RECHNUNGSHOF
RHEINLAND-PFALZ

Auszug aus dem Jahresbericht 2019

Nr. 10 Einsatz mobiler Endgeräte - erhebliche Risiken für IT-Sicherheit und Datenschutz -

Impressum:

Rechnungshof Rheinland-Pfalz
Gerhart-Hauptmann-Straße 4
67346 Speyer

Telefon: 06232 617-0
Telefax: 06232 617-100
E-Mail: poststelle@rechnungshof.rlp.de
Internet: https://rechnungshof.rlp.de

Nr. 10 Einsatz mobiler Endgeräte - erhebliche Risiken für IT-Sicherheit und Datenschutz -

Die Landesverwaltung setzte 2017 fast 2.000 mobile Endgeräte (Smartphones und Tablets) ein. Es wurden 201 Gerätetypen von 16 Herstellern verwendet. Auf knapp 1.000 Geräten (ohne Polizei) waren 59 verschiedene Betriebssystemversionen installiert. Eine einheitliche Produktstrategie auf Grundlage einer Wirtschaftlichkeitsuntersuchung war nicht vorhanden.

Die Betriebssysteme von 62 % der Geräte waren nicht auf einem aktuellen Stand. Sicherheitsrelevante Updates waren nicht durchgeführt worden oder nicht mehr verfügbar. Dadurch waren ein sicherer Betrieb und der Datenschutz nicht gewährleistet.

Die Konfiguration des überwiegenden Teils der mobilen Endgeräte entsprach nicht den Mindestanforderungen des Bundesamts für Sicherheit in der Informationstechnik. Landeseinheitliche und verbindliche Mindeststandards für die technischen und organisatorischen Sicherheitsmaßnahmen für den Einsatz mobiler Endgeräte fehlten.

Auf den zentral verwalteten mobilen Endgeräten waren fast 700 verschiedene Apps installiert, ohne dass die damit verbundenen Risiken für die Informationssicherheit in einem Freigabeprozess bewertet worden waren. Eine Prüfung, ob ein dienstlicher Bedarf für die Nutzung der Apps besteht und welcher Schutzbedarf für die verarbeiteten Daten und Informationen zu berücksichtigen ist, war unterblieben.

Bei über 700 Geräten, die nicht zentral verwaltet wurden, konnten keine einheitlichen Sicherheitsstandards durchgesetzt und Notfallaktionen ausgelöst werden. Ein großer Teil dieser Geräte hatte Zugriff auf die IT-Infrastruktur des Landes.

Bei auch privater Nutzung dienstlicher Geräte lagen keine Einwilligungserklärungen der Benutzer vor, die es den Dienststellen gestatteten, die für die IT-Sicherheit und den Datenschutz erforderlichen Zugriffe, Kontrollen und Maßnahmen durchzuführen.

1 Allgemeines

Zu den mobilen Endgeräten (Mobile Devices) gehören Smartphones und Tablets. Sie sind üblicherweise mit einem berührungsempfindlichen Bildschirm ausgestattet und vereinen in der Regel Mobiltelefon, Media-Player, Personal Information Manager (Adressverwaltung, Kalender, E-Mail-Dienste) und Digitalkamera in einem Gerät.

Mobile Endgeräte ermöglichen ortsunabhängiges Arbeiten und verbessern die Erreichbarkeit ihrer Anwender. Ihr Einsatz in der Landesverwaltung hat an Bedeutung gewonnen, insbesondere bei Führungskräften, bei der Polizei und bei im Außendienst tätigen Mitarbeitern.

Wesentliche Voraussetzung für die dienstliche Nutzung solcher Geräte ist der Schutz der verwendeten Daten. Diese sind sowohl bei der Übermittlung als auch bei der Verarbeitung und Speicherung auf dem Gerät vor Verlust, Veränderung und Missbrauch durch Dritte zu schützen.

Der Einsatz mobiler Endgeräte birgt Risiken für die IT-Infrastruktur und die IT-Systeme des Landes. Durch die Anbindung an die behördlichen Netzwerke über das rlp-Netz können Daten abfließen oder es kann Schadsoftware in diese Netzwerke und angebundene IT-Systeme eingeschleust werden.

