Einsatz mobiler Endgeräte in der Staatsverwaltung

13

Der Einsatz mobiler Endgeräte in der sächsischen Staatsverwaltung erfolgt mit grundlegenden Mängeln bei der Informationssicherheit. Es handelt sich nicht um Einzelfälle.

Das Gebot der Wirtschaftlichkeit und Sparsamkeit der Beschaffung setzt eine Bedarfsermittlung voraus. Diese fehlt häufig.

1 Prüfungsgegenstand

1 Der SRH hat den Einsatz mobiler Endgeräte in der SK und allen Ministerien sowie deren nachgeordneten Behörden und Einrichtungen geprüft.[1] Ziel der Querschnittsprüfung war es, Aussagen über die Ausstattung der Dienststellen mit mobilen Endgeräten, deren Betrieb und Nutzung zu treffen.

2 Aus der Vielzahl unterschiedlicher Geräteklassen hat der SRH für seine Prüfung die Smartphones und Tablets ausgewählt.

3 Bis zum 31.12.2019 waren in den geprüften Stellen 4.898 Smartphones und 898 Tablets für insgesamt mindestens 1,6 Mio. € beschafft worden. Von den 5.796 Geräten waren 5.507 Geräte im Einsatz. Die laufenden Ausgaben für die mobilen Endgeräte betrugen im Hj. 2019 mindestens 2,1 Mio. €.

2 Prüfungsergebnisse

2.1 Istanalyse

4 In den Behörden und Einrichtungen werden mobile Endgeräte verschiedener Hersteller eingesetzt. Den größten Anteil haben mit rd. 69 % Samsung-Geräte. Danach folgen Geräte der Hersteller Apple (rd. 18 %), Nokia (rd. 4 %), Blackberry (rd. 2 %), Huawei (rd. 2 %), Microsoft (rd. 1,7 %), Fujitsu (rd. 1,4 %), Lenovo (rd. 0,5 %) und weitere.

5 Weil in den Behörden und Einrichtungen regelmäßig unterschiedliche Gerätemodelle jedes Herstellers eingesetzt werden, steigt die Gerätevielfalt enorm.

6 **Nach den Angaben der geprüften Stellen sind in der Staatsverwaltung mehr als 280 verschiedene Gerätemodelle im Einsatz.**

7 Dies hat Folgen, denn aus der Gerätevielfalt ergibt sich zwangsläufig eine hohe Vielfalt an eingesetzten Betriebssystemen und damit verbunden eine hohe Anzahl an Betriebssystemversionen.

8 Mit jedem zu unterstützenden Endgerätetyp steigt der Administrationsaufwand, da mit jedem neuen Endgerätetyp neuer Aufwand bei Planung, Konfiguration und technischer Umsetzung an den zentralen Systemkomponenten entsteht.[2]

9 **Die Notwendigkeit der Modell- und Betriebssystemvielfalt sollte deshalb kritisch hinterfragt werden.**

10 **Für den Einsatz mobiler Endgeräte in der sächsischen Staatsverwaltung sollte eine landesweite Produktstrategie erarbeitet und verabschiedet werden, die diese Vielfalt begrenzt.**

---

[1] Nicht in die Prüfung einbezogen wurden der SLT, der SRH, aus dem Ressort des SMI das Landesamt für Verfassungsschutz sowie aus dem Bereich des SMWK die Hochschulen, die Universitätsklinika, die Berufsakademie Sachsen und die Studentenwerke.

[2] Vgl. BSI, Sicheres mobiles Arbeiten, 2016, S. 15.

2.2 Bedarfsermittlung

11 Ausgaben dürfen nur insoweit geleistet werden, wie sie zur wirtschaftlichen und sparsamen Verwaltung erforderlich sind. Eine wesentliche Voraussetzung für die Vergabe von Lieferungen und Leistungen ist deshalb die Ermittlung des tatsächlichen Bedarfs.

12 Nur 67 der geprüften 145 Stellen (46 %) gaben an, Bedarfsermittlungen vor der Beschaffung von Smartphones und Tablets durchgeführt zu haben.

