com	/image/apps.47093.9007199267163071.afa2c461-b588-4b32-97c1-b7daddc7d914.9e65fb00-e27b-4e87-b6aa-c6626c8503b1

Im Detail handelt es sich dabei um das Herunterladen von Bildern, u.a. von der Anwendung „Office Sway“, bei der es sich um eine Präsentations-Webanwendung handelt. Grund dafür ist vermutlich, die Anwendung als Schnellzugriff im dynamischen Startmenü von Windows anzubieten zu können.



Neben den Bilddaten, sind im Rahmen der Datenverbindung folgende Informationen übertragen worden.



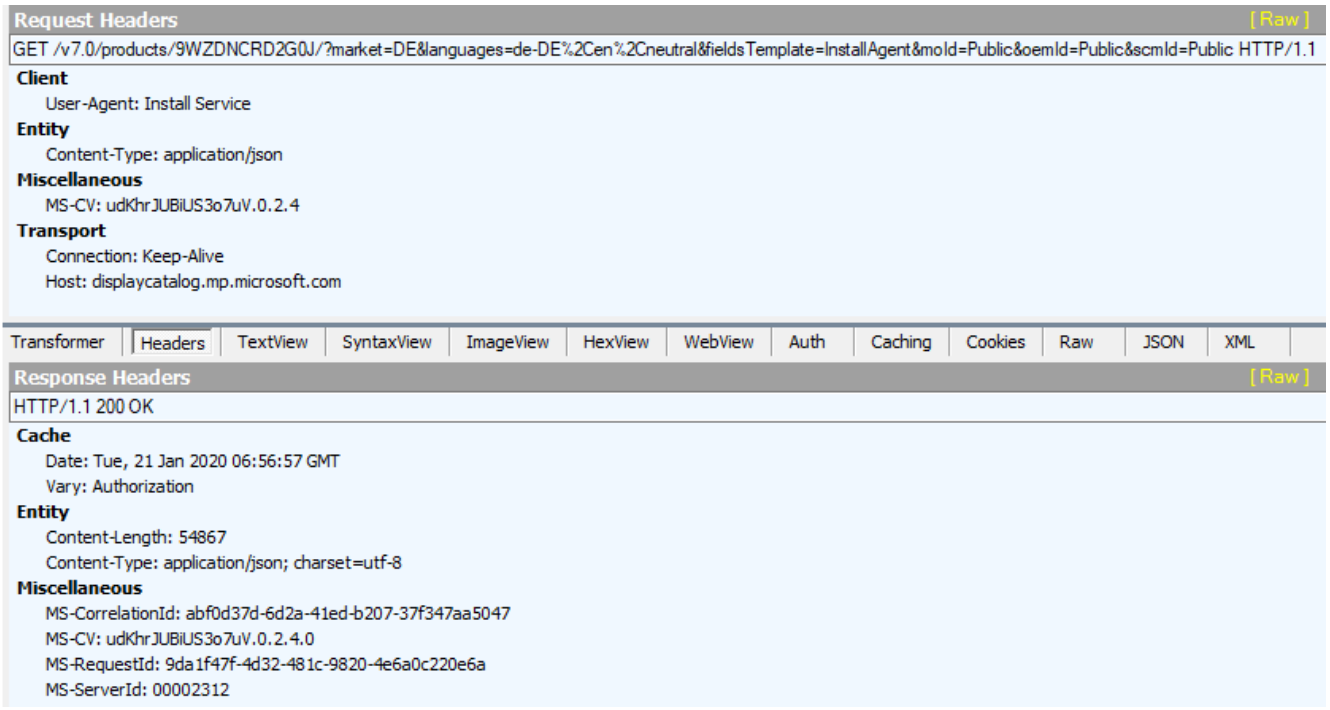
Diese Verbindung ist unerwartet, da davon ausgegangen wurde, dass sämtliche Verbindungen zum Microsoft Store durch Anwendung der Windows Restricted Traffic Limited Functionality Baseline unterbunden bzw. deaktiviert sind.

Dennoch geben die übertragenen Daten keinen Anlass, darin ein Risiko bzw. ein Offenlegen vertrauenswürdiger Informationen zu sehen.

