Der Hamburgische Beauftragte für
Datenschutz und Informationsfreiheit

Az. 30.02-32 19.12.2019

T1

Überprüfung der Dataport BASIS Konfiguration von Windows 10 Enterprise Version 1809 für den Einsatz beim HmbBfDI

Im Rahmen der Windows 10-Einführung für die gesamte FHH durch Dataport hat sich der HmbBfDI bereits im August 2018 mit der Frage auseinandergesetzt, ob Windows 10 Enterprise für den behördlichen Einsatz tauglich ist und dabei insoweit datenschutzgerecht betrieben werden kann, als dass keinerlei Tracking durch Microsoft mehr stattfindet, mit dem ein einzelner Nutzer oder ein bestimmtes Gerät identifizierbar wird. Dieser Test wird aufgrund von aktualisierten Betriebssystem-Versionen nun erneut durchgeführt.

Der HmbBfDI vertritt die Position, dass ein Betriebssystem als Plattform für die Arbeit mit Computern keinerlei für den Nutzer nachteilige Funktionen aufweisen darf, die nicht erforderlich sind und für die keine Rechtsgrundlage besteht. Hierbei stehen insbesondere die Funktionen im Fokus, die für den Betrieb des Gerätes nicht notwendig sind, wie Nutzungstelemetrie, Benutzertracking, Werbung oder die erzwungene Bereitstellung unerwünschter Software.

Hiervon ausgenommen sind erforderliche Funktionen, die die Sicherheit gewährleisten wie die regelmäßige Prüfung auf und Installation von Systemupdates oder die Verfolgung des Netzwerkverkehrs durch eine lokal operierende Firewall und die Systemprotokollierung.

Windows 10 steht seit seiner Einführung in der Kritik von Datenschützern und IT-Fachleuten, da es neben einer Reihe von Software, die unabhängig vom Nutzungsbedarf installiert wird und deren Entfernung zum Teil unmöglich ist, auch umfangreiche Telemetriedaten an Microsoft sendet und dabei auf Pseudonyme setzt, um die Installation oder den Nutzer wiedererkennen zu können. Diese Funktionalität steht einem datenschutzgerechten Einsatz im Weg und ist daher regelmäßig Gegenstand von Untersuchungen.

Diese Untersuchung beschäftigt sich mit der BASIS Konfiguration, die von Dataport für die öffentliche

www.datenschutz-hamburg.de

E-Mail: mailbox@datenschutz.hamburg.de
Klosterwall 6 - D-20095 Hamburg - Tel.: 040 - 4 28 54 - 40 40 - Fax: 040 - 4 28 54 – 40 00

Verwaltung der Freien und Hansestadt Hamburg betrieben wird. Im Kern steht die Frage, ob die BASIS-Konfiguration einen datenschutzgerechten Betrieb für den HmbBfDI und die FHH ermöglicht.

Zielsetzung

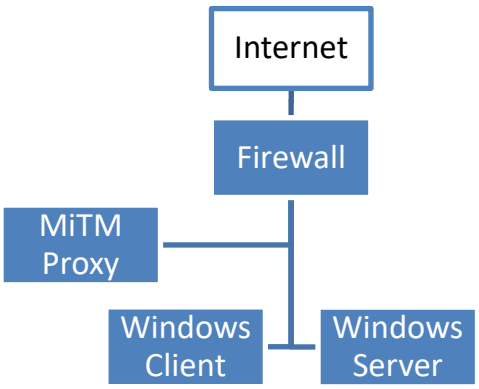
Ziel dieses Projekts ist weiterhin die Beantwortung der Frage, ob Dataport BASIS PC mit Windows 10 Enterprise datenschutzgerecht betrieben werden kann und wie datenschutzfreundlich dieser konfiguriert ist. Da „Datenschutzfreundlichkeit“ durch keine einheitliche Metrik bemessen ist, wird versucht, die folgenden Unterfragen zu beantworten:

- Ist sämtliche nicht erforderliche Software per Default deaktiviert
- Konnte alle unerwünscht installierte Software deinstalliert oder deaktiviert werden?
- Ist die Telemetriekommunikation von Windows 10 an Microsoft per Default deaktiviert?
- Inwieweit lässt sich die Telemetriekommunikation von Windows 10 an Microsoft minimieren oder vollständig deaktivieren?
- Kann bei dem eventuell verbleibenden Verkehr sichergestellt werden, dass keinerlei Tracking stattfindet?

