Telefon: 233 – 76 77 77

IT-Referat

Datenschutzproblem von Windows 10: Wie wurde es von der Stadtverwaltung gelöst?

Datenschutzproblem von Windows 10: Wie wurde es von der Stadtverwaltung gelöst?
Antrag Nr. 14-20 / A 03968 der ÖDP vom 11.04.2018

Sitzungsvorlage Nr. 20-26 / V 00095

1 Anlage

Beschluss des IT-Ausschusses vom 27.05.2020 (SB)

Öffentliche Sitzung

Inhaltsverzeichnis

I. Vortrag des Referenten

Zusammenfassung

Im Antrag „Datenschutzproblem von Windows 10: Wie wurde es von der Stadtverwaltung gelöst?“ der ÖDP vom 11.04.2018 wird die Stadtverwaltung gebeten, zu erläutern, wie potentielle Datenschutzprobleme des Betriebssystems Windows 10 rechtlich und technisch gelöst wurden.

Für das Betriebssystem Windows10 wurde durch das IT-Referat bzw. den IT-Dienstleister it@M ein Security Konzept erstellt, das im Detail beschreibt, wie der Windows-Client in der Landeshauptstadt München eingesetzt und konfiguriert wird, um IT-sicherheits- und datenschutzkonform betrieben zu werden. Das Konzept basiert auf der Empfehlung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und verschiedener für die Einhaltung des Datenschutzes verantwortlichen Stellen.

Auf Grundlage dieses Konzeptes sieht das IT-Referat die Voraussetzungen gegeben, um Windows10 in der Stadt München als Betriebssystem auf den städtischen Arbeitsplatzrechnern einzusetzen.

1. Stadtratsantrag

Im Antrag „Datenschutzproblem von Windows 10: Wie wurde es von der Stadtverwaltung gelöst?“ der ÖDP vom 11.04.2018 wird die Stadtverwaltung gebeten, zu erläutern, wie potentielle Datenschutzprobleme des Betriebssystems Windows 10 rechtlich und technisch gelöst wurden.

Als Begründung wurde in diesem Antrag aufgeführt, dass Windows 10 vom Benutzer die Einwilligung verlange, dass wesentliche Teile seiner persönlichen Daten an externe Server außerhalb seiner Verfügungsgewalt übermittelt werden.

Ausgehend davon wurde die Stadtverwaltung gebeten, ihre Lösung „im Detail (natürlich ohne München-spezifische Informationen)“ darzustellen.

2. Umsetzung der Client-Sicherheit

Die LHM setzt derzeit noch Windows 10 Version 1809 (Build 17763) Enterprise produktiv ein. Für dieses Betriebssystem existiert ein Security Konzept, das LHM spezifische Konfigurationseinstellungen und Empfehlungen des Windows10-Clients enthält. Ab Mai 2020 wird mit dem Rollout von Windows 10 1909 (Build 18363) Enterprise begonnen. Das Security Konzept der LHM wurde im Hinblick auf die technischen Möglichkeiten und Empfehlungen dieser Version fortgeschrieben.

Vorgaben und Empfehlungen für eine sicherheitstechnisch und datenschutzrechtlich konforme Bereitstellung von Windows 10 in Behörden und Unternehmen werden im Wesentlichen von fünf Institutionen getroffen:

- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)
- Bayerisches Landesamt für Sicherheit in der Informationstechnik (LSI)

- Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK)
- Microsoft als Produkthersteller (Empfehlung: nach hinten stellen; Position 1 erweckt einen falschen Eindruck)

Das in der LHM umgesetzte Security Konzept berücksichtigt Empfehlungen all dieser Stellen und geht z.T. sogar deutlich darüber hinaus.

Vorgaben des BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist eine Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat, die für Fragen der IT-Sicherheit zuständig ist. Der Leitsatz des BSI lautet: „Das BSI als die nationale Cyber-Sicherheitsbehörde gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft."