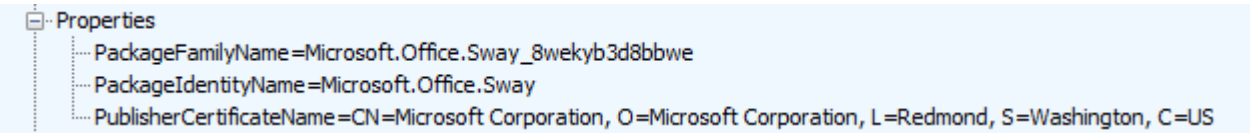
52.155.217.156 – displaycatalog.mp.microsoft.com – 126 KB / 123 Pakete

Im Zusammenhang mit der Überprüfung auf Updates konnten regelmäßig Verbindungen zur Domain „displaycatalog.mp.microsoft.com“ festgestellt werden, die die Grundlage zum vorher genannten Abruf der Bilddaten von „store-images.s-microsoft.com“ darzustellen scheint.

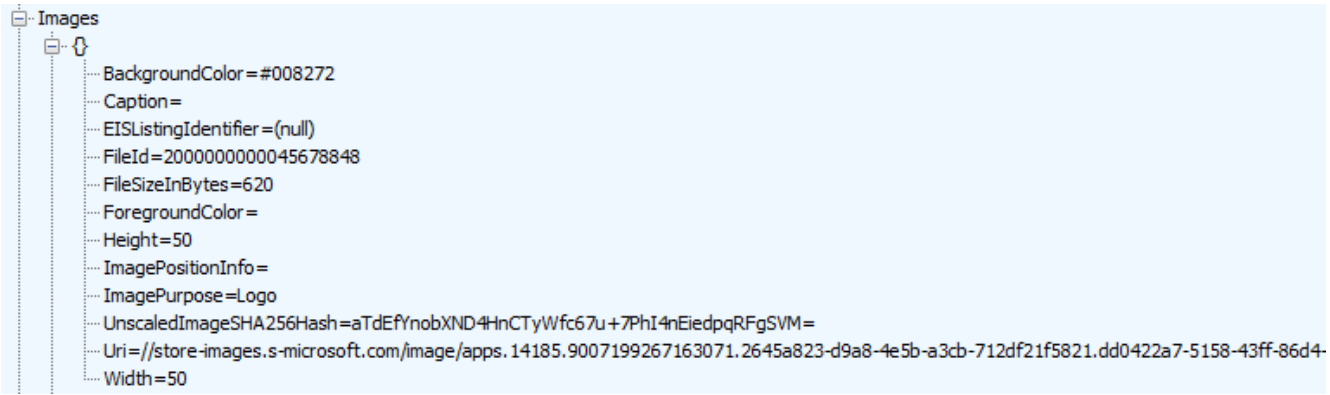
Die Kopfdaten der Verbindung stellen sich wie folgt dar:



Als Antwort erhielt der Client Informationen zu von Microsoft angebotenen Produkten; hier zu Office Sway in JSON-kodierter Form.



Dabei sind u.a. auch die Links zu den im Bildarchiv des Microsoft-Stores abgerufenen Icons zu finden.



Auch wenn diese Verbindung unerwünscht ist und i.R. der Windows Restricted Traffic Limited Functionality Baseline nicht auftreten sollte, kann auf Grund der wenigen Daten, die der Client selbst sendet und dem Inhalt der empfangenen Daten keine Gefährdung erkannt werden.

23.210.253.93 – crl.microsoft.com – 2 KB / 12 Pakete

Hierbei handelt es sich um eine Verbindung zur Certificate Revocation List (CRL) bei Microsoft, um zu prüfen, ob Zertifikate gesperrt oder widerrufen wurden. Diese Verbindung konnte im Untersuchungszeitraum nur einmal beobachtet werden, nämlich nach dem erstmaligen Start der Anwendung „procmon“. Dieses Programm ist mit einem Zertifikat signiert, um die Echtzeit nachzuweisen. In diesem Zusammenhang hat Windows offensichtlich die CRL kontaktiert.

