Forschungsgemeinschaft elektronische Medien e. V.

Stellungnahme zum Gesetz zur Förderung der elektronischen Verwaltung in Thüringen sowie zur Änderung verwaltungsverfahrensrechtlicher Vorschriften

---

vorgelegt von: Alexander Votteler
Christian Dieckhoff
und weiteren Mitglieder der FeM e. V.

vom: 2. Februar 2018

Inhaltsverzeichnis

1 Einleitung

Das Gesetz zur Förderung der elektronischen Verwaltung in Thüringen sowie zur Änderung verwaltungsverfahrensrechtlicher Vorschriften soll die Digitalisierung der Verwaltung in Thüringen regeln und digitale Behördengänge ermöglichen. Die Forschungsgemeinschaft elektronische Medien e. V. (im folgenden FeM e. V. genannt) sieht den Gesetzesentwurf und die grundlegende Initiative positiv, allerdings muss ein sehr großes Augenmerk auf die Qualität und Sicherheit der eingesetzten Software und Kommunikationskanäle gelegt werden. Dabei sollte insbesondere darauf geachtet werden in der Vergangenheit gemachte Fehler bei IT-Großprojekten nicht zu wiederholen und auf eine offene und freie Gestaltung der technischen Umsetzung und der Projektdurchführung zu achten. Diese Stellungnahme wird sich hauptsächlich mit technischen Grundsätzen und Verfahrensweisen beschäftigen, welche für einen Erfolg des Gesetzes unumgänglich sind.

Zum Thema Datenschutz:

Der Datenschutz und die Datensicherheit sind bei diesem Projekt essenziell. Die FeM e. V. versteht allerdings ihre primären Kompetenzen vor allem im technischen Bereich. Wir vertrauen in diesem Bereich aber auf die Meinung der anderen Sachverständigen, insbesondere von Netzpolitik.org.

2 Stellungnahme

2.1 Open Source

Aus dem Gesetzesentwurf wird nicht ersichtlich, wie die zum Einsatz kommende Software entwickelt werden soll. Hier wird empfohlen, alle Softwarerzeugnisse im Sinne des Open Source Gedanken öffentlich einsehbar zu machen.

So können interessierte Bürger und Fachleute unabhängig die Software prüfen und auf mögliche Sicherheitslücken schon frühzeitig hinweisen. Außerdem wird die Software schon im Entwicklungsprozess einer öffentlichen Revision unterzogen und es können Planungsfehler vermieden werden (siehe aktuelles Debakel um das "Besondere elektronische Anwaltspostfach").

Open Source bezieht sich aber nicht nur auf eine reine Offenlegung der Quelltexte, sondern auch auf die Möglichkeit der Partizipation. Dies beinhaltet eine Möglichkeit zu Kommentaren, Fehlerberichten, dem Vorschlagen neuer Funktionen aber auch dem Beitragen von eigenem Code als Vorschlag (sog. Pull-Requests"). Open Source bietet, trotz seiner Offenheit, dem Projektverantwortlichen die Möglichkeit die volle Kontrolle zu behalten. Durch fachliche Audits (eine beauftragte Überprüfung von Software) von Institutionen, die nicht mit dem Unternehmen in Verbindung stehen, welches die Software entwickelt hat, kann eine konstant hohe Codequalität, sowie die Sicherheit des E-Government-Systems sichergestellt werden. Essenziell dafür ist es, dass die Audit-Institutionen vollen Zugriff auf den zu überprüfenden Qullcode haben.

Sollte eine Software zusätzlich noch unter einer Lizenz zur Verfügung gestellt werden, die eine Wiederverwendung erlaubt, kann Thüringen Maßstäbe in Sa-

chen Digitalisierung setzen. Andere Länder und Behörden könnten die in Thüringen entwickelte Verwaltungssoftware benutzen und ebenfalls mit Ressourcen zur Weiterentwicklung beitragen. So ließe sich in Thüringen eine Vorreiterstellung in Deutschland in Sachen E-Government erringen.

2.2 Dezentralität

Der aktuelle Gesetzesentwurf sieht eine Zentralisierung des Systems vor. Davon wird stark abgeraten. Eine Zentralisierung ist risikobehaftet und führt zu einem Single-Point-Of-Failure. Dies gilt sowohl für die Verfügbarkeit des Dienstes als auch für die Daten- und Anwendungssicherheit. Auch dezentrale Systeme lassen sich geordnet aufbauen und unkompliziert verwalten.

