Auszug aus

Denkschrift 2022

zur Haushalts- und Wirtschaftsführung
des Landes Baden-Württemberg

Beitrag Nr. 7

Mobile Endgeräte in der Landesverwaltung

Baden-Württemberg

RECHNUNGSHOF

Mobile Endgeräte in der Landesverwaltung

Der Einsatz und der Betrieb mobiler Endgeräte werden weitgehend dezentral durch die einzelnen Ressorts bzw. Dienststellen gesteuert. Diese Praxis weist unter Sicherheits- und Datenschutzaspekten, aber auch mit Blick auf die Wirtschaftlichkeit erhebliche Schwächen auf. Durch eine Zentralisierung des Managements bei der IT Baden-Württemberg und einheitliche Vorgaben zur Nutzung mobiler Endgeräte könnten Sicherheitsrisiken verringert und die Wirtschaftlichkeit verbessert werden. Eine einheitliche Produktstrategie würde das Erreichen dieser Ziele unterstützen.

1 Ausgangslage

In der Landesverwaltung Baden-Württemberg werden zunehmend mobile Endgeräte (Tablets und Smartphones) eingesetzt. Die Corona-Pandemie hat die Bedeutung des mobilen Arbeitens nochmals verstärkt. Mit dem Einsatz solcher Geräte steigen auch die Herausforderungen hinsichtlich der Informationssicherheit und des Datenschutzes. Die aktuelle Mobilstrategie des Landes datiert aus dem Jahr 2017.

Der Rechnungshof hat den Einsatz und den Betrieb mobiler Endgeräte in der Landesverwaltung mit dem Schwerpunkt Geräte- und Applikationsmanagement, Beschaffung, Informationssicherheit sowie Dienstvorschriften zur Nutzung geprüft. Er hat hierzu bei den Ministerien und nachgeordneten Dienststellen (außer den Hochschulen) unter anderem die Zahl der Geräte erhoben; Ende 2019 waren etwas mehr als 4.800 Geräte verfügbar. Hinzu kommen rund 5.000 mobile Endgeräte, welche die Polizei Anfang 2021 neu beschafft hat.

2 Prüfungsergebnisse

2.1 Management von Geräten, Apps und Mobilfunkverträgen

Mobile Endgeräte können in einem Mobile Device Management (MDM) verwaltet werden. Dies ermöglicht insbesondere eine einheitliche standardisierte Konfiguration und Inventarisierung von mobilen Endgeräten. Der Einsatz eines MDM ist insbesondere angezeigt, wenn - wie in der öffentlichen Verwaltung - sicherheitsrelevante Daten verarbeitet werden. Die IT Baden-Württemberg (BITBW) bietet den Dienststellen des Landes über ihren IT-Servicekatalog das Management von mobilen Endgeräten an.

Allerdings wurde nur knapp ein Viertel aller zum Stichtag Ende 2019 gemeldeten Geräte durch ein MDM der BITBW verwaltet, rund 40 Prozent in anderen, nicht von der BITBW bezogenen MDM. Die Polizei lässt ihre 2021 neu beschafften mobilen Endgeräte in einem MDM pflegen, das von einem privaten Dienstleister betrieben wird.

Eine gut gemanagte mobile IT verfügt auch über ein Mobile Application Management (MAM), das ein Lizenzmanagement, die Verteilung, Sicherung und das Lebenszyklusmanagement von Apps ermöglicht. Etwa 13 Prozent aller gemeldeten Geräte - ohne die neu beschafften der Polizei - waren in einem MAM der BITBW eingepflegt, etwa die gleiche Anzahl wird in anderen MAM verwaltet. Die Apps der restlichen Geräte werden nicht in einem System gemanagt, wodurch - bei Wahlfreiheit hinsichtlich der Installation von Apps - ein Sicherheitsrisiko entstehen kann.

Die für den Betrieb mobiler Endgeräte in der Regel notwendigen Mobilfunkverträge werden fast ausschließlich über einen Rahmenvertrag des Landes mit einem Mobilfunkanbieter geschlossen. Für deren Verwaltung hat die BITBW eine Lösung entwickelt, die sie aber nur für die von ihr selbst genutzten Verträge einsetzte.

Die Erhebung zeigte auch, dass das Spektrum der eingesetzten Modelle sehr breit ist. Insgesamt waren mehr als 100 unterschiedliche Modelle von mehr als 20 verschiedenen Herstellern im Einsatz. Dies führt aufgrund der verschiedenen Konfigurationsmöglichkeiten zu erhöhtem Aufwand für deren Verwaltung einschließlich der für die Sicherheit erforderlichen Maßnahmen.