Der nachfolgende Screenshot zeigt die Eigenschaften der Verbindung.

```
GET /pkiops/crl/MicCodSigPCA2011_2011-07-08.crl HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Microsoft-CryptoAPI/10.0
Host: www.microsoft.com

HTTP/1.1 200 OK
Content-Type: application/octet-stream
Content-Length: 813
Content-MD5: w9MsPQooRx3ylPz3q1ix5w==
Last-Modified: Mon, 13 Jan 2020 06:00:56 GMT
ETag: 0x8D797EDF4BC8643
x-ms-request-id: 46820ea4-b01e-0001-12db-c9468d000000
x-ms-version: 2009-09-19
x-ms-lease-status: unlocked
x-ms-blob-type: BlockBlob
Date: Wed, 15 Jan 2020 07:03:28 GMT
TLS_version: UNKNOWN
X-RTag: RT
X-Cache: MISS from dsl-ga.tn-ga
X-Cache-Lookup: HIT from dsl-ga.tn-ga:800
Connection: keep-alive
```

Auch hier geben die übertragenen Daten keinen Anlass, darin ein Risiko bzw. ein Offenlegen vertrauenswürdiger Informationen zu sehen.

2.22.119.98 / 2.22.119.33 / 2.22.89.31 / 2.22.94.250 / 2.19.241.220
***.deploy.static.akameitechnologies.com – 45 KB / 212 Pakete**

Bei diesen IP-Adressen und Domains handelt es sich um ein Content Delivery Network (CDN) von Akamei, das der Auslieferung und Beschleunigung von Online-Anwendungen dient. Diese Endpunkte stellen Aliase dar, den anderen, hier bereits analysierten Endpunkten entsprechen.

2.22.119.98 → crl.microsoft.com
2.22.119.33 → crl.microsoft.com

2.22.94.250 → store-images.microsoft.com
2.22.89.31 → store-images.microsoft.com
2.19.241.220 → store-images.microsoft.com

40.74.35.71 – settings-win.data.microsoft.com – 124 KB / 344 Pakete

Diese Verbindung wird vom System regelmäßig – vorrangig vor dem Überprüfen auf Windows Updates – hergestellt.

Auffällig bei dieser Verbindung war, dass sie zunächst nur auf dem Router und nicht im lokalen Proxy beobachtet werden konnte. Der per GUI / Fiddler in Windows konfigurierte Proxy-Server wurde nicht verwendet. Vielmehr war es notwendig, eine weitere Konfiguration über das Kommando „netsh winhttp set proxy“ vorzunehmen.

Anschließend konnte der Aufbau der Verbindung zwar in Fiddler beobachtet werden, die Verbindung selbst hat jedoch keinerlei Nutzdaten mehr übertragen, was auf die Verwendung von Zertifikats-Pinnung durch Microsoft hindeutet.

Weitere Versuche, an den unverschlüsselten Datenverkehr zu gelangen, wurden nicht unternommen. Zu den Inhalten dieser Verbindung kann daher keine Aussage getroffen werden.

Nach Angaben[2] von Microsoft würden Apps diesen Endpunkte verwenden, um ihre Konfiguration dynamisch zu aktualisieren. So seien u.a. die Windows-Komponente „Benutzererfahrungen und Telemetrie im verbundenen Modus“ und das „Windows-Insider-Programm“ betroffen.

Auch im BSI-Projekt „SiSyPHuS“[3] ist diese Domain mehrfach im Zusammenhang mit der dynamischen Konfiguration der Windows-Telemetrie genannt. Den Feststellungen zur Folge könnte Microsoft darüber das Verhalten des Telemetriedienstes anpassen, Art und Umfang der Datenerhebung konfigurieren oder Kommandos zur Anreicherung der Daten ausführen, ohne

2 https://docs.microsoft.com/de-de/windows/privacy/manage-windows-1803-endpoints
3 https://bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Workpackage4_Telemetry.pdf

dass der Nutzer dem Zustimmen muss oder das kontrollieren kann. Vor diesem Hintergrund sind Verbindungen zu diesem Endpunkt zumindest als bedenklich einzustufen.

Auf Nachfrage ist im Gespräch mit Microsoft am 10./11.12.2019 in Ansbach mündlich bestätigt worden, dass die in dieser Verbindungen übertragenen Daten nach Anwendung der Windows Restricted Traffic Limited Functionality Baseline (und damit des Telemetrielevels „Security“) von der Windows-Telemetriekomponente nicht weiter verwendet werden würden und das Abrufen allein technische Ursachen in der Implementierung habe.

Was diese Datenverbindung tatsächlich überträgt und ob damit sicherheits- oder datenschutzrelevante Konfigurationen am System vorgenommen werden kann, mangels Einblick in den Datenverkehr, nicht bewertet werden.

