Landtag von Baden-Württemberg **Drucksache 17 / 4923**

17. Wahlperiode **12.6.2023**

Mitteilung

der Landesregierung

Bericht der Landesregierung zu einem Beschluss des Landtags; hier: Denkschrift 2022 des Rechnungshofs zur Haushalts- und Wirtschaftsführung des Landes Baden-Württemberg – Beitrag Nr. 7: Mobile Endgeräte in der Landesverwaltung

Landtagsbeschluss

Der Landtag hat am 10. November 2022 folgenden Beschluss gefasst (Drucksache 17/3307 Abschnitt II):

Die Landesregierung zu ersuchen,

1. die Mobilstrategie des Landes fortzuschreiben;

2. alle mobilen Endgeräte und die Mobilfunkverträge zentral, möglichst bei der BITBW, zu verwalten;

3. entsprechend den Empfehlungen des Rechnungshofs landesweit geltende Vorgaben zur Beschaffung und für die Nutzung mobiler Endgeräte zu machen und dabei die Bandbreite der Hersteller und Modelle einzuschränken;

4. mit Blick auf die Bedrohungslage die Informationssicherheit von mobilen Endgeräten weiter zu verbessern;

5. dem Landtag über das Veranlasste bis 30. Juni 2023 zu berichten.

Eingegangen: 12.6.2023 / Ausgegeben: 26.6.2023

Bericht

Mit Schreiben vom 12. Juni 2023, Az.: 0451.1-3/7/2, berichtet das Staatsministerium wie folgt:

Zu Ziffer 1:

Die IT Baden-Württemberg (BITBW) strebt entsprechend den Empfehlungen des Rechnungshofes aus dem Jahr 2021 mit ihrer Mobilstrategie eine Einschränkung der Produktvielfalt von mobilen Endgeräten an. Gleichermaßen wird eine zentrale Verwaltung und Steuerung über ein Mobile Device Management (MDM) realisiert. Hierfür stellt die BITBW den Service iOS Enterprise Mobility Management (EMM) zur Verfügung. Dieser verfügt über unterschiedliche Szenarien, um auf unterschiedliche Bedürfnisse innerhalb der Landesverwaltung eingehen zu können. So können die dienstlichen Endgeräte entweder rein dienstlich (COBO – Corporate Owned, Business Only Szenario) oder dienstlich und privat (COPE – Corporate Owned, Personally Enabled Szenario) genutzt werden, ohne Sicherheitsstandards oder die Benutzerfreundlichkeit signifikant einzuschränken. Private Geräte (BYOD – Bring Your Own Device) werden für den iOS EMM Dienst u. a. aus rechtlichen Gründen abgelehnt. Alle mit iOS EMM ausgestatteten Endgeräte sind im Apple Business Manager (ABM) einzutragen, um eine ideale Verwaltung der Geräte über das MDM zu ermöglichen.

Mittels des im Jahr 2022 geschlossenen Mobilfunkrahmenvertrags wird der Fokus auf Apple Hardware in Bundles gelegt. Mit Apple wird ein Hersteller, der sowohl Hardware als auch ein einheitliches und sicheres Betriebssystem für Smartphones (iOS) und Tablets (iPadOS) anbietet, fokussiert. Anders als in der Ausschreibung bis zum Jahr 2022 sind für Hauptkunden der BITBW nicht mehr alle Geräte uneingeschränkt über die Provider bestellbar. Dies ist unter anderem in den Webshops der Provider realisiert. Auch werden die Geräte durch die Provider im Device Enrollment Program (DEP) des ressortspezifischen ABM eingetragen. Dieser ist jeweils mit dem MDM der BITBW verknüpft.

Neben der kontinuierlichen Weiterentwicklung des seit dem Jahr 2021 im Servicekatalog enthaltenen iOS EMM Services, wurden auch weitere Services angepasst. So ist der Service Mobile Management mit Pushmail (MMP) für Neukunden seit dem Jahr 2023 nicht mehr buchbar. Der Dienst Mobile Management Service (MMS) ist für Neukunden ebenfalls nicht mehr für iOS bestellbar, sondern fokussiert sich auf vereinzelt betriebene Android Geräte.