Um diese Fragen zu beantworten wurde mit Unterstützung von Dataport ein Laborsetup entworfen, das eine geschlossene BASIS-Umgebung nachbaut. Hierfür werden die tatsächlichen Group Policies verwendet, die im BASIS-Umfeld für den HmbBfDI im Einsatz sind (Stand: 10.12.2019).

Aufbau

- Das Testsetup besteht aus vier Komponenten:
- Windows 10 Enterprise Client (Version 1809 Build 17763.379)
- Windows Server 2016 Server (Version 1607 Build 14393.693)
- Firewall sowie Überwachung sämtlicher (virtueller) Interfaces mittels Wireshark
- MitM SSL Proxy (Burp)



Um die Kommunikation zwischen Windows und Microsoft zuverlässig betrachten zu können, war es nötig die SSL-Verbindungen durch einen Man-in-the-Middle Proxy zu leiten. Hierfür wurde über die BASIS-

konfiguration hinaus ein Group Policy Object (GPO) erstellt, das eine entsprechende Konfiguration samt SSL-CA-Zertifikat auf dem BASIS Client installiert.
Ein vom Windows Client ausgehender Request wird transparent durch den Proxy umgeleitet. Der Proxy ist in der Lage, für jeden per HTTPS aufgerufenen Host ein passendes Zertifikat bereitzustellen, sodass alle übermittelten Inhalte inspiziert werden können.
Dataport hat für diesen Testaufbau einen Export der tatsächlich beim HmbBfDI im Einsatz befindlichen GPOs zur Verfügung gestellt.
Zusätzlich erfolgte die Kontrolle weiterer Protokolle durch Wireshark.

BASIS

Die von Dataport zur Verfügung gestellte Konfiguration hat bereits einen starken Datenschutzfokus. Sofern ohne Einschränkungen für die tägliche Arbeit möglich, sind auf einem BASIS PC alle zusätzlichen Apps entweder deaktiviert oder entfernt. Darüber hinaus ist der Windows Store deaktiviert, sodass ein Nutzer nicht in der Lage ist, Software mit Trackingpotential selbst zu installieren.
Ebenso ist die Onlinekomponente des Windows-Suchassistenten Cortana deaktiviert. Hier konnte vor Übernahme der BASIS Konfiguration eine Menge Datenverkehr beobachtet werden, unter anderem wurde jeder Tastendruck mit Fokus auf das Cortana-Suchfeld direkt an Microsoft übertragen.
Leider lassen sich auch in der genutzten Enterprise Version von Windows 10 nicht alle von Microsoft per Default installierten Apps vollständig vom System entfernen. So finden sich auf einem BASIS System weiterhin unter anderem Verweise auf die Wetter-App, X-Box App, die Calendar App und die Mail App. Diese werden jedoch unter Nutzung von AppArmor an der Ausführung gehindert. In der Produktivumgebung wird laut Aussage Dataports ein zusätzliches Bereinigungs-Script genutzt, um die Anzeige der ohnehin unterdrückten Anwendungen zu entfernen.