Das Land hat angesichts der weitgehend dezentralen Verwaltung keinen Überblick über die Anzahl, Vielfalt, Nutzung und Sicherheitsstandards der eingesetzten mobilen Endgeräte. Eine Zentralisierung des Managements oder zumindest eine Anbindung von Managementsystemen Dritter für Geräte, Apps und Mobilfunkverträge an die übergeordneten IT-Service-Managementwerkzeuge der BITBW ist dringend geboten. Sicherheitsbedrohungen durch eingesetzte mobile Endgeräte können dann früher und besser erkannt und entsprechende Vorkehrungen zu deren Abwehr getroffen werden. Zudem könnten Beschaffungsprozesse und das Vertragsmanagement wirtschaftlicher gestaltet werden.

2.2 Vorgaben für die Nutzung mobiler Endgeräte

Es gibt keine landesweit einheitlichen Vorgaben für den Einsatz und die Nutzung mobiler Endgeräte. Die einzelnen Ressorts und Dienststellen handeln unterschiedlich. So wird beispielsweise bei der Frage, ob private mobile Endgeräte auch zu dienstlichen Zwecken und ob dienstliche Geräte auch zu privaten Zwecken eingesetzt werden dürfen, trotz grundsätzlich gleicher Problematik sehr uneinheitlich verfahren.

Auch einheitliche Vorgaben zum Umgang mit auszusondernden Geräten fehlen. In der Folge werden Aspekte wie Aussonderungskriterien, Anforderungen an die Datenlöschung und Verwertung der Geräte in den Ressorts unterschiedlich gehandhabt.

In der Landesverwaltung werden verschiedene Messenger(-Apps) eingesetzt. Bei deren Einsatz ist zum einen unter Sicherheitsgesichtspunkten Vorsicht geboten, zum anderen sind Datenschutzvorgaben zu beachten. Bei verschiedenen verwendeten Messengern, die häufig vorinstalliert sind, können diese nicht oder nicht ohne Weiteres eingehalten werden. Vorgaben für eine einheitliche Handhabung fehlen auch hier.

2.3 Informationssicherheit

Die Betriebssysteme der eingesetzten mobilen Endgeräte sind teilweise völlig veraltet. Es sind Versionen im Einsatz, für die von den Herstellern keine Sicherheitsupdates mehr zur Verfügung gestellt werden. Für die bei der BITBW gemanagten Geräte war zwar ein - aus dem MDM-System abgeleiteter - Mindeststand vorgegeben, der aber nicht zwingend dem vom Hersteller des Betriebssystems empfohlenen Versionsstand entspricht.

Veraltete, nicht mehr updatefähige Geräte, mit denen ein Zugriff auf dienstliche Informationen möglich ist, sind ein Sicherheitsrisiko. Um solche Risiken zu verringern, ist die Definition von Mindestständen für die eingesetzten Betriebssysteme und deren fortlaufende Anpassung entsprechend der technischen Entwicklung erforderlich.

Derzeit ist die BITBW nicht einmal für die von ihr verwalteten Geräte berechtigt, verpflichtende Updates auf den mobilen Endgeräten zu initiieren. Akute Sicherheitslücken des Betriebssystems oder von Apps können daher nicht zentral geschlossen werden, vielmehr müssen die jeweils verwaltenden Dienststellen dezentral tätig werden. Hierdurch können sich Rückwirkungen auf die gesamte IT des Landes ergeben.

Die unterschiedliche Handhabung wirkt sich auch bei weiteren Sicherheitsaspekten aus. Die von der BITBW gemanagten Geräte und SIM-Karten wiesen durch eine standardisierte Inbetriebnahme erhöhte Sicherheitsmerkmale auf. Bei den in den Ressorts eingesetzten Geräten zeigten sich dagegen Mängel in der sicherheitsrelevanten Konfiguration. Unterschiedlich gehandhabt wird auch die Bereitstellung von Apps. Häufig ist der Zugriff auf die Hersteller-Appstores uneingeschränkt möglich. So können die Endanwender jegliche App installieren, auch wenn diese sicherheitskritisch ist.