Die Entwicklung des iOS EMM Dienstes seit dem Jahr 2021 zeigt den Erfolg des Dienstes und das Voranschreiten der Mobilstrategie. So ist eine Steigerung von einer Behörde mit 16 Nutzenden im Januar 2021 auf 29 Ressorts/Dienststellen und 1 834 Nutzende im März 2023 zu verzeichnen. Dies zeigt auch folgende Grafik:

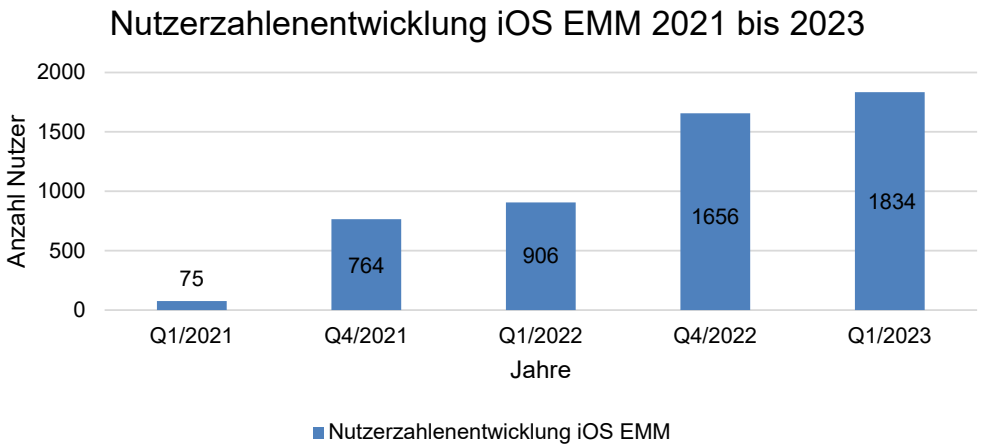

Abbildung 1: Nutzerzahlenentwicklung iOS EMM Service (Service 65) 2021 bis 2023

Doch nicht nur die Nutzerzahlen, sondern auch die Verteilung über alle von der BITBW betreuten Kunden hinweg zeigt, dass die im MDM der BITBW betreuten Endgeräte hauptsächlich mit dem iOS EMM Dienst ausgestattet sind. Nach den größeren Ministerien folgen im Jahr 2023 die kleineren Dienststellen und Ressorts. Folgende Grafik zeigt die Verteilung der mobilen Dienste der BITBW für alle Kunden.

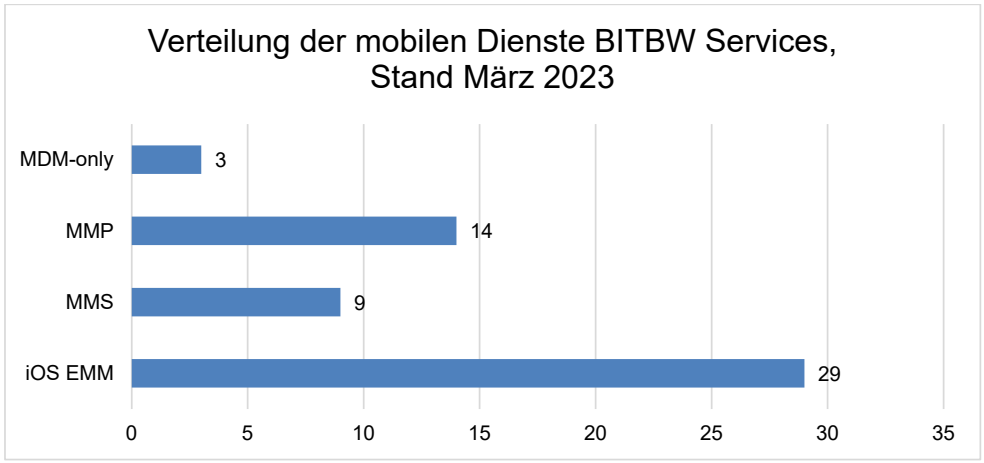

Abbildung 2: Ressortverteilung mobile Dienste BITBW nach Anzahl der Kunden

In der Grafik und in der weiteren Erörterung wird nur von den im MDM registrierten Geräten ausgegangen. Alle nicht im MDM registrierten und somit nicht durch die BITBW verwalteten Geräte bei den Kunden liegen außerhalb des Einflussbereichs der BITBW.

Der iOS EMM Dienst basiert auf einem EMM System. Dieses beinhaltet neben dem MDM, wie in der Beschlussempfehlung bzw. der Denkschrift des Rechnungshofes empfohlen, auch das Mobile Application Management (MAM).

