Bundesamt
für Sicherheit in der
Informationstechnik

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:

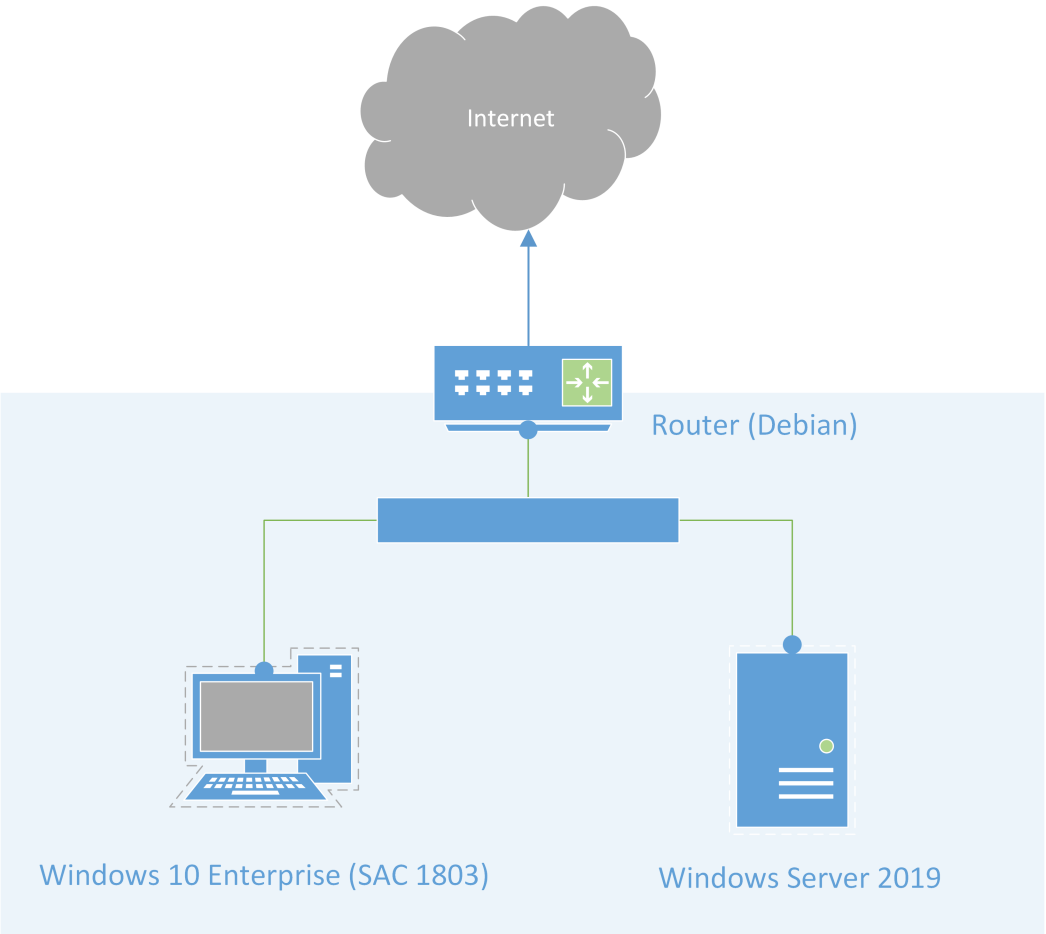
- Router (Debian 10)
  - Einsatz als Router, DHCP-Server, DNS-Server
  - Verwendung von tcpdump zur Aufzeichnung des Netzwerkverkehrs
  - Verwendung zur live-Darstellung der Datenverbindungen

- 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

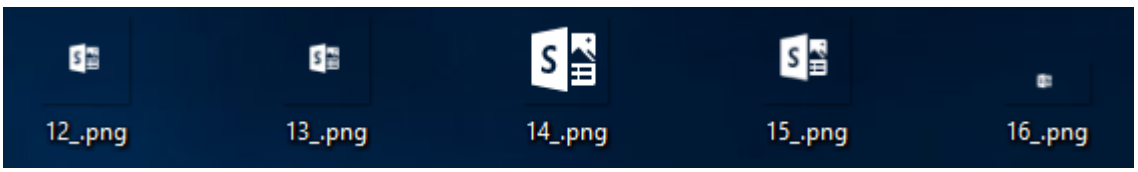
Diese IP wurde jeweils beim Starten der Anwendung „Fiddler2“ abgerufen und dient der Überprüfung und dem Bezug von Aktualisierungen. Es handelt sich um eine Verbindung, die nicht Microsoft Windows zuzurechnen ist und kann daher bei dieser Untersuchung unbeachtet bleiben.

