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.