Beobachteter Verkehr

Nachdem auf dem beschriebenen Testsetup erfolgreich ein BASIS System konfiguriert war, wurde der Windows Client für einige Tage sporadisch genutzt, während er fünf Tage betrieben wurde. Da es im Rahmen dieses empirischen Tests keine Möglichkeit der vollständigen Erfassung allen möglichen Netzwerkverkehrs gibt, beschränkt sich diese Betrachtung auf die mitgeschnittenen Requests. Es ist nicht ausgeschlossen, dass bei anderer Nutzung, z.B. dem Starten anderer Apps oder Anwendungen weitere Netzwerkverbindungen entstehen. Zudem gehen wir davon aus, dass die virtualisierten Installationen des Windows Server sowie des Clients zu keinen anderen Verhalten im Gegensatz zu einem nicht-virtua-

lisierten Betrieb führen. Für eine Betrachtung des BASIS Systems im Rohzustand mit Hinblick auf regelmäßige Telemetrie ist dieser Test jedoch geeignet. Außerdem wurden sämtliche Standardprogramme testweise ausgeführt, um zu analysieren, ob einzelne Anwendungen ggf. noch nicht vollständig mittel GPOs reguliert worden sind.

Jeder der folgenden Requests wurde mehr als einmal beobachtet. Die dargestellten Parameter sind tatsächlichen Requests entnommen, unterliegen im Vergleich jedoch Veränderungen.

URL	`http://pki.servicedpaor.de`

POST/GET	`/ctl/pinrulesstl.cab?2a7f352042f5e461`
	
	`/ctl/disallowedcertstl.cab?c0af6a5dc63efda6`

Daten	Komprimierte .stl-Dateien für den Austausch und die Aktualisierung sicherer bzw. unsicherer Root-CA-Zertifikate
Kommentar	
Handlungs-empfehlung	Keine

URL	`https://settings-win.data.microsoft.com`
POST/GET	`/settings/v2.0/analog/ASAP_VES?`**`os`**`=windows&`**`osver`**`=10.0.17763.1.amd64fre.rs5_release.180914-1434&`**`deviceid`**`=%7B1E4105D2-3156-475A-A236-47EB287CC622%7D`
Daten	Telemetrie-Daten zum Betriebssystem, der Betriebssystem-Version und der Geräte-ID
Kommentar	Dieser Endpunkt wird für das Update der Konfiguration von Windows Connected User Experience Anwendungen sowie der Telemetriekomponente verwendet. Microsoft warnt davor, dass das Deaktivieren dieses Traffics negative Auswirkungen auf die entsprechenden Anwendungen haben könnte.
Handlungs-empfehlung	Unterbinden sämtlicher Verbindungen, die einen Rückschluss auf individuelle Geräte zulassen. Im Zweifel vollständig Blocken.

URL	`wbswvpa032.fhhnet.stadt.hamburg.de:8531`

POST/GET	Nur `CONNECT`
Daten	Response `200`
Kommentar	Offenbar handelt es sich hier um einen Server der BSW. Es ist nicht ersichtlich, wofür diese Verbindung aufgebaut wird.
Handlungs-empfehlung	Blocken

URL	`http://ocsp.msocsp.com`
POST/GET	`/MFQwUjBQME4wTDAJBgUrDgMCG-gUABBSIGkp0%2Fv9GUvNUu1EP06Tu7%2BChyA-QUkZ47RGw9V5xCdyo010%2FRzEqXLNoCEyAAAgthQ5WjuUYjsrUAAAACC2E%3D`
Daten	
Kommentar	Online Certificate Status-Abfrage bei Microsoft, 4 Tage Gültigkeit
Handlungs-empfehlung	Es sollte geklärt werden, was genau der Parameter für Informationen beinhaltet. Ggf. kann Dataport diese OCSP-Informationen selbst anbieten, sodass die Verbindung zu Microsoft nicht mehr aufgebaut werden muss.

URL	`http://ocsp.digicert.com`
POST/GET	`/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUE-wQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEAi4elAbvpzaLRZNPjlRv1U%3D`
Daten	
Kommentar	Online Certificate Status-Abfrage bei Digicert, 7 Tage Gültigkeit
Handlungs-empfehlung	Es sollte geklärt werden, was genau der Parameter für Informationen beinhaltet. Ggf. kann Dataport diese OCSP-Informationen selbst anbieten, sodass die Verbindung zu Digicert nicht mehr aufgebaut werden muss.