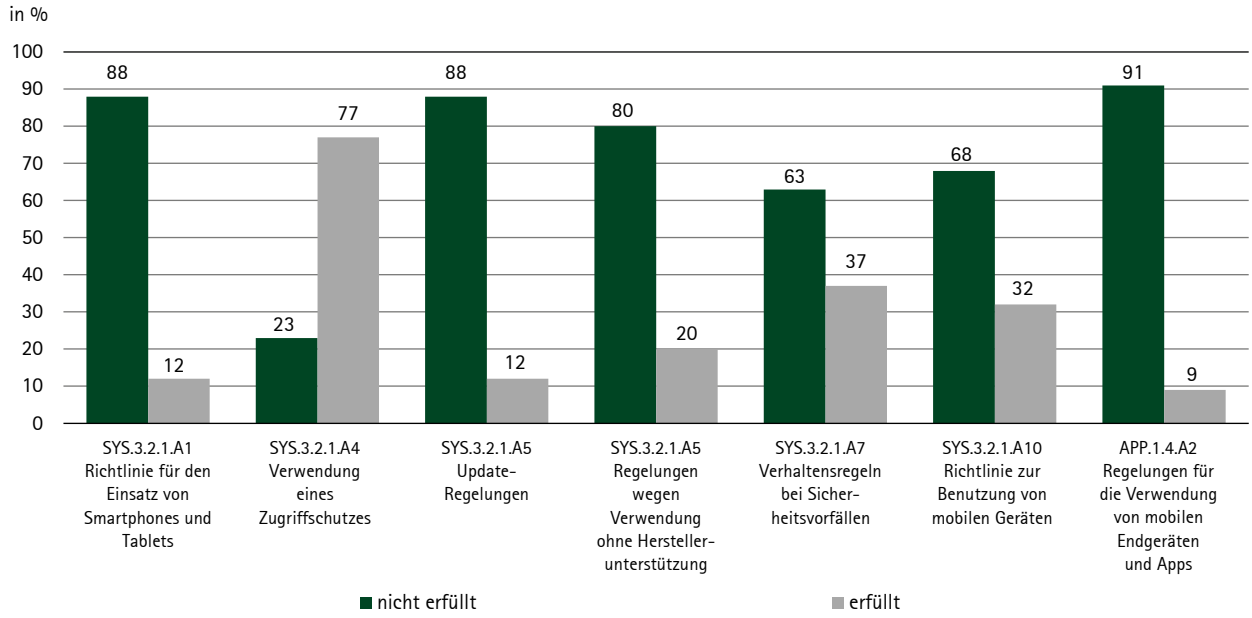
13 **Mehr als die Hälfte der geprüften Stellen hat keine Bedarfsermittlungen durchgeführt. Dies widerspricht dem Grundsatz der Wirtschaftlichkeit und Sparsamkeit.**

2.3 Informationssicherheit – Basisanforderungen

14 In 84 % der geprüften Stellen greifen die dienstlich beschafften Smartphones und Tablets auf dienstliche Informationen der Behörde (E-Mails, Kontaktdaten, Termindaten, Dokumente) zu oder speichern diese. Der Informationssicherheit kommt hier, z. B. wegen der Möglichkeit des Verlusts des Smartphones oder Tablets, eine besondere Bedeutung zu.

15 Um ein angemessenes Informationssicherheitsniveau zu gewährleisten, haben alle staatlichen Stellen die jeweils geltenden Standards und das jeweils geltende IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu berücksichtigen. Der SRH hat in seiner Prüfung den Fokus auf die Erfüllung von BSI-Basisanforderungen („Mussanforderungen") gelegt, wie die Richtlinie für den Einsatz von Smartphones und Tablets, die Update-Regelungen oder die Verhaltensregeln bei Sicherheitsvorfällen (siehe Abbildung 1).

Abbildung: Erfüllungsgrad von BSI-Anforderungen



Quelle: Angaben der geprüften Stellen.

