Microsoft Windows Telemetrie-Überwachung ab Windows 7
==========

Für das Versenden, Sammeln etc. persönlichen Daten sind die Telemetrie-Elemente unter Windows verantwortlich. Microsoft nennt das auch **Benutzererfahrung und Telemetrie.** **Und: die Überwachung ist in Windows fest implementiert, so dass eine Abschaltung nur mit Kenntnissen des Betriebssystems möglich ist.**

Telemetrie-Internet-Adressen und hosts

Unter Nutzung der Admin-Rechte kann die Datei C:\Windows\system32\drivers\etc\hosts editiert werden, um zu sperrende Internet-Adressen zu hinterlegen. Jeder Internet-Adresse wird die IP 0.0.0.0 zugeordnet. Geht bzw. ist Windows online und will die IP ansprechen, so wird die IP 0.0.0.0 benutzt und die ist keine Online-IP (bitte nicht "localhost" oder 127.0.0.0verwenden).

Nachfolgende Liste ist nicht vollständig, das Microsoft zig Domains nutzt. Außerdem wird die Überwachung per Windows Updates implementiert oder manipuliert. Alles andere als für den Nutzer transparent.

0.0.0.0 a-0001.a-msedge.net
0.0.0.0 a-0002.a-msedge.net
0.0.0.0 a-0003.a-msedge.net
0.0.0.0 a-0004.a-msedge.net
0.0.0.0 a-0005.a-msedge.net
0.0.0.0 a-0006.a-msedge.net
0.0.0.0 a-0007.a-msedge.net
0.0.0.0 a-0008.a-msedge.net
0.0.0.0 a-0009.a-msedge.net
0.0.0.0 a-msedge.net
0.0.0.0 a.ads1.msn.com
0.0.0.0 a.ads2.msads.net
0.0.0.0 a.ads2.msn.com
0.0.0.0 a.rad.msn.com
0.0.0.0 ac3.msn.com
0.0.0.0 ad.doubleclick.net
0.0.0.0 adnexus.net
0.0.0.0 adnxs.com
0.0.0.0 ads.msn.com
0.0.0.0 ads1.msads.net
0.0.0.0 ads1.msn.com
0.0.0.0 aidps.atdmt.com
0.0.0.0 aka-cdn-ns.adtech.de
0.0.0.0 apps.skype.com
0.0.0.0 az361816.vo.msecnd.net
0.0.0.0 az512334.vo.msecnd.net
0.0.0.0 b.ads1.msn.com
0.0.0.0 b.ads2.msads.net
0.0.0.0 b.rad.msn.com
0.0.0.0 bs.serving-sys.com
0.0.0.0 c.atdmt.com
0.0.0.0 c.msn.com
0.0.0.0 cdn.atdmt.com
0.0.0.0 cds26.ams9.msecn.net
0.0.0.0 choice.microsoft.com
0.0.0.0 choice.microsoft.com.nstac.net
0.0.0.0 compatexchange.cloudapp.net
0.0.0.0 corp.sts.microsoft.com
0.0.0.0 corpext.msitadfs.glbdns2.microsoft.com
0.0.0.0 cs1.wpc.v0cdn.net
0.0.0.0 db3aqu.atdmt.com
0.0.0.0 df.telemetry.microsoft.com
0.0.0.0 diagnostics.support.microsoft.com
0.0.0.0 ec.atdmt.com
0.0.0.0 fe2.update.microsoft.com.akadns.net