MAM bezogen auf mobile Endgeräte meint dabei unter anderem die eingesetzten Secure Container (Secure Mail, Secure Web) um auf Ressourcen zuzugreifen. Darüber hinaus erfolgt die Beschaffung von Apps über das Volume Purchase Program (VPP) der ABM. Die Zuweisung der Apps in den verwalteten Bereich der Endgeräte via MDM gewährleistet eine selektive Verteilung, Sicherung und das Lebenszyklusmanagement von Apps (bspw. Aussonderung von Apps, die keinen Herstellersupport mehr haben).

Im Rahmen der Mobilstrategie werden auch die Weiterentwicklungsprojekte im mobilen Bereich ausschließlich mit dem iOS EMM Dienst als Basis realisiert. So ist der iOS EMM Dienst bspw. für die mobile App der E-Akte BW (VIS-Mobile Client-iOS) oder auch für die Skype for Business mobile App die Voraussetzung. Auch wird bei derzeit durchgeführten Projekten der Polizei der iOS EMM Dienst als Basis genutzt. Dies sorgt für eine weitere Attraktivitätssteigerung des Standard-Dienstes.

Zu Ziffer 2:

Gemäß der Empfehlung zur zentralen Verwaltung der Mobilfunkverträge wurde im Jahr 2022 ein neuer Mobilfunkrahmenvertrag geschlossen (vgl. Antwort zu Ziffer 1). Mit diesem wurde nicht nur die grundsätzliche Mobilstrategie des Landes fokussiert, sondern auch eine Dual Carrier Strategie mit den zwei großen Carriern in Deutschland erreicht. Aus diesem Rahmenvertrag können alle bezugsberechtigten Kunden der BITBW abrufen und profitieren. Für diese Kunden werden einheitliche Vorgaben gemacht. Die BITBW steht in engem Austausch mit den Providern und definiert entsprechend einheitliche Prozesse. Hierbei wird auch die zentrale Verwaltung der Endgeräte in einem System der BITBW ermöglicht (Asset Management in USU Valuemation).

Bei den beiden Providern können Bundles bestellt werden, die aus aktuellen Apple Endgeräten mit einer SIM-Karte des Providers und als weitere Serviceleistung mit dem iOS EMM Service der BITBW ausgestattet werden. Die Tarife umfassen dabei attraktive Preise und führten bereits zu einem weiteren Anstieg der Nachfrage nach dem iOS EMM Dienst. Zudem wurde definiert, dass die Provider die ABM DEP Eintragung für alle iOS EMM Geräte übernehmen (Grundvoraussetzung für die Nutzung des iOS EMM Dienstes).

Zu Ziffer 3:

Mit dem Mobilfunkrahmenvertrag und dem Fokus auf den iOS EMM Dienst gibt die BITBW eine klare Empfehlung in Richtung Apple-Produkte. Eine Einschränkung auf Modelle wird dahingehend realisiert, dass lediglich aktuelle Geräte (mit iOS/iPad OS Updates) bei den Providern bestellbar sind. Der iOS EMM Dienst ist lediglich für Apple-Endgeräte konzipiert und schreibt ebenfalls eine bestimmte aktuelle Betriebssystemversion vor.

Die Strategie der BITBW spiegelt sich auch in einer Auswertung vom MDM wider:

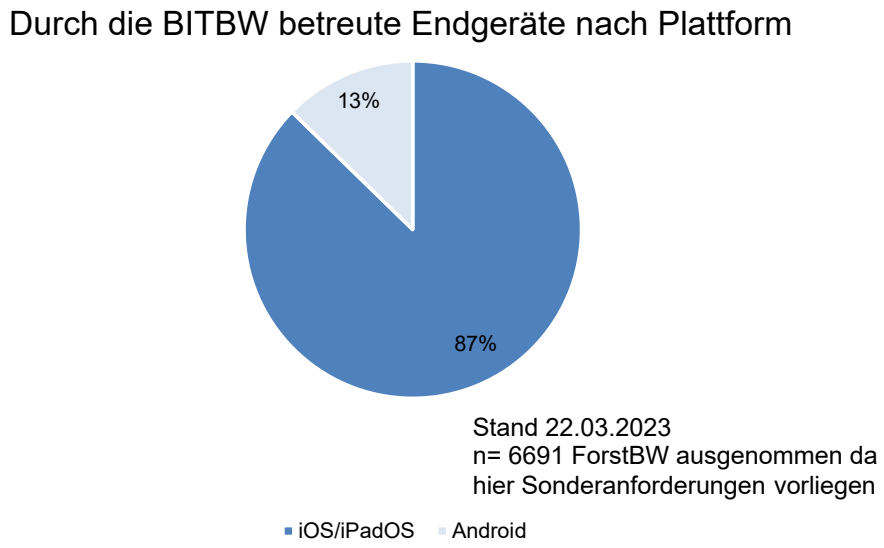

Abbildung 3: Über BITBW-MDM betreute Endgeräte nach Plattform

Eine weitere Reduktion der Android Endgeräte wird durch die attraktiven Preise und den Fokus auf Apple-Hardware im Rahmenvertrag Mobilfunk erwartet. Zudem wird der Anstieg an Apple-Endgeräten durch die beschriebenen Weiterentwicklungsprojekte für mobile Endgeräte mit iOS EMM als Basis forciert. So kann ein Tarif mit Apple-Hardware mit Schutzfolie und -hülle sowie dem iOS EMM Dienst direkt für User bestellt werden (weitere Staging-Leistungen für Zero Touch Ansatz). Mit dem Zero Touch Ansatz verfolgt die BITBW eine vollständige und automatisierte Inbetriebnahme von Apple-Endgeräten ohne Zutun des Kunden. Neben der Zuordnung der Endanwenderin bzw. des Endanwenders zum Service sind auch Staging Leistungen (Sichtschutzfolie und Schutzhülle Gerät) buchbar. Das Endgerät kann von der Endanwenderin bzw. dem Endanwender bei Übergabe direkt in Betrieb genommen werden. Diese Sonderleistungen (i. S. v. Services) sind für Android bewusst nicht realisiert.

Im neuen Mobilfunkrahmenvertrag sind darüber hinaus nur besondere Dienststellen mit speziellen Anforderungen an Robustheit von dem Apple-Fokus ausgenommen. Dienststellen können nur auf Nachfrage andere Geräte mit einem anderen Betriebssystem (Android) bei den Providern bestellen.

Bei den Providern ist neben der Beschaffung der Hardware auch eine BSI-konforme Löschung sowie eine Rückkaufoption realisiert. Somit wird der komplette Lebenszyklus von der Beschaffung bis zur Entsorgung des Endgeräts berücksichtigt.

Dennoch ist zu erwähnen, dass die Beschaffung der mobilen Endgeräte und die Entscheidung bei den Ressorts liegt und daher nicht vollumfänglich durch die BITBW gesteuert werden kann.

Zu Ziffer 4:

Durch die oben genannten Punkte wird die Informationssicherheit mobiler Endgeräte automatisch weiter verbessert. Der iOS EMM Dienst ist BSI-konform gestaltet, weist ein umfangreiches Sicherheitskonzept auf und berücksichtigt die entsprechenden BSI-Bausteine im Pflichtenheft. Dies zeigt auch folgende Grafik:

