

Anlage zur BV „Digitale Souveränität als strategisches Leitprinzip – Sichere Software für München“:

Check des IT-Serviceportfolios der LHM auf digitale Souveränität

Für die Beantwortung der Stadtratsanträge zur digitalen Souveränität wurde eine Methodik für die Prüfung des IT-Serviceportfolios entwickelt. Aktuell liegt die Version 1.0 vor.

Zuerst wird die Methodik der Vorgehensweise erläutert und im zweiten Schritt die Ergebnisse der Auswertung auf Anwendungsservice-Ebene.

Die LHM nutzt 2780 Anwendungsservices (Stand Oktober 2025), die die Geschäftsprozesse der LHM digital unterstützen. Der Check auf digitale Souveränität in der Software wird auf diese Anwendungsservices angewandt.

Die hohe Zahl der Anwendungsservices legt eine Fokussierung nahe.

Als objektivierbares Kriterium bietet sich die Business-Kritikalität der Services an.

Die Einwertung der Anwendungsservices in Bezug auf ihre Business-Kritikalität mittels einer Business Impact Analyse¹ ist in der IT der LHM bereits etabliert und findet zum Beispiel im IT-Notfallmanagement Anwendung.

Aufgrund der Fokussierung auf die Business-Kritikalität resultierten zu diesem Zeitpunkt noch 194 zu betrachtende Anwendungsservices.

Aktuell liegt kein Kriterienkatalog vom Bund, einem Bundesland oder einem führenden Forschungsinstitut vor, aufgrund dessen eine Bewertung von IT-Services auf ihre digitale Souveränität hin durchgeführt und mit einer quantitativen Bewertung abgeschlossen werden könnte. Unsere Ausarbeitung des Checks auf digitale Souveränität beruht maßgeblich auf Quellen des Fraunhofer Instituts „Kompetenzzentrum öffentliche IT“² und einem Fragebogen der „Digital Sovereignty-Plattform“³.

Auf diesen drei Konzepten aufbauend hat das IT-Referat einen kurzen Fragenkatalog und eine quantitative Bewertung entwickelt.

Der Check auf digitale Souveränität der Anwendungsservices nutzt folgende Fragen:

1. Hat die Software eine marktbeherrschende Stellung innerhalb ihrer Kategorie (über 50%)?
2. Trifft eine der zwei Möglichkeiten zu?
Bietet der Markt eine Enterprise Software mit ähnlicher Funktionalität an und it@M kann mit angemessenen Kosten und Aufwand auf dieses Angebot wechseln?
Oder
Kann it@M mit angemessenen Kosten und Aufwand selber eine Lösung bauen?
3. Besteht Support für Security Updates des Anbieters z.B. im Rahmen eines Lifecyclemanagements?
4. Handelt es sich um Open Source-Software?
5. Nutzt die Software ausschließlich standardisierte Schnittstellen?
6. Nutzt die Software ausschließlich standardisierte Dateiformate?

¹ <https://wilma.muenchen.de/workspaces/it-notfallmanagement/apps/content/inhalt>

² „Digitale Souveränität als strategische Autonomie“ auf <https://publica-rest.fraunhofer.de/server/api/core/bitstreams/46778b73-6f29-4a35-a801-b3024108a4d6/content> und „Digitale Souveränität“ auf <https://publica.fraunhofer.de/entities/publication/8a0846aa-ec67-4788-8f0b-4bb540d97162>

³ <https://digital-sovereignty.net>

7. Ist der Firmensitz des Mutterkonzerns des Softwareherstellers bzw. Cloud Service-Anbieters in der EU?

Für die o.g. 194 Anwendungsservices mit hoher Business-Kritikalität wurden diese Fragen durch insgesamt 79 verantwortliche Service Owner beantwortet.

Ziel ist es, dass die Erfassung der digitalen Souveränität ausschließlich innerhalb des IT-Servicemanagementtools des IT-Referats erfolgen kann. Da es sich aktuell um die Version 1.0 des digitalen Souveränitätschecks handelt und die Zeit der Befragung auch kurz war, schloss sich an die Modellierung der Kriterien und die Erfassung der Status der einzelnen Anwendungsservices im Tool eine Phase der manuellen Validierung der Servicedaten an.