0.0.0.0 feedback.microsoft-hohm.com
0.0.0.0 feedback.search.microsoft.com
0.0.0.0 feedback.windows.com
0.0.0.0 flex.msn.com
0.0.0.0 g.msn.com
0.0.0.0 h1.msn.com
0.0.0.0 i1.services.social.microsoft.com
0.0.0.0 i1.services.social.microsoft.com.nsatc.net
0.0.0.0 lb1.www.ms.akadns.net
0.0.0.0 live.rads.msn.com
0.0.0.0 m.adnxs.com
0.0.0.0 m.hotmail.com
0.0.0.0 msedge.net
0.0.0.0 msftncsi.com
0.0.0.0 msnbot-65-55-108-23.search.msn.com
0.0.0.0 msntest.serving-sys.com
0.0.0.0 oca.telemetry.microsoft.com
0.0.0.0 oca.telemetry.microsoft.com.nsatc.net
0.0.0.0 pre.footprintpredict.com
0.0.0.0 preview.msn.com
0.0.0.0 pricelist.skype.com
0.0.0.0 rad.live.com
0.0.0.0 rad.msn.com
0.0.0.0 redir.metaservices.microsoft.com
0.0.0.0 reports.wes.df.telemetry.microsoft.com
0.0.0.0 s.gateway.messenger.live.com
0.0.0.0 s0.2mdn.net
0.0.0.0 schemas.microsoft.akadns.net
0.0.0.0 secure.adnxs.com
0.0.0.0 secure.flashtalking.com
0.0.0.0 services.wes.df.telemetry.microsoft.com
0.0.0.0 settings-sandbox.data.microsoft.com
0.0.0.0 settings-win.data.microsoft.com
0.0.0.0 sls.update.microsoft.com.akadns.net
0.0.0.0 sqm.df.telemetry.microsoft.com
0.0.0.0 sqm.telemetry.microsoft.com
0.0.0.0 sqm.telemetry.microsoft.com.nsatc.net
0.0.0.0 static.2mdn.net
0.0.0.0 statsfe1.ws.microsoft.com
0.0.0.0 statsfe2.update.microsoft.com.akadns.net
0.0.0.0 statsfe2.ws.microsoft.com
0.0.0.0 survey.watson.microsoft.com
0.0.0.0 telecommand.telemetry.microsoft.com
0.0.0.0 telecommand.telemetry.microsoft.com.nsatc.net
0.0.0.0 telemetry.appex.bing.net
0.0.0.0 telemetry.microsoft.com
0.0.0.0 telemetry.urs.microsoft.com
0.0.0.0 view.atdmt.com
0.0.0.0 vortex-bn2.metron.live.com.nsatc.net
0.0.0.0 vortex-cy2.metron.live.com.nsatc.net
0.0.0.0 vortex-sandbox.data.microsoft.com
0.0.0.0 vortex-win.data.microsoft.com
0.0.0.0 vortex.data.microsoft.com
0.0.0.0 watson.live.com
0.0.0.0 watson.microsoft.com
0.0.0.0 watson.ppe.telemetry.microsoft.com
0.0.0.0 watson.telemetry.microsoft.com
0.0.0.0 watson.telemetry.microsoft.com.nsatc.net
0.0.0.0 wes.df.telemetry.microsoft.com
0.0.0.0 www.msftncsi.com

Wer auch blockieren will:

0.0.0.0 time.windows.com
0.0.0.0 teredo.ipv6.microsoft.com
0.0.0.0 nexus.officeapps.live.com
0.0.0.0 watson.microsoft.com

Benutzer einer Fritzbox haben die Möglichkeit, die schon uralte Software FritzDSL! zu installieren, denn die zeigt Programme an, die online gehen wollen. Im Log-Bereich sind die Programme mit Internetadressen sichtbar. Man kann Programme, die online gehen wollen, auch daran hindern. Was FritzDSL! nicht kann: Selektive Sperrung. Bsp.: Will man mit einem Browser online gehen, dann führt Windows die Aktivierung des Browsers aus. JEDES normale Programm, das online gehen will, wird von Windows aktiviert. Browser sollen ja ins Internet. Aber wenn z.B. ein Videoschnittprogramm mit Start online geht, ohne dass ersichtlich ist, wozu, dann kann man das NICHT selektiv verhindern. Man müsste nämlich Windows den Internet-Zugang sperren - und damit auch Browser lahmlegen. FritzDSL! ist unprofessionell, aber wegen der Log nutzbar. Dort kann man z.B. lesen, wenn ein windows-eigener Systemdienst online geht, z.B. svchost.exe. Dieses Programm existiert in zig Instanzen und bedient u.a. Instanzen der Windows-Dienste, z.B. die der ... na ? .... klar, Überwachung ! Wenn also svchost.exe einen Dienst online gehen lässt, dann kann man mit FritzDSL! nur generell svchost.exe sperren, also alle Dienste lahm legen. Oder auch z.B. das Windows Update. Wie auch immer: Es ist erbärmlich, was dem Nutzer so zugemutet wird.