Es sollte ein dezentrales System aufgebaut werden, bei dem Daten verteilt bei verschiedenen Behörden gehalten werden und diese über autorisierte und zeitgemäß verschlüsselte Schnittstellen kommunizieren. Dezentrale Systeme können sicherer gestaltet werden als ein einzelnes zentrales System und bieten eine höhere Flexibilität und Ausfallsicherheit.

2.3 Vernichtung von digitalisierten Originalen

Da nicht gewährleistet werden kann, dass alle Originale fehlerfrei in digitale Kopien übertragen werden können wird empfohlen, sämtliche Originale bis zum Ablauf der Aufbewahrungsfristen nicht zu vernichten. Papierarchive sollten weiterhin gepflegt werden.

2.4 Maschinenlesbarkeit und Programmierschnittstellen

Das Gesetz zeigt bereits an einigen Stellen Grundsätze der Maschinenlesbarkeit von Ausgabedateien. Wir empfehlen eine Verankerung der Maschinenlesbarkeit

für sämtliche durch das System bereitgestellte Daten im Gesetz.

Sämtliche Ausgaben der Verwaltungssoftware sollten (zusätzlich zu einem menschenlesbaren Format) in einem standardisierten maschinenlesbaren Format zur Verfügung gestellt werden. Diese Funktion kann zur weiteren Auswertung oder Verwendung in anderen Applikationen genutzt werden, ohne dass Dokumente manuell und damit fehleranfällig und zeitaufwendig abgetippt werden müssen.

Das System sollte modular aufgebaut werden und die einzelnen Komponenten sollten über eine dokumentierte Schnittstelle kommunizieren. Zusätzlich sollten viel genutzte Funktionen mit einer für externe Programme zugänglichen Programmierschnittstelle (API) ausgestattet werden. Diese externen Programme sollten, wenn sie persönliche Daten abrufen, erst nach vorhergehender Authentifizierung und Autorisierung durch den entsprechenden Nutzer Zugriff auf Daten erhalten. Auch muss genau festgelegt werden auf welche Daten und zu welchen Zeiträumen die externe Schnittstelle Zugriff haben darf. Der Zugang zu Daten welche unter Open Data fallen, wie zum Beispiel Katasterinformationen oder Mietspiegel, sollten ohne die oben genannten Einschränkungen öffentlich abrufbar sein.

Durch eine solche Schnittstelle kann das Verwaltungssystem in bestehende Systeme integriert werden. Dies führt zu erheblich weniger Aufwand im Austausch und der automatischen Verarbeitung von Daten.

2.5 De-Mail

Die FeM e. V. sieht De-Mail nicht als ein sicheres Kommunikationsmedium an. Nur eine wirkliche Ende-zu-Ende-Verschlüsselung der Mail sichert Datenschutz und Vertrauenswürdigkeit der Kommunikation ab. Bei der De-Mail wird der Bürger rechtlich gegenüber der klassischen Briefpost benachteiligt. Bei nicht ständiger Überprüfung steigt die Gefahr unbemerkter Zustellungen, auch wenn dies durch Gesetze oder AGBs anders vorgeschrieben ist. Die De-Mail ist mit der

normalen E-Mail absichtlich nicht kompatibel gehalten. Diese Inkompatibilität wird zu Verwechslungen und fehlgeschlagener Kommunikation bei fachlich nicht mit De-Mail vertrauten Anwendern führen. Es ist auch nicht absehbar, dass das De-Mail-System zu einer Akzeptanz bei privaten Anwendern kommt. Die Vorteile von De-Mail sind ausschließlich für die Behörden ersichtlich.

Um wirkliche Sicherheit zu gewährleisten, muss für persönliche Kommunikation eine verpflichtende Ende-zu-Ende-Verschlüsselung festgelegt werden. Dafür sollten etablierte internationale Standards wie S/MIME oder PGP verwendet werden.

Dafür empfiehlt sich anstelle des Betriebs eines De-Mail Gateways die Schaffung einer Zertifizierungs- und Signierungsstelle, die die entsprechenden Werkzeuge und kryptografischen Grundlagen bereitstellt und für die Bürger und Behörden des Landes verifiziert.

Referenzen:

- `https://www.ccc.de/system/uploads/64/original/CCC-de-mail-2011.pdf`
- `https://media.ccc.de/v/30C3_-_5210_-_de_-_saal_g_-_201312282030_-_bullshit_made_in_germany_-_linus_neumann`

3 Fazit und Schluss

3.1 Fazit

Allgemein ist die Initiative der Landesregierung zu begrüßen. Allerdings gibt es viel zu beachten, denn nur wenn auch Benutzbarkeit und Integration in bestehende Prozesse gewährleistet wird kann das System erfolgreich werden.