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

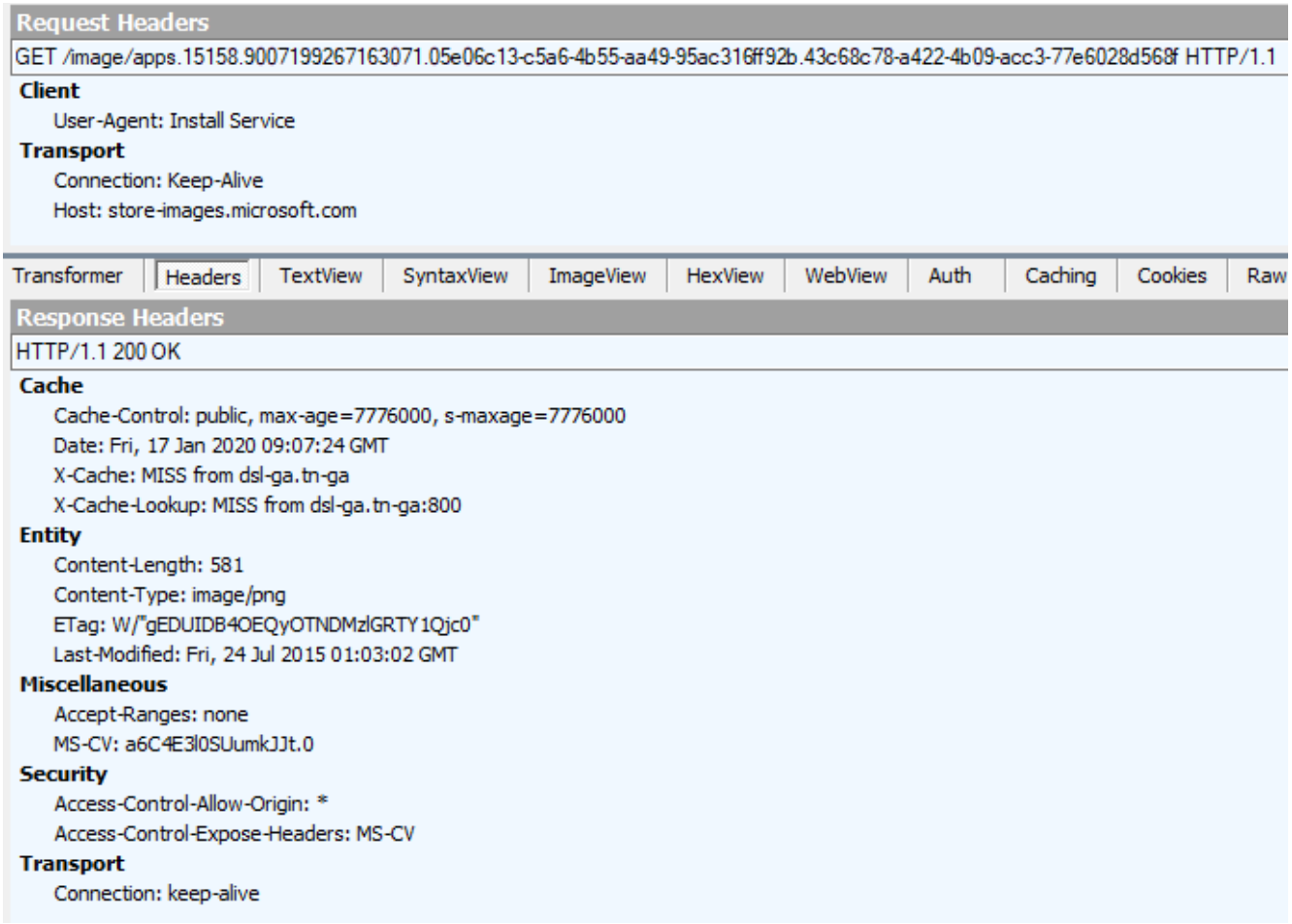
Über den gesamten Zeitraum sind Verbindungen zum Bildarchiv des Microsoft Stores zu verzeichnen.