Nachfolgend wird gezeigt, wie man den Zugriff auf
www.msftncsi.com (bzw. der IP-Adresse "131.107.255.255")
bzw. ipv6.msftncsi.com für aktive IPv6-Treiber von Windows
unterbindet.
Diese Internet-Adressen sollen angeblich dafür dienen, dass anstelle eine Ping nun Daten die Existenz der Zugriffsfähigkeit auf das Internet erkannt wird - Hirnrissig, da ja Ping ausreichen würde. Microsoft will aber, immer wenn die Verbindung zum Internet zugeschaltet wird, wissen, wer das wann tut. Das nennt Microsoft auch Microsoft NCSI = Network Connectivity Status Indicator.
Die Abschaltung dieser Überwachung erfolgt wie folgt:
Die Registry ist per Registry-Editor bearbeitbar ("**Win** + **R**", "**regedit**" eingeben).
Registry-Pfad HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NlaSvc\Parameters\Internet
dort doppelklicken auf den Schlüssel "EnableActiveProbing" bzw. erstellen.
dann neuen DWORD-Wert mit Name "EnableActiveProbing" und Wert dezimal 0
(0 für deaktiviert, 1 für aktiviert).
Registry schließen.
dann Computer neu starten.

Das Märchen der Verbesserung Benutzerfreundlichkeit der Gesamtanwendung

Microsoft erklärt dem Windows-Nutzer folgendes:

"Diagnose- und Telemetrie Service erfasst Diagnoseinformationen Probleme unter Windows Windows Customer Experience Improvement Program (CEIP) teilnehmen. CEIP-Berichte enthalten keine Kontaktinformationen wie Name, Adresse oder Telefonnummer. Dies bedeutet, dass CEIP Sie nicht auffordern wird , an Umfragen teilzunehmen oder Junk-Mails zu lesen, und Sie werden auf keinen Fall auf irgend eine Art kontaktiert.

Windows-Benutzer können ändern ihre Windows CEIP-Teilnahme auf der Seite " Einstellungen für das Programm zur Verbesserung der Benutzerfreundlichkeit " ändern, indem Sie die Systemsteuerung öffnen und Wartungscenter auswählen - Wartungscentereinstellungen ändern - Einstellungen für das Programm zur Verbesserung der Benutzerfreundlichkeit auswählen.

Programme mit eigener Diagnose und Telemetrie, wie Application Insights, können von diesem Dienst abhänging sein, um ihre Telemetrie an Microsoft zu übertragen. Anwendungsbenutzer können über die jeweiligen Einstellungen der Anwendungen an solchen Programmen teilnehmen.

Dieses Update verwendet SSL (TCP-Port 443) für das Herunterladen der Manifeste und das Hochladen der Telemetriedaten an Microsoft, wobei die folgenden DNS-Endpunkte verwendet werden:

vortex-win.data.microsoft.com
settings-win.data.microsoft.com

Dieses Update enthält die folgenden zwei Manifeste, die vom Dienst verwendet werden, wenn der Benutzer Windows CEIP-Programm oder Telemetrie-Programme, die speziell von einer Anwendung wie verwaltet werden, die Anwendung Einblicke beteiligt.

telemetry.ASM-WindowsDefault.json
utc.app.json"

Na, alles verstanden ? Nö ?? Na hier die ultimative Antwort:
Die per Systemsteuerung mögliche Abschaltung der Verbesserung der Benutzerfreundlichkeit funktioniert NICHT.

Jetzt ist alles klar !

Telemetrie-Dienste (ev. nicht Win 7)

Die windows-eigenen Telemetriedienste organisieren die Überwachung.

Dienst "**DiagTrack**" (Service für Benutzererfahrung und Telemetrie im verbundenen Modus)
Dienst "**dmwappushservice**" (Service für dmwappushsvc / WAP Push-Nachrichtenroutingdienst).

Dienste sind in der Dienste-Verwaltung ("**Win + R**" dann "**services.msc**" eingeben) sichtbar,
Dienste lassen sich dort konfigurieren. Die Beschreibung der Dienste kann ellenlang sein.
Der Dienstname zugleich so sinnlos wie "**dmwappushservice**".

In der Spalte "Name" ist der Dienst "**Benutzererfahrung und Telemetrie...**" zu markieren (Dienst ist ev. nicht bei Win 7 vorhanden). Dann rechte Maus - Eigenschaften: Bitte Beenden (warten bis beendet) und dann deaktivieren.

Analog dazu den Dienst "**DiagTrack**" beeenden und deaktivieren.
Analog dazu den Dienst "**dmwappushsvc**" beeenden und deaktivieren.
Analog dazu den Dienst "**Remoteregistrierung**" (Dienstname: **RemoteRegistry**) beenden und deaktivieren (ist eventuell bereits beendet ist und deaktiviert).