2.4 Beschaffung

Die mobilen Endgeräte werden durchweg von den Dienststellen dezentral beschafft. Für Android-basierte Geräte können sie sich aus dem Warenkorb des Mobilfunk-Partners des Landes bedienen. Für iOS-Geräte besteht ein eigener Rahmenvertrag mit einem Großhändler, der aber von den Dienststellen nicht verpflichtend genutzt werden muss.

Im Prüfungsverfahren gaben einige Dienststellen an, dass der Bezug von Geräten auf dem freien Markt günstiger sei. Dies kann auch damit zusammenhängen, dass der aktuelle Rahmenvertrag den üblichen Preisverfall von neuen Geräten nach erfolgter Markteinführung nur eingeschränkt berücksichtigt, weil der Preis an den Herstellershop und nicht an den Marktpreis gekoppelt ist.

Bei einer ausschließlich auf dem reinen Gerätepreis basierenden Beschaffungsentscheidung bleibt gegebenenfalls unberücksichtigt, dass bei der Nutzung von Rahmenverträgen auch Mehrwerte entstehen, die die Wirtschaftlichkeit beeinflussen. So pflegt der Auftragnehmer des genannten Rahmenvertrages Informationen der iOS-Geräte in den Business Manager des betreffenden Herstellers ein - eine Leistung, die ansonsten von der Verwaltung selbst vorgenommen werden müsste, was aber regelmäßig nicht erfolgt.

Aus dem Rahmenvertrag für iOS-Geräte wurden teilweise Geräte von Institutionen außerhalb der Landesverwaltung abgerufen, die nicht bezugsberechtigt waren. Das Land als Auftraggeber wurde hierüber erst mit zeitlicher Verzögerung informiert. Entsprechende unberechtigte Abrufe gehen zu Lasten der bedarfsorientiert ausgeschriebenen Kontingente des Landes. Sie führen deshalb zu einer früher notwendigen erneuten Ausschreibung mit entsprechendem Verwaltungsaufwand und Kosten.

Ein Ressort hatte rund 40 Prozent seines gesamten Gerätebestandes auf Lager. Eine Vorratshaltung in diesem Umfang ist nicht wirtschaftlich. Bei mobilen Endgeräten ist der Preisverfall besonders im ersten Jahr nach der Markteinführung erheblich, teilweise fällt der Verkaufspreis um rund 30 bis 45 Prozent. Zudem verkürzt sich durch Lagerzeiten die Nutzungsdauer, weil nur für eine bestimmte Zeit Updates von den Geräteherstellern angeboten werden.

Eine verkürzte Nutzungsdauer ergibt sich generell auch, wenn Geräte beschafft werden, die zum Zeitpunkt des Kaufs bereits lange auf dem Markt eingeführt waren. Nicht nur aus wirtschaftlichen, sondern auch aus informationssicherheitstechnischen Gründen ist die Aktualität der Hardware und des Betriebssystems beim Kauf zu berücksichtigen.

In einer übergreifenden IT-Strategie könnte mittelfristig an die Nutzung eines einzigen mobilen Gerätes (One-Device) anstatt mehrerer Geräte (Desktop, Laptop, Tablet und/oder Smartphone) gedacht werden. In Anbetracht der technischen Entwicklung mobiler Endgeräte einerseits und zunehmender rein webbasierter IT-Verfahren andererseits könnte sich daraus eine universellere und wirtschaftlichere IT-Ausstattung der Endanwender ergeben.

3 Empfehlungen

Die Landesregierung sollte die Mobilstrategie des Landes vor dem Hintergrund der dynamischen Entwicklung bei der Nutzung von mobilen Endgeräten und der zunehmenden Sicherheitsanforderungen fortschreiben.

3.1 Mobile IT vereinheitlichen und standardisieren

Alle in der Landesverwaltung eingesetzten mobilen Endgeräte sollten durch ein zentrales, bei der BITBW installiertes MDM und MAM verwaltet werden. Das Management von Mobilfunkverträgen sollte eingebunden werden; die BITBW sollte hierzu das von ihr genutzte Verfahren allen Ressorts zur Verfügung stellen. Andere, nicht von der BITBW betriebene Managementumgebungen sollten eingestellt werden, sofern sie nicht im Rahmen von Kooperationen mit dem Bund, anderen Ländern oder Kommunen eingerichtet sind. Die spezifischen Management-Systeme für die im Land eingesetzten mobilen Endgeräte sollten relevante Informationen mit den Werkzeugen des zentralen IT Service-Managements der BITBW synchronisieren.