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.



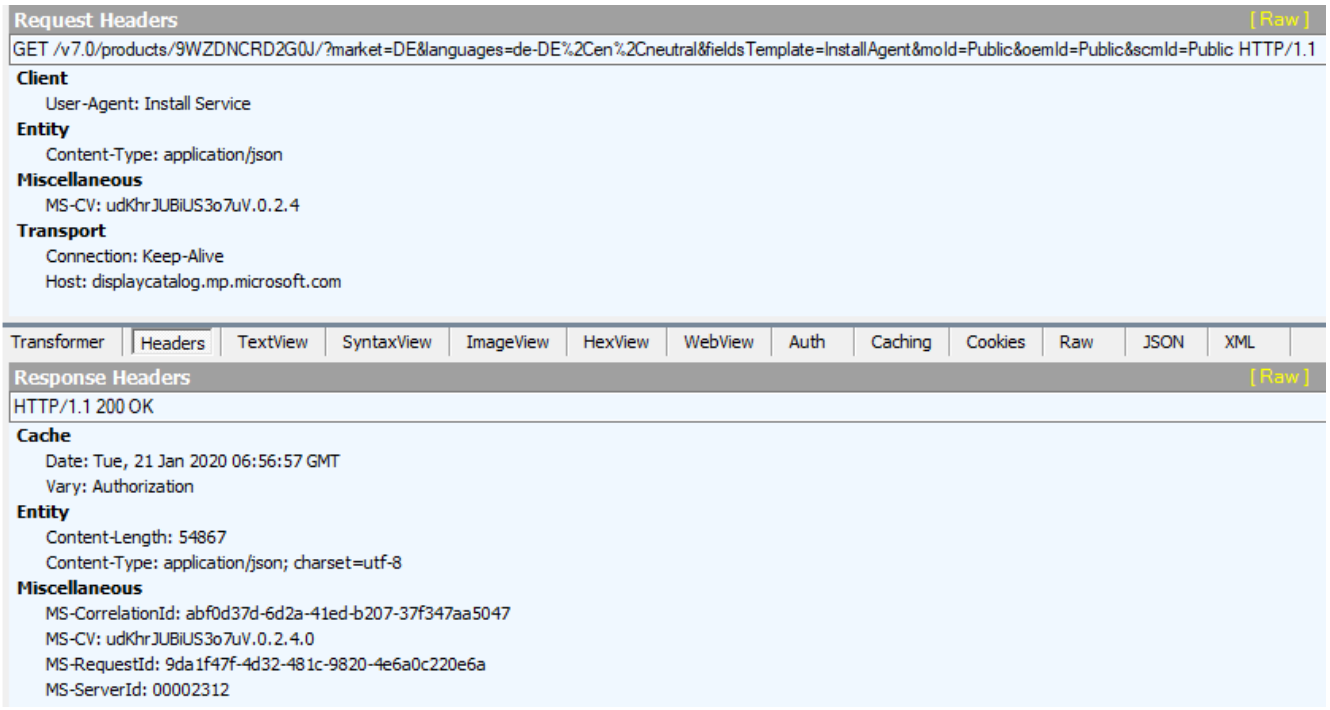
Diese Verbindung ist unerwartet, da davon ausgegangen wurde, dass sämtliche Verbindungen zum Microsoft Store durch Anwendung der Windows Restricted Traffic Limited Functionality Baseline unterbunden bzw. deaktiviert sind.