Telemetrie-Aufgaben mit Zeitpunktvorgabe

Microsoft lässt auch mittels Timer überwachen: **Geplante Aufgaben: CEIP (Consumer Experience Improvement Program).**

Natürlich muss zum Zeitpunkt des Aufgabenstartes das entsprechende Programm oder der Dienst aktivierbar sein oder bereits aktiv sein.

Nachfolgend wird erklärt, wie die CEIP-Aufgaben aus dem System entfernt werden.

Aufgaben sind in der Aufgabenplanung ("**Win + R**", dann "**taskschd.msc**" eingeben).

Links im Baum folgenden Pfad öffnen
Aufgabenplanungsbibliothek - Microsoft - Windows - Application Experience

Die Aufgaben "**Microsoft Compatibility Appraiser**" ,"**ProgramDataUpdater**" und **"AitAgent"** deaktivieren oder gleich löschen.

Links im Baum folgenden Pfad öffnen
Aufgabenplanungsbibliothek - Microsoft - Windows - Autochk

Die Aufgabe **"Proxy"** deaktivieren oder gleich löschen.

Links im Baum folgenden Pfad öffnen (eventuell nicht in Win 7 vorhanden)
Aufgabenplanungsbibliothek - Microsoft - Windows - Application DiskDiagnostic

Die Aufgabe **"Microsoft-Windows-DiskDiagnosticDataCollector"** deaktivieren oder gleich löschen.

Links im Baum folgenden Pfad öffnen
Aufgabenplanungsbibliothek - Microsoft - Windows - Customer Experience Improvement Program

Alle Aufgabe deaktivieren oder gleich löschen "**Consolidator**", "**KernlCeipTask**", "**USBCeip**".

Telemetrie-Registry-Einträge

Die Registry ist per Registry-Editor bearbeitbar ("**Win + R**", "**regedit**" eingeben).

Nach der Bearbeitung der Registry diese schließen und Computer neu starten.

Im Baum links sind die Kategorien der Registry (**(Hives)**, deren Element u.a. Schlüssel und deren Werte sind. Auch Schlüsselverschachtelung. Bestimmte Bereich hält Windows als nicht-editierbar unter laufenden Windows. Ansonsten tummeln sich in der Registry natürlich auch Einträge von Trojanern etc.. Die Registry ist ein Einfallstor für Sinn und Unsinn.

Im Baum den Pfad öffnen
"**HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows**"

Dort das Element "**DataCollection**" suchen: Wenn vorhanden dann Maus auf den Eintrag setzen, dann rechte Maus - löschen.

Maus auf den Eintrag Windows, dann rechte Maus - Neu - Schlüssel
Als Name des Schlüssel **"DataCollection"** eingeben**.**

Maus auf **DataCollection**, dann rechte Maus - Neu - **DWORD-Wert (32-Bit)**
Als Name "**AllowTelemetry**" verwenden

Maus auf **AllowTelemetry**, dann rechte Maus - ändern
Als Binärwert 0 eintragen. Damit wird die Telemetry verboten. (1 für erlauben).

Im Baum den Pfad öffnen
"**HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion"**

Neuen Schlüssel erstellen: **AdvertisingInfo**
Neuen DWORD-Wert mit Name **Enabled und Wert 0**

Im Baum den Pfad öffnen **(ab Windows 10)**
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\DeliveryOptimization\Config

neuen DWORD-Wert erstellen mit Name **DODownloadMode und Wert 0**

Diese Einstellung lässt Windows -Updates direkt vom Microsoft einspielen, ohne das Point-to-Point-Prinzip (P2P): Die Daten werden nicht über fremde PC empfangen. Microsoft sammelt nämlich die IP der fremden PC mit ein. Außerdem könnten fremde PC die Daten manipulieren.

Für JEDES Benutzerkonto (am Konto anmelden und dann Nachfolgendes ausführen)

Im Baum den Pfad öffnen **(falls verfügbar)**
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\DeliveryOptimization

neuen DWORD-Wert erstellen mit Namen "**SystemSettingsDownloadMode**" mit Wert 3

Im Baum den Pfad öffnen
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows

neuen Schlüssel erstellen "**Windows Search**"
dort neue DWORD-Werte erstellen
DisableWebSearch mit Wert 1
ConnectedSearchUseWeb mit Wert 0
ConnectedSearchUseWebOverMeteredConnections mit Wert 0
AllowCortana mit Wert 0

Nachfolgend wird gezeigt, wie man den Zugriff auf
www.msftncsi.com (bzw. der IP-Adresse "131.107.255.255")
bzw. ipv6.msftncsi.com für aktive IPv6-Treiber von Windows
unterbindet.