16 Die für den Einsatz mobiler Endgeräte in der sächsischen Staatsverwaltung maßgebenden Anforderungen des BSI wurden häufig nicht erfüllt.

17 So wurde gegen fast alle Basisanforderungen des BSI, die der SRH in seine Prüfung einbezogen hat, in der Mehrzahl der Dienststellen verstoßen. Es handelt sich nicht um Einzelfälle. Verstöße gibt es in allen Ressorts.

18 **Der Einsatz mobiler Endgeräte in der sächsischen Staatsverwaltung erfolgt mit grundlegenden Mängeln bei der Informationssicherheit.**

19 So muss z. B. eine Institution nach der Basisanforderung „SYS 3.2.1.A1", bevor sie Smartphones oder Tablets bereitstellt, betreibt oder einsetzt, eine generelle Richtlinie im Hinblick auf die Nutzung und Kontrolle der Geräte festlegen. Hierbei muss u. a. festgelegt werden, wer auf welche Informationen der Institution zugreifen darf.

20 **Etwa 88 % der geprüften Stellen hatten zwar keine Richtlinie im Sinne des BSI festgelegt, setzten jedoch rd. 1.500 mobile Endgeräte ein.**

2.4 Mobile Device Management[3]

21 Der Einsatz mobiler Endgeräte birgt eine Vielzahl von Risiken in sich (z. B. Verlust oder Manipulation von Smartphones und Tablets, fehlende Betriebssystem-Updates, Software-Schwachstellen in Anwendungen oder Schadprogramme).

22 Diese Risiken können durch ein MDM - ein zentrales Management von mobilen Endgeräten - minimiert werden. Durch ein MDM können Sicherheitsstandards und Konfigurationsparameter wirksam auf allen Endgeräten einer Einrichtung durchgesetzt werden. Bei Diebstahl oder Verlust können mobile Endgeräte aus der Ferne gelöscht bzw. in den Werkszustand zurückgesetzt werden.

23 78 % der geprüften Stellen verwalten mobile Endgeräte nicht über eine MDM-Lösung. Dies betrifft 1.250 im Einsatz befindliche Smartphones und 313 Tablets. Das ist etwa ein Drittel aller gemeldeten mobilen Endgeräte.

24 **Der SRH empfiehlt die Nutzung eines MDM, um den vielfältigen Bedrohungen und Risiken für die Informationssicherheit besser zu begegnen.**

25 Der Staatsbetrieb Sächsische Informatik Dienste (SID), als zentraler IT-Dienstleister, betreibt eine MDM-Lösung und bietet diese den Behörden zur Nutzung an, um ihre mobilen Endgeräte selbst administrieren zu können.

26 Neben dem MDM des zentralen IT-Dienstleisters gibt es eine Vielfalt an MDM-Lösungen in der Staatsverwaltung. Es sind in 10 der geprüften Stellen weitere 8 MDM-Lösungen anderer Hersteller im Einsatz.

27 **Die Behörden und Einrichtungen sollten kritisch prüfen, ob diese Vielfalt an unterschiedlichen MDM-Lösungen notwendig ist.**

28 Der zentrale Betrieb eines MDM ist nach der Positivliste über IT-Leistungen des SID eine Leistungspflicht mit Kontrahierungszwang. Das heißt, die Behörden und Einrichtungen sind verpflichtet, diese IT-Leistungen dem SID anzudienen und von ihm abzunehmen. Die VwV SID[4] lässt jedoch viele Ausnahmen zu.

29 Die Folge dieser umfassenden Ausnahmeregelung ist der oben dargestellte bunte Strauß an unterschiedlichen MDM-Lösungen einerseits und der parallele Betrieb der gleichen MDM-Software an mehreren Orten andererseits.

30 Durch die Aufteilung von IT-Aufgaben - weg vom zentralen IT-Dienstleister - entsteht ein unwirtschaftlicher Mehraufwand. Lösungen zur Mobilgeräteverwaltung sowie entsprechendes Fachpersonal müssen mehrfach vorgehalten werden.