Die Auswertung der Fragen erfolgt in zwei Phasen:

In der ersten Phase wird ein Service als digital nicht souverän mit dem Score E bewertet, wenn es sich beim Hersteller um einen Monopolisten handelt und keine Alternative für diese Software besteht (Frage 1 „ja“ und Frage 2 „nein“).

Wenn dem nicht so ist, werden in der zweiten Phase die Antworten auf die weiteren Fragen 3–7 ausgewertet. Jede Antwort auf eine der Fragen, die die digitale Souveränität unterstützt, erhält eine Bepunktung mit 20%.

Der aufsummierte Wert wurde auf eine 5-Punkte-Skala von SDS 1 bis SDS 5 mit folgenden Wertebereichen gemappt:

SDS 1 ≥ 80 % digital souverän, und darunter mit SDS 2 ≥ 60 %, und darunter mit SDS 3 ≥ 40 %, und darunter mit SDS 4 ≥ 20 % und letztendlich SDS 5 mit < 20 % als niedrigste Kategorie.

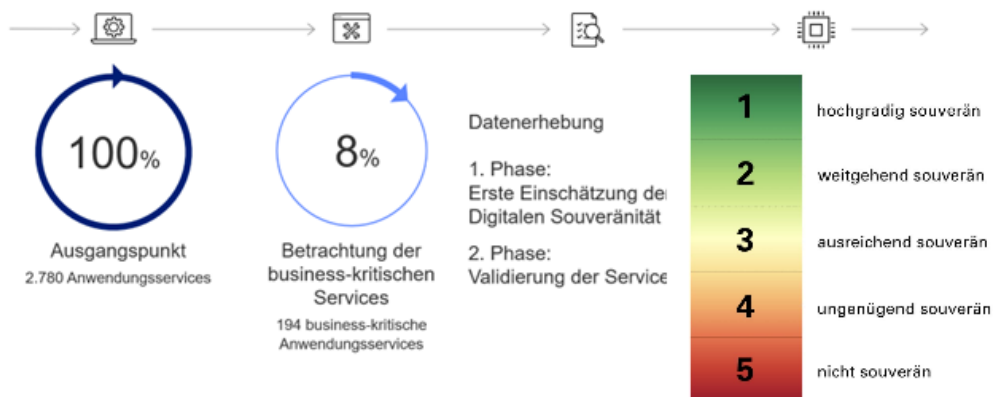


Abbildung 1 Vier Schritte der Auswertung des IT-Serviceportfolios auf digitale Souveränität

Die Ergebnisse der Prüfung lauten wie folgt (Absolute Zahlen in Klammern):

- SDS 1: 33 % (64)
- SDS 2: 33 % (64)
- SDS 3: 8 % (16)
- SDS 4: 5 % (9)
- SDS 5: 21 % (41)

Einzelaspekte der Analyse:

- Von den 194 Anwendungsservices befindet sich bei 31 Softwareherstellern der Mutter-sitz nicht in der EU: Bei einem Anwendungsservice ist er in der Schweiz, bei 29 in den USA und bei einem im Vereinigten Königreich.
- Die Kategorie SDS 5 setzt sich fachlich aus den folgenden Rubriken zusammen: gesetzlich vorgeschriebene Leistungen zur e-Vergabe, Anwendungsservices einer großen Anstalt öffentlichen Rechts in Bayern, Software für die eAkte, ein Anwendungsservice einer großen Anstalt des öffentlichen Rechts der Hansestadt Hamburg, zwei Services eines Softwareherstellers in den USA, deutsche Softwarehersteller spezialisiert auf die öffentliche Verwaltung u.a. im Kontext von Wahlen und eine Reihe von Anwendungsservices im Kontext des Personalmanagementsystems der LHM eines deutschen Softwareherstellers.

Der jetzt vorliegende Softwarecheck auf digitale Souveränität in der Version 1.0 wird vom IT-Referat gemeinsam mit der TU München in Zukunft fortgeschrieben und weiterentwickelt. Er dient als Grundlage, das Thema digitale Souveränität sachlich strukturiert im Rahmen der gesamten Risiko-Betrachtung zu adressieren und zu bewerten und so letztlich die, für die Landeshauptstadt München erforderliche digitale Souveränität herzustellen.