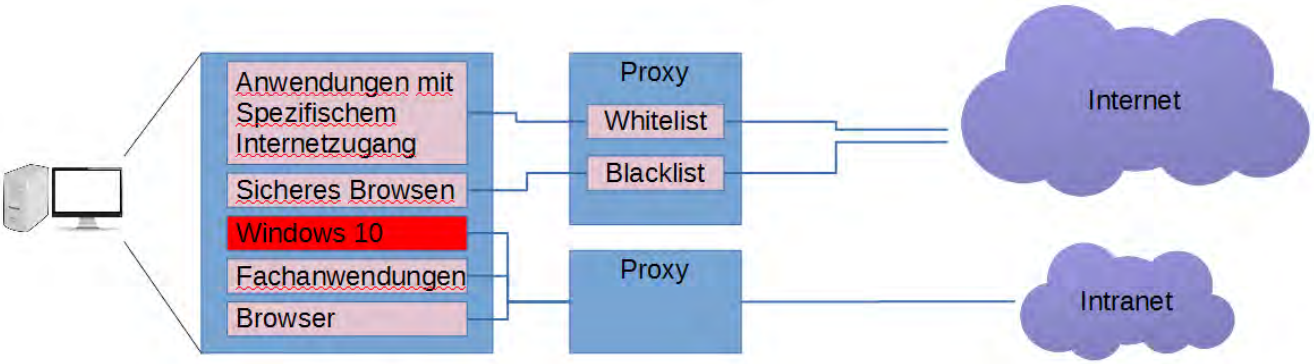
Bewertung

Im Rahmen dieser Untersuchung haben sich keine Hinweise ergeben, dass Windows 10 Enterprise mit der Konfiguration „Windows Restricted Traffic Limited Functionality Baseline“ Daten an Microsoft übertragen hat, die aus h.S. ein Risiko oder das Offenlegen vertrauenswürdiger Informationen darstellen. Insbesondere konnte keine Übertragung von Telemetriedaten an Microsoft beobachtet werden.

Dabei ist jedoch zu beachten, dass die Verbindungen zu „settings-win.data.microsoft.com“ nicht im Klartext analysiert werden konnte und somit die Möglichkeit besteht, dass Microsoft über diesen Kanal Daten exfiltriert oder in unerwünschter Weise Einfluss auf das System nimmt.

Darüber hinaus stellt diese Untersuchung nur eine Momentaufnahme für eine explizite Version von Windows 10 Enterprise in diesem Patchstand und einer speziellen Konfiguration dar. Durch weitere Updates und Änderungen am System durch Microsoft oder Konfigurationen des Nutzer kann sich dieses Verhalten verändern. Eine regelmäßige Aktualisierung und Prüfung der Untersuchungsergebnisse ist daher erforderlich.

Trotz der gewonnenen Erkenntnisse wird die Empfehlung des BSI, Windows 10 im Rahmen einer Netztrennung zu betreiben aufrecht erhalten. Grund dafür ist einerseits die Möglichkeit, dass sich das festgestellte Systemverhalten jederzeit durch Updates oder Konfigurationsänderungen des Herstellers ändern kann. Insbesondere die Nichtbewertbarkeit der bei der dynamischen Konfiguration der Telemetrie beteiligten Verbindung zu „settings-win.data.microsoft.com“ zeigt, dass keine belastbare, abschließende Aussage möglich ist und weitere Datenkommunikation auftreten kann. Andererseits wird mit der Netztrennung eines Systems dem Grundsatz „Defence in depth“ Rechnung getragen. So können nicht nur möglicherweise auftretende, unerwünschte Datenübertragungen von Anwendungen auf dem System verhindert, sondern auch wirkungsvoll die Exfiltration von Daten z.B. durch Malware vorgebeugt werden.



Dennoch bewirkt die Anwendung der Windows Restricted Traffic Limited Functionality Baseline für Windows 10 Enterprise einen deutlich verminderten Umfang an Daten, die in das Internet übertragen werden. Eine ähnliche Konfigurationsmöglichkeit auch für Windows 10 Pro/Home wäre wünschenswert.

Dabei ist jedoch – entsprechend der Benennung der Richtlinie – ein verminderter Funktionsumfang zu verzeichnen. So konnten beispielsweise im Rahmen der Untersuchung keine Anwendungen mehr gestartet werden, die Bezüge zum Windows Store haben. Die Auswirkungen auf die Praxistauglichkeit dieser Richtlinie werden auf Grund der Testergebnisse jedoch als eher gering bewertet.

Im Auftrag

Dr. Wippig