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

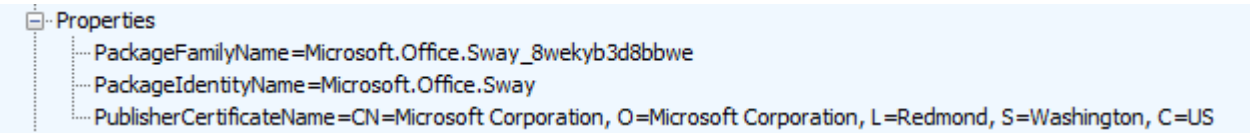
52.155.217.156 – displaycatalog.mp.microsoft.com – 126 KB / 123 Pakete

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.

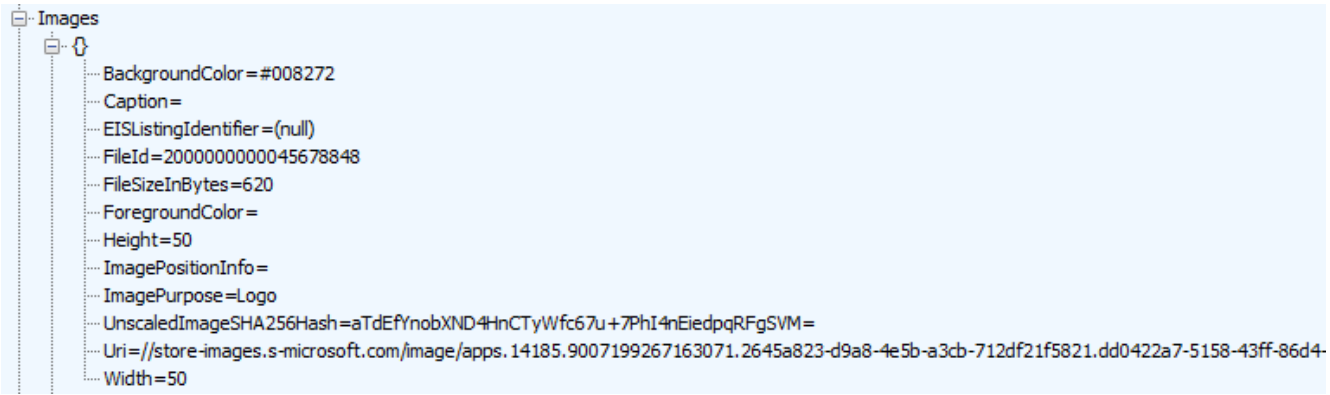
Die Kopfdaten der Verbindung stellen sich wie folgt dar:



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.

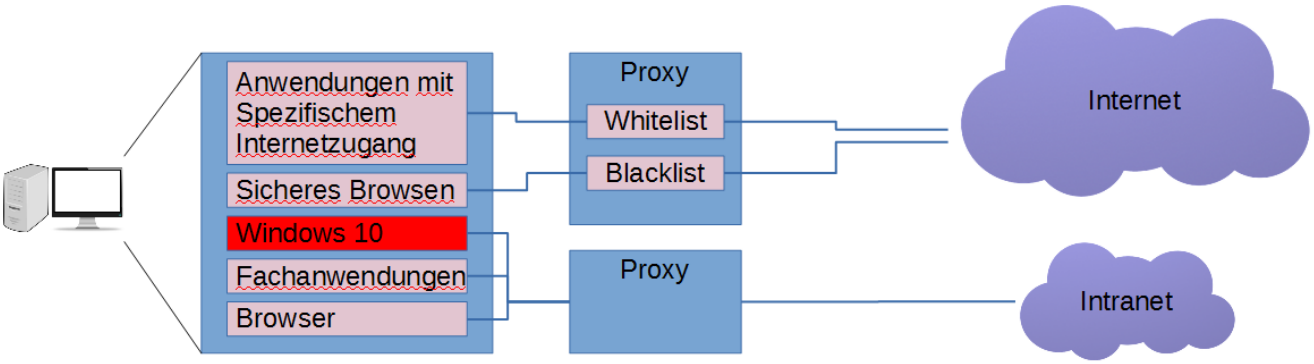
Bewertung

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