Das BSI veröffentlicht regelmäßig Vorgaben für die sichere Konfiguration der unterschiedlichsten Produkte im Behördenumfeld. Diese werden im Rahmen des so genannten IT-Grundschutzes Beispiel, vgl.[1])bei der LHM schon seit Jahren angewendet.

Die Vorgabencluster des BSI sind in Bezug auf das Security Konzept der LHM am relevantesten, so dass diese im Folgenden kurz aufgelistet werden:

- SYS.2.2.3.A1 Planung des Einsatzes von Cloud-Diensten
- SYS.2.2.3.A2 Geeignete Auswahl einer Windows 10-Version und Beschaffung
- SYS.2.2.3.A3 Geeignetes Patch- und Änderungsmanagement
- SYS.2.2.3.A4 Telemetrie und Datenschutzeinstellungen
- SYS.2.2.3.A5 Schutz vor Schadsoftware
- SYS.2.2.3.A6 Integration von Online-Konten in das Betriebssystem [Benutzer]
- SYS.2.2.3.A7 Lokale Sicherheitsrichtlinien
- SYS.2.2.3.A8 Zentrale Verwaltung der Sicherheitsrichtlinien von Clients
- SYS.2.2.3.A9 Sichere zentrale Authentisierung der Windows-Clients
- SYS.2.2.3.A10 Konfiguration zum Schutz von Anwendungen in Windows 10
- SYS.2.2.3.A11 Schutz der Anmeldeinformationen in Windows 10
- SYS.2.2.3.A12 Datei- und Freigabeberechtigungen
- SYS.2.2.3.A13 Einsatz der SmartScreen-Funktionen
- SYS.2.2.3.A14 Einsatz des Sprachassistenten Cortana [Benutzer]
- SYS.2.2.3.A15 Einsatz der Synchronisationsmechanismen in Windows 10
- SYS.2.2.3.A16 Anbindung von Windows 10 an den Microsoft-Store
- SYS.2.2.3.A17 Verwendung der automatischen Anmeldung
- SYS.2.2.3.A18 Einsatz der Windows-Remoteunterstützung
- SYS.2.2.3.A19 Verwendung des Fernzugriffs über RDP [Benutzer]
- SYS.2.2.3.A20 Einsatz der Benutzerkontensteuerung für privilegierte Konten

1 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_2_2_3_Clients_unter_Windows_10.html

- SYS.2.2.3.A21 Einsatz des Encrypting File System EFS(CI)
- SYS.2.2.3.A22 Windows PowerShell(CIA)
- SYS.2.2.3.A23 Erweiterter Schutz der Anmeldeinformationen in Windows 10(CI)
- SYS.2.2.3.A24 Aktivierung des Last-Access-Zeitstempels(A)
- SYS.2.2.3.A25 Umgang mit Fernzugriffsfunktionen der "Connected User Experience and Telemetry"(CI)

Vorgaben des BayLDA

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) ist in Bayern die Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich, das heißt es kontrolliert private Wirtschaftsunternehmen, selbstständig, freiberuflich Tätige, private Krankenhäuser und Heime, Vereine, Parteien und Privatpersonen. Die Hinweise des BayLDA können – auch wenn nicht direkt für Behörden bindend – doch relevante Auswirkungen auf die Sicherheitskonfiguration haben.

Aus diesem Grunde sind auch Einstellungen und Empfehlungen dieser Stelle in das Security Konzept der LHM mit eingeflossen[2].

Vorgaben des LSI

Das Landesamt für Sicherheit in der Informationstechnik ist die IT-Sicherheitsbehörde des Freistaats Bayern. Aufgaben sind neben dem aktiven Schutz der staatlichen IT-Systeme die Beratung von Kommunen, öffentlichen Unternehmen als Betreiber kritischer Infrastrukturen und der Staatsverwaltung an sich.