Die Landesverwaltung sollte die Bandbreite der Hersteller und Modelle der mobilen Endgeräte vorgeben und einschränken. Bestehende Rahmenverträge zur Beschaffung von Hardware sollten, gegebenenfalls durch eine Vor-

gabe in der VwV Beschaffung, verbindlich genutzt werden müssen; Ausnahmen sollten sehr eng begrenzt werden. Die Abgabe von Geräten aus Rahmenverträgen an Nicht-Bezugsberechtigte sollte explizit untersagt und Verstöße z. B. durch eine Vertragsstrafe sanktioniert werden.

Bei der Beschaffung von mobilen Endgeräten sollte aus wirtschaftlichen und sicherheitstechnischen Gründen die Aktualität der Hardware und des Betriebssystems sowie die Updateversorgung maßgeblich berücksichtigt werden.

Die BITBW sollte die technische und funktionale Möglichkeit eines One-Device-Konzeptes, also des Einsatzes eines einzigen Gerätes sowohl am Arbeitsplatz als auch zur mobilen Nutzung, laufend beobachten und mittelfristig eine Umsetzung auch unter wirtschaftlichen Aspekten prüfen.

3.2 Einheitliche Vorgaben schaffen

Für die regelkonforme Nutzung der Geräte sollten einheitliche landesweite Vorgaben etabliert werden, etwa in Form einer verbindlichen „Dienstanweisung für die Nutzung von mobilen Endgeräten“. Darin sollten alle Aspekte des Lebenszyklus berücksichtigt werden, also von der Beschaffung bis zur Aussonderung.

Es sollten nur dienstliche, in ein MDM eingebundene mobile Endgeräte zu dienstlichen Zwecken oder in Ausnahmefällen auch zum abgesicherten privaten Gebrauch eingesetzt werden dürfen. Der Lagerbestand an mobilen Geräten sollte möglichst gering gehalten werden.

Die Landesverwaltung sollte die Auswahl von Messenger-Apps eng begrenzen. Hierzu sollte idealerweise nur ein einziger datenschutzkonform nutzbarer Messenger ausgewählt und zugelassen werden.

3.3 Informationssicherheit verbessern

Die Informationssicherheit sollte durch einen einheitlichen Mindeststand an Betriebssystem-Versionen gewährleistet werden. Geräte, die diesen nicht erfüllen, sollten ausgesondert, zumindest aber vom Zugang auf dienstliche Informationen ausgeschlossen werden.

Bei besonders sicherheitsrelevanten Updates sollte der BITBW gestattet werden, entsprechende Aktualisierungen zentral auszulösen. Der übergreifende Aspekt von aktuell zu haltenden IT-Systemen könnte in einer Änderung der VwV Informationssicherheit oder in der künftigen Cybersicherheits-Verordnung Berücksichtigung finden.

Die Maßnahmen zur Informationssicherheit sollten erhöht werden. Es sollte verbindlich vorgegeben werden, dass mobile Endgeräte mit einer PIN (Personal Identification Number) und einer Bildschirmsperre versehen sind sowie über die Möglichkeit einer Fernlöschung verfügen. Ein Zugriff auf Hersteller-Appstores sollte unterbunden werden; Apps sollten nur nach Prüfung und Freigabe aus den spezifischen Stores eines MAM bezogen werden können.

Entsprechende Einstellungen mobiler Endgeräte können am besten durch eine standardisierte automatisierte Grundkonfiguration in einem zentralisierten MDM und MAM umgesetzt werden.

4 Stellungnahme des Ministeriums

Das Innenministerium stimmt den Prüfungsergebnissen des Rechnungshofs zu. Es teilt insbesondere die Einschätzung, dass die Mobilstrategie des Landes auf aktuelle Anforderungen fortzuschreiben sei. Der BITBW komme hierbei für die Beschaffung und das Verwalten der Mobilgeräte eine zentrale Rolle zu. Die Möglichkeiten des Mobile Device Managements seien zwischenzeitlich deutlich verbessert und ausgebaut worden. Daher könnten mit neuen Techniken durchaus Szenarien realisiert werden, die zum Zeitpunkt der Prüfung noch nicht möglich gewesen seien. Als Beispiel nennt das Ministerium die private Nutzung von dienstlichen Mobilgeräten, was neuerdings mit der sogenannten COPE-Strategie (d. h. Corporate-Owned, Personally Enabled) ermöglicht werden könne und auch alle sicherheitstechnischen Anforderungen erfülle.