Diese Internet-Adressen sollen angeblich dafür dienen, dass anstelle eine Ping nun Daten die Existenz der Zugriffsfähigkeit auf das Internet erkannt wird - Hirnrissig, da ja Ping ausreichen würde. Microsoft will aber, immer wenn die Verbindung zum Internet zugeschaltet wird, wissen, wer das wann tut. Das nennt Microsoft auch Microsoft NCSI = Network Connectivity Status Indicator.
Die Abschaltung dieser Überwachung erfolgt wie folgt:

Registry-Pfad HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NlaSvc\Parameters\Internet
dort doppelklicken auf den Schlüssel "EnableActiveProbing" bzw. erstellen.
dann neuen DWORD-Wert mit Name "EnableActiveProbing" und Wert dezimal 0
(0 für deaktiviert, 1 für aktiviert).
Registry schließen.
dann Computer neu starten.

Telemetrie-Gruppenregeln

Windows kann die **Gruppenregel (Group Policy)** verwenden. In den Home-Versionen von Windows fehlt eventuell diese Möglichkeit.

CEIP (Consumer Experience Improvement Program) Gruppenregel (Group Policy)

Pfad: **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft**
Erstelle dort einen neuen Schlüssel: **SQMClient**
Erstelle dort einen neuen Schlüssel: **Windows**
Erstelle dort einen neuen DWORD-Wert: **Name CEIPEnable mit Wert 0**

AIT (Application Impact Telemetry) & Steps Recorder - Gruppenregel (Group Policy)

Pfad: **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows**
Erstelle dort einen neuen Schlüssel: **AppCompat**
Erstelle dort 2 neue DWORD-Werte: "**AITEnable**" und "**DisableUAR**".
AITEnable muss "**0**" sein, DisableUAR muss auf "**1**" gesetzt werden.

WiFi Sense (HotSpot Verteilung) - Gruppenregel (Group Policy)

Pfad: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\default\Wifi**
In allen Schlüsseln muss der DWORD Wert "**value**" auf "**1**" sein.
Nur "WLANScanMode" auf "**0**" setzen.

Cortana - Gruppenregel (Group Policy)
Pfad: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\default\Experience\AllowCortana**
neuen DWORD-Wert erstellen mit Name **value und Wert 1**

Onedrive-Dienste und Gruppenregel (Group Policy)

nur wenn OnDrive UND Windows NICHT benutzt werden sollen:

Erst per **services.msc** die Dienste "**Synchronisierungshost**" (Dienstname: OneSyncSvc) und "**Host_Session1**" (Dienstname: OneSyncSvc_Session1) beenden und dann deaktivieren.

Falls die Dienste nicht existieren, ist OneDrive nicht installiert. Dann nachfolgende Registry-Änderung nicht ausführen.

Dann Pfad: **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows**
neuer Schlüssel **OneDrive**
neuer DWORD-Wert mit Name **DisableFileSyncNGSC und Wert** "**1**".

Registry schließen, dann Computer neu starten.

Telemetrie Office v15 (2013) & Office v16 (2016)

Erst Aufgaben deaktivieren: Wenn Aufgaben nicht verfügbar, dann ist Telemetrie nicht aktiv.

Per "**taskschd.msc**" unter "**Microsoft - Office**" die Aufgaben
"**OfficeTelemetryAgentFallBack**"
"**OfficeTelemetryAgentLogOn**"
entfernen
Im Namen steht die Office-Version 2013 bzw. 2016

Dann Registry ändern
HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\office\15.0\osm
bzw. **HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\office\16.0\osm**

neue DWORD-Werte erstellen
enablelogging mit Wert 0
enablefileobfuscation mit Wert 0
enableupload mit Wert 0

Registry schließen, dann Computer neu starten.

Telemetrie-Auto-Key-Logger

Mir Admin-Rechten die Datei

C:\ProgramData\Microsoft\Diagnosis\ETLLogs\AutoLogger\AutoLogger-Diagtrack-Listener.etl

per notepad.exe editieren: Inhalt löschen, dann die Zeichenfolge "" eingeben (2 Gänsefüßchen).
und Datei speichern.

dann rechte Maus und Dateieigenschaften: Schreibschutz abhaken.