Das Security Konzept für Windows10 der LHM orientiert sich an den vom Landesamt für Sicherheit in der Informationstechnik (LSI) gemachten Vorgaben, die im sog. „Windows10-Leitfaden“ des LSI beschrieben sind.

Prüfschema der Datenschutzkonferenz (DSK)

Die DSK (Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder) hat im November 2019 ein Prüfschema veröffentlicht, das für den Einsatz von Windows 10 Verantwortliche darin unterstützt, die Einhaltung der rechtlichen Vorgaben des DSGVO im konkreten Fall zu prüfen und zu dokumentieren[3].

Dass und warum dies notwendig ist, wird in diesem Dokument gleich in der Einleitung begründet: „*Die Abarbeitung des nachfolgenden Prüfschemas ist deshalb erforderlich, weil sich die Übermittlung von Daten an Microsoft in bislang keiner Edition und Version durch eine Änderung der Konfigurationseinstellungen komplett abstellen lässt und sich das Kommunikationsverhalten und die Konfigurationsmöglichkeiten von Windows 10 mit neuen Versionen ändern können.*“

Das Prüfschema ist somit eine Hilfestellung für alle, die Windows 10 einsetzen, gibt Hinweise für die rechtliche Prüfung des Einsatzes von Windows 10, erläutert welche Normen im Rahmen der Prüfung einzuhalten sind und welche Maßnahmen getroffen werden sollten, um einen datenschutzkonformen Einsatz von Windows 10 zu ermöglichen.

2 https://www.gp-pack.com/gp-pack-lda-windows-10-investigation-report/
3 https://www.datenschutzkonferenz-online.de/media/ah/20191106_win10_pruefschema_dsk.pdf

Vorgaben von Microsoft

Microsoft gibt als Hersteller des Betriebssystems ausführliche Vorgaben zur Konfiguration des Betriebssystems Windows 10 in Unternehmen und Behörden. Diese Hinweise zum sicheren Betrieb von Windows10 in Unternehmensumgebungen werden in den regelmäßig aktualisierten so genannten „Windows Security Baselines[4]“ veröffentlicht.

Die Inhalte der Windows Security Baseline für das o. g. Produkt Microsoft Windows 10 1909 Enterprise wurden im Security Konzept der LHM berücksichtigt und umgesetzt.

Umsetzung im Security Konzept der LHM

Basierend auf den oben beschriebenen Grundlagen beschreibt das Security Konzept der LHM, wie Windows 10 in der Stadt München eingesetzt wird, um datenschutzkonform und sicher eingesetzt zu werden.

Das Security-Konzept zu Windows10 beinhaltet dazu detaillierte technische Vorgaben und Restriktionen.

Um den Datenschutzbelangen der Beschäftigten sowie der Bürger*innen Rechnung zu tragen, wird im Security Konzept unter Anderem definiert, dass Einstellungen und Funktionen, die die Verwendung von Nutzerdaten durch Microsoft erfordern, so weit wie möglich technisch deaktiviert sind.

Hierdurch ist insbesondere

- die Nutzung von Microsoft-Konten,
- die Nutzung von Werbe-Ids,
- die Übermittlung von Eingabe- und Schreibverhalten,
- die Übermittlung von Sprache bei Spracheingabe an Microsoft,
- die Positionserkennung und Positionsdienste,
- der persönliche Assistent Cortana,
- der SmartScreen-Filter

deaktiviert.

Wie beschrieben wird in der LHM von den grundsätzlich verfügbaren Varianten von Microsoft Windows 10 (Windows 10 Home, Windows 10 Professional und Windows 10 Enterprise) die Version Windows 10 Enterprise zu Einsatz gebracht. Die Versionen unterscheiden sich ganz erheblich im Konfigurationsumfang und auch in den Betriebsarten.

Bei der in der LHM eingesetzten Version Windows 10 Enterprise ist eine deutlich granularere Kommunikationseinstellung möglich als bei den Varianten „Home“ und „Professional“. Diesbezüglich gibt es u. a. entsprechende Erkenntnisse seitens des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA) aus Mitte 2017 bei der Prüfung der Windows 10 Enterprise Version 1607 (Builds 14393) und 1703 (Build 15063)[5].