31 **Die Ressorts sollten bedenken, ob sie wirklich ausreichend IT-Personal haben, um es für die Bearbeitung einer Aufgabe einzusetzen, die der SID gemäß VwV SID für sie betreibt.**

3 Folgerungen

32 Für den Einsatz mobiler Endgeräte in der sächsischen Staatsverwaltung sollte eine Produktstrategie erarbeitet und verabschiedet werden. Ziel dieser Strategie muss sein, die Vielfalt an Gerätetypen und Betriebssystemen zu reduzieren.

---

[3] MDM = Mobile Device Management: Management/Verwaltung mobiler Endgeräte

[4] Verwaltungsvorschrift der Sächsischen Staatsregierung über den Staatsbetrieb Sächsische Informatik Dienste vom 05.04.2019.

33 Die festgestellten Defizite im Bereich Informationssicherheit sind abzustellen.

34 Der SRH empfiehlt die Nutzung eines MDM beim zentralen IT-Dienstleister. Ausnahmen davon sollten begründet und eng begrenzt sein.

4 Stellungnahmen

35 Die SK und die Ministerien hatten keine Einwände oder Bedenken zur Sachdarstellung des SRH.

36 Die SK und der SID stimmten den Aussagen und Schlussfolgerungen im Jahresbericht ausdrücklich zu. Die Betrachtung sollte perspektivisch auf weitere mobile Endgeräte ausgedehnt werden. Das Thema sei der SK ein besonderes Anliegen, da im Rahmen des direkt beim Amtschef der SK und CIO[5] des Freistaates Sachsen verorteten Programms proSID das Ziel verfolgt werde, das Clientmanagement für den Regierungscampus beim SID zu bündeln und dadurch sowohl die Geräteverwaltung als auch die Gerätelandschaft zu konsolidieren.

37 SMS und SMWK begrüßten eine Reduzierung der Anzahl an Gerätemodellen und Betriebssystemen grundsätzlich, um diese auf ein den jeweiligen Anforderungen gerecht werdendes Minimum zu begrenzen. Das SMWA hat der Empfehlung zur Erarbeitung und Verabschiedung einer Produktstrategie zugestimmt.

38 Das SMEKUL wies auf das Ziel des Geschäftsbereiches hin, ein Maximum an Standardisierung hinsichtlich Geräten und Infrastruktur zu erreichen, Ausnahmen zu minimieren und damit den Anforderungen und Aufgaben hinsichtlich Administration, Sicherheit und Wirtschaftlichkeit gerecht zu werden.

39 Zum Thema Informationssicherheit erklärte das SMWK, der Jahresbericht beleuchte zentrale Themen zum Einsatz mobiler Endgeräte. Im SMWK sei zwischenzeitlich bspw. eine Richtlinie zur Nutzung dienstlicher Smartphones und Tablets erlassen worden, welche die Forderung aus dem BSI-Grundschutz erfülle.

40 Das SMS plant die Umstellung und Aktualisierung der Sicherheitsrichtlinien. Der wirtschaftliche Aspekt sowie die Chance, vielfältigen Bedrohungen und Risiken besser zu begegnen, seien auch die Gründe für die Entscheidung des SMS und der Einrichtungen im Geschäftsbereich zur Nutzung eines MDM. Die Auffassung des SRH, das Dienstleistungsangebot des SID beim Betrieb des MDM zu nutzen, werde geteilt.

5 Schlussbemerkung

41 Behörden und Einrichtungen haben die Hinweise des SRH zu den Verstößen gegen die Basisanforderungen des BSI aufgegriffen und mit der Umsetzung von Maßnahmen begonnen, diese teilweise schon umgesetzt oder deren Umsetzung zugesagt.

42 In diesem Prozess dürfen die Behörden und Einrichtungen nicht nachlassen, wenn sie mobile Endgeräte einsetzen wollen.

43 Der SRH befürwortet das Ziel der SK, sowohl die Geräteverwaltung als auch die Gerätelandschaft konsolidieren zu wollen.

[5] Chief Information Officer - Beauftragter für Informationstechnologie des Freistaates Sachsen.