Ein solches E-Goverment-System wird von den Bürgern nicht angenommen werden, wenn es für diese nicht einfach und intuitiv zu Bedienen ist oder zu Unmut führen, wenn die Nutzung, trotz schlechter Bedienbarkeit verpflichtend ist. In letzterem Fall würde dies eine bundesweite schlechte Reputation für den Freistaat Thüringen bedeuten.

Die Daten- und Anwendungssicherheit muss durch die Verwendung von etablierten Standards, Audits durch unabhängige Experten, sowie die jederzeit mögliche Überprüfung des zugrunde liegenden Quellcodes durch jedermann gewährleistet werden.

3.2 Über die Forschungsgemeinschaft elektronische Medien

Die Forschungsgemeinschaft elektronische Medien e. V. (FeM e. V.) ist einer der größten studentischen Vereine an der Technischen Universität Ilmenau. Gegründet wurde der Verein im Jahr 1997 im Umfeld der TU Ilmenau. Er umfasst derzeit circa 2.000 Mitglieder und betreibt eines der größten selbstverwalteten studentische Netzwerk Deutschlands. Über verschiedene Streamingprojekte erreichte der Verein auch außerhalb Thüringens Bekanntheit.

Ziele des Vereins sind die Durchführung von Projekten der Forschung, Wissenschaft & Bildung, Erziehung, Kunst & Kultur sowie der Völkerverständigung im Bereich elektronischer Medien. Außerdem werden ähnliche Vorhaben anderer Organisationen, die den Bereich elektronische Medien betreffen oder im Umfeld desselben angesiedelt sind, gefördert. Weiterhin wird Jugendarbeit betrieben, insbesondere die Förderung jugendlicher Computerbenutzer. Hierbei werden diese an neue Technologien herangeführt, um diese kennen und nutzen zu lernen. Die FeM e. V. leistet Öffentlichkeitsarbeit, um die Bevölkerung mit neuen Technologien vertraut zu machen und auf die Chancen und Risiken derselben hinzuweisen.

Glossar

Audits Als Audit bezeichnet man das systematische Untersuchen von Software auf Fehler und Sicherheitslücken.

authentifiziert Unter einem authenifizierten Zugriff versteht man einen Zugriff, bei dem überprüft wurde, dass der Zugreifer wirklich derjenige ist, für den er sich ausgibt.

autorisiert Unter einem autorisierten Zugriff versteht man einen Zugriff, bei dem überprüft wurde, ob der Zugreifer auf die Daten zugreifen darf.

Freie Software Als Freie Software wird ein Lizenztechnscher Aspekt von Software betrachtet, Freie Software darf von jedem kopiert und dann verändert und weiterverteilt werden, ohne dass dies die Zustimmung des Autors benötigt.

Maintainer Als Maintainer wird der/die Leiter eines Softwareprojekt bezeichnet, unter anderem werden Pull-Requests bewertet, kommentiert und gegebenenfalls aufgenomment.

Maschinenlesbarkeit Die Daten liegen in einem freien, dokumentierten Format vor und können durch Software einfach ausgewertet werden.

Open Data Als Open Data (zu Deutsch: offene Daten) werden Daten bezeichnet, die jedermann ohne Einschränkung einsehen und benutzen darf. Darunter fallen auch beispielsweise Geodaten, Statistiken oder Verkehrsinformationen

Open Source Open Source (zu Deutsch: offene Quelle) beschreibt eine Software dessen Quelltext öffentlich zur Verfügung steht und von Dritten eingesehen und, je nach Lizenz, geändert und genutzt werden kann.

Pull-Request Als Pull-Requests werden Anträge auf Codezusammenführung bezeichnet, der Begriff wird häufig im Zusammenhang mit verteilten Versionskontrollsytemen verwendet.

Single-Point-Of-Failure. Als Single-Point-Of-Failure (zu Deutsch: einzelne Stelle des Scheiterns) wird ein Teil eines informationstechnischen Systems bezeichnet, dessen Ausfall zu einem Ausfall des gesamten technischen System führt, bezeichnet

zeitgemäße Verschlüsselung Unter zeitgemäßer Verschlüsselung verstehen wir den Einsatz von vorhandenen, weit verbreiteten und allgemein als sicher anerkannten Protokollen, Dateiformaten und Standards.