URL	`http://ts-ocsp.ws.symantec.com`

POST/GET	/MFEwTzBNMEswSTAJBgUrDgMCGgU-ABBRi82PVYYKWGJWdgVNyePy5kYTdqQQUX5r1blzMzHSa1N197z%2Fb7Ey-ALt0CEA7P9DjI%2Fr81bgTYapgbGlA%3D
Daten	
Kommentar	Online Certificate Status-Abfrage bei Symantex, 7 Tage Gültigkeit
Handlungs-empfehlung	Es sollte geklärt werden, was genau der Parameter für Informationen beinhaltet. Ggf. kann Dataport diese OCSP-Informationen selbst anbieten, sodass die Verbindung zu Symantec nicht mehr aufgebaut werden muss.

URL	http://tile-service.weather.microsoft.com
POST/GET	/de-DE/livetile/preinstall?**region**=DE&**ap-pid**=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold
Daten	
Kommentar	Updates für die Live-Kacheln der Wetter-App (Wetter-Informationen)
Handlungs-empfehlung	Blocken

URL	http://blob.weather.microsoft.com
POST/GET	/static/mws-new/LiveTile/W2.png?a
Daten	
Kommentar	Updates für die Live-Kacheln der Wetter-App (Hintergrundbild)
Handlungs-empfehlung	Blocken

Fazit

Das Betriebssystem Windows 10 Enterprise Version 1809 weist keine datenschutzfreundliche Konfiguration auf, da weder nicht erforderliche Software noch die Telemetriekommunikation an Microsoft per Default deaktiviert ist

Die BASIS Konfiguration schränkt die Kommunikation zwischen Windows 10 und dem Microsoft Back-End durch entsprechend konfigurierte GPOs weitgehend ein. Im Gegensatz zum Test des letzten Jahres konnten die Verbindungsversuche, mit Ausnahme der Verbindung zu https://settings-win.data.microsoft.com in dem diesjährigen Test nicht erneut festgestellt werden. Dieser Test kann keine abschließende Erkenntnis darüber liefern, ob im Falle zusätzlich installierter Software weiter Traffic zu beobachten wäre. Die BASIS-Grundkonfiguration stellt jedoch einen weitgehenddatenschutzgerechten Standard bereit.
Die verbleibenden Verbindungen lassen sich nicht vollständig anhand der von Microsoft veröffentlichen Dokumente erklären, sodass im Einzelnen nicht transparent ist, welche Daten übermittelt werden.

Nach unserer Erkenntnis und in Absprache mit Dataport empfiehlt der HmbBfDI die Deaktivierung der Kommunikation, die als unkritisch für den Systembetrieb eingestuft wurde und möglichst viel der restlichen Kommunikation. Darüber hinaus muss dieser Status-Quo weiterhin regelmäßig, spätestens mit jedem turnusmäßigen Update der Windows Plattform wiederholt, die Ergebnisse verifiziert und unter Umständen an der Konfiguration nachgebessert werden.

Weiteres Vorgehen

1. Der Senatskanzlei und Dataport wird das Prüfungsergebnis zur Verfügung gestellt.
2. Die Senatskanzlei und Dataport werden gebeten, für den aufgezeigten Netzverkehr, der über GPOs nicht unterbunden werden kann, einerseits zu erläutern, zu welchem Ziel diese jeweils erfolgt. An einer Erörterung mit Microsoft zu dieser Frage würde sich der HmbBfDI gerne beteiligen. Andererseits wird gebeten, für die produktiv genutzten BASIS-PC im Behördenumfeld den aufgezeigten verbliebenen Verkehr zu blocken und das Verhalten der Rechner zu überwachen, um ggf. nachsteuern zu können.
3. Sobald Klarheit über die übermittelten Daten besteht, ist zu bewerten ob es sich bei den übermittelten Daten um personenbezogene Daten handelt. Falls dies der Fall ist, ist anschließend zu prüfen, ob es für die Übertragung an Microsoft eine Rechtsgrundlage gibt und ob die Übertragung erforderlich und verhältnismäßig ist.
4. Untersuchung sollte mit der für Herbst 2020 erwarteten nächsten zu installierenden Version von Windows 10 wiederholt werden.