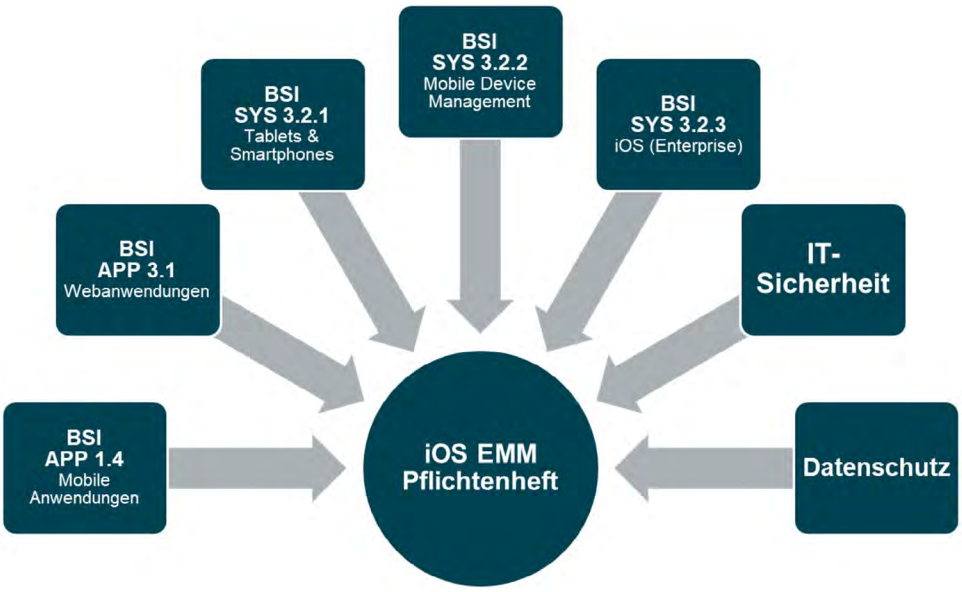

Abbildung 4: Bestandteile Pflichtenheft iOS EMM Dienst

Die Sicherheit ist sowohl im Szenario COBO als auch COPE gewährleistet.

Zur Einhaltung der Sicherheit des Dienstes werden unterschiedliche Maßnahmen ergriffen, so fanden bspw. Gremienauftritte statt, um für die Bedeutung des Themas iOS-Updates zu sensibilisieren und auf die notwendige Aussonderung veralteter Geräte hinzuweisen. Mit diesen Maßnahmen soll das MDM aktuell gehalten und die Sicherheit gewährleistet werden. Apple-Updates unterliegen gewissen Vorbedingungen, daher ist deren Installation auf den Endgeräten nicht zentral steuerbar (Installation nicht automatisiert über MDM möglich). Jedoch wird von der BITBW ein Test neuer Versionen durchgeführt und eine Informationsmail an alle Nutzenden bei einem neuen verfügbaren Update gesendet mit der Aufforderung, dieses zu installieren. Zusätzlich wird derzeit ein Plan ausgearbeitet, die Aussonderung/Sperrung veralteter Geräte zu forcieren.

Neben der Option, Gerätestände und -aktivitäten auf dem MDM zu betrachten, werden hier auch Apps verteilt, die zuvor im VPP beschafft wurden. Um die Sicherheit, insbesondere in Bezug auf zentral verteilte Apps, zu erhöhen, hat die BITBW eine Ausschreibung zum Thema Appvalidierung durchgeführt. Der hierdurch erreichte Rahmenvertrag zur Appvalidierungslösung für die Landesverwaltung bietet diverse Möglichkeiten, um mit Hilfe eines Webportals Risiken von Apps zu identifizieren und für diese bei Bedarf ein „Blacklisting“ (die Verwendung von Negativ-Listen; bedeutet, dass die Installation von ausgewählten Apps über das MDM verhindert wird) vorzunehmen. Die Installation von Apps über den Apple App Store ist unkritisch, da die Apps vor Veröffentlichung einer Prüfung von Apple unterliegen, im iOS EMM Dienst die Datenseparation greift und das MDM „Black-listing“ vorgenommen wird.

Vom MDM verteilte und verwaltete Apps sind von der Endanwenderin bzw. dem Endanwender im Secure Hub zu finden. Für die hier als erforderlich markierten Apps werden dabei eine automatische Installation und automatische Updates umgesetzt. Weiterhin werden einheitliche Vorgaben für den Sperrcode und den Sperrbildschirm realisiert, womit bspw. auch die Darstellung von Nachrichten umfasst ist. Auch ist ein Fernlöschen bspw. bei Verlust der Endgeräte Pflicht. Zum Thema „Messenger Dienst“ bietet die BITBW derzeit ein optionales Angebot an, da es sich um einen kostenpflichtigen Dienst bei einem Drittanbieter handelt. Perspektivisch ist auch hier eine Ausschreibung eines Rahmenvertrages für die Landesverwaltung denkbar.

Wie bereits beschrieben wird die Sicherheit nicht nur im Betrieb der Geräte betrachtet, sondern auch bei der Aussonderung von Geräten. Insbesondere die Option der BSI-konformen Löschung, welche über die Provider des Mobilfunkrahmenvertrags abgedeckt ist, sei hier zu nennen.

Zusammengefasst kann festgehalten werden, dass die BITBW mit dem Standard-Dienst iOS EMM und weiteren Aktivitäten wie dem Mobilfunkrahmenvertrag die Mobilstrategie des Landes weiter vorantreibt. Dabei wird neben Sicherheit auch ein hohes Maß an Benutzerfreundlichkeit realisiert und die Herstellervielfalt weiter eingeschränkt.