4 https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines
5 https://www.heise.de/newsticker/meldung/Datenschuetzer-Unternehmen-koennen-Windows-10-Enterprise-datenschutzkonform-einsetzen-3835496.html

Microsoft Windows 10 Enterprise ist weltweit in Unternehmen und Behörden im Einsatz und somit Marktstandard. Durch den Einsatz dieses Standards ist die LHM erstmalig seit Jahrzehnten in der Lage, aktuelle Technologie einzusetzen. Somit ist auch eine Grundlage geschaffen, zeitgerecht und zukünftig angemessen auf Bedrohungen bei der IT Sicherheit reagieren zu können.

Das vorliegende Security Konzept wird kontinuierlich fortgeschrieben und angepasst. Insbesondere wurde es für den derzeit in Entwicklung befindlichen zukünftigen Win10-Standard-Client (Basis ist die Windows10-Version 1909) weiter entwickelt.

Es ist sicher gestellt, dass das Konzept und die damit verbundenen Einstellungen mit jedem Windows 10 Release neu bewertet und bei Bedarf angepasst werden. Somit wird auch die Aktualität des Clients hinsichtlich Datenschutz und Security fortlaufend gewährleistet sein.

Seitens der LHM werden die maximal möglichen Maßnahmen ergriffen. Bei der Thematik handelt es sich jedoch um ein weltweite Sachlage, welche die LHM ebenso betrifft. Auf Grundlage der getroffenen Maßnahmen und Vorkehrungen ist der Einsatz von Windows 10 mit den getroffenen Konfigurationsmöglichkeiten und Einschränkungen aus Sicht des IT-Referats möglich und zulässig.

Wichtig ist dabei anzuerkennen, dass sich die technologischen Gegebenheiten, Möglichkeiten und Restriktionen, aber auch die gesetzlichen Rahmenbedingungen auch in Zukunft verändern und weiter entwickeln werden. Aus diesem Grund ist eine fortwährende Beobachtung und Überprüfung dieser Einschätzung unerlässlich. Dazu gehört ein enger Dialog zwischen dem IT-Sicherheitsmanagement im IT-Referat, dem IT-Dienstleister it@M und den behördlichen Datenschutzbeauftragten, um sicher zu stellen, dass bestehende Konzepte und technische Maßnahmen fortgeschrieben und gegebenenfalls angepasst und weiter entwickelt werden.

Diese Abstimmung hat sich etabliert und bewährt und wird auch in Zukunft intensiv fortgesetzt werden.

3. Beteiligungen

Der Korreferent / die Korreferentin des IT-Referats hat einen Abdruck der Beschlussvorlage erhalten.

Anhörung des Bezirksausschusses

In dieser Beratungsangelegenheit ist die Anhörung des Bezirksausschusses nicht vorgesehen (vgl. Anlage 1 der BA-Satzung).

II. Antrag des Referenten

1. Mit diesem Beschluss ist der Antrag Nr. 14-20 / A 03968 „Datenschutzproblem von Windows 10: Wie wurde es von der Stadtverwaltung gelöst?“ der ÖDP vom 11.04.2018 geschäftsordnungsgemäß erledigt.
2. Der Beschluss unterliegt nicht der Beschlussvollzugskontrolle.

III. Beschluss

nach Antrag.

Der Stadtrat der Landeshauptstadt München

Der / Die Vorsitzende — Der Referent

Ober-/Bürgermeister/-in
ea. Stadtrat / ea. Stadträtin

Thomas Bönig
Berufsm. Stadtrat

IV. Abdruck von I. mit III.

über die Stadtratsprotokolle

an das Direktorium - Dokumentationsstelle
an die Stadtkämmerei
an das Revisionsamt

z. K.

V. Wv. - IT-Referat - Beschlusswesen