Der Rechnungshof hat geprüft, ob die IT-Sicherheit und der Datenschutz beim Einsatz mobiler Endgeräte gewährleistet sind, diese zentral verwaltet und sicher betrieben werden und die getroffenen rechtlichen, technischen und organisatorischen Regelungen den Anforderungen genügen. Als Prüfungsmaßstäbe hat der Rechnungshof insbesondere den Mindeststandard des Bundesamts für Sicherheit in der Informationstechnik für Mobile Device Management sowie dessen Grundschutz-Kompendium herangezogen. Die Prüfung erstreckte sich auf die gesamte Landesverwaltung mit Ausnahme der Hochschulen.

2 Wesentliche Prüfungsergebnisse

2.1 Unübersichtliche Vielfalt von Geräten und Betriebssystemversionen

In der Landesverwaltung waren Ende März 2017 fast 2.000 mobile Endgeräte eingesetzt, davon über 1.000 bei der Polizei.[1] Insgesamt wurden 201 verschiedene Gerätetypen von 16 Herstellern verwendet.

Auf den - nicht durch die Polizei[2] genutzten - Geräten waren 59 verschiedene Betriebssystemversionen zur Verwaltung der Systemressourcen (z. B. Arbeitsspeicher und Festplatte) und der Anwendungsprogramme installiert. Eine einheitliche Produktstrategie, die auf einer angemessenen Wirtschaftlichkeitsuntersuchung beruhen und die insbesondere zur Vermeidung von Administrationsaufwand die Beschaffung möglichst weniger Gerätetypen und Betriebssysteme vorsehen sollte, war nicht vorhanden.

Die Hersteller der Betriebssysteme stellen regelmäßig Patches (Korrekturprogramme zur Fehlerbehebung) für Software und Updates für die Betriebssysteme zur Verfügung, um nachträglich bekannt gewordene Schwachstellen zu beheben und die Geräte vor Gefährdungen zu schützen.

Auf 62 % der eingesetzten mobilen Endgeräte waren die Betriebssysteme nicht auf einem aktuellen Stand. Für 456 ältere Geräte wurden von den Herstellern keine Updates mehr bereitgestellt, auf 216 Geräten waren Updates nicht durchgeführt worden. Damit waren der sichere Betrieb sowie der gebotene Datenschutz bei der Übertragung, Verarbeitung und Speicherung der Daten nicht gewährleistet.

Das Ministerium des Innern und für Sport hat erklärt, der Ministerrat habe als Folge der Prüfung eine Verwaltungsvorschrift (VV) Mobile Endgeräte beschlossen, die für die Gewährleistung eines einheitlichen Sicherheitsniveaus die Anwendung einer ressortübergreifenden Produktstrategie fordere. Das Ministerium sei beauftragt worden, diese zu entwerfen und der Konferenz der Staatssekretäre zur Entscheidung vorzulegen. In der VV Mobile Endgeräte sei die Implementierung eines Updateprozesses vorgesehen. Der von den Herstellern zugesicherte Nutzungszeitraum werde insbesondere im Hinblick auf die Verfügbarkeit von Software-Updates in der Produktstrategie berücksichtigt.

---

1 Ohne Landeskriminalamt.

2 Die mobilen Endgeräte der Polizei wurden nur summarisch erfasst. Sie sind in den folgenden Auswertungen nicht berücksichtigt.

Hierzu bemerkt der Rechnungshof, dass der Entscheidung über die künftige Beschaffung mobiler Endgeräte nach einer ressortübergreifenden Produktstrategie eine angemessene Wirtschaftlichkeitsuntersuchung zugrunde gelegt werden sollte.

2.2 Großer Teil mobiler Endgeräte nicht zentral verwaltet

Für die zentrale Verwaltung und einheitliche Absicherung der mobilen Endgeräte stellt der Landesbetrieb Daten und Information seit 2013 die Mobile Device Management-Lösung (MDM-Lösung) AirWatch bereit. Diese wurde regelmäßig gepflegt. Ihr Betrieb war auch Gegenstand der Zertifizierung des rlp-Netzes durch das Bundesamt für Sicherheit in der Informationstechnik.[3]

Der Landesbetrieb richtete auf einer zentralen Plattform für die einzelnen Behörden und Einrichtungen sogenannte Mandanten ein, in denen die jeweils zugehörigen mobilen Endgeräte verwaltet werden.

Durch die MDM-Lösung können einheitliche Sicherheitsstandards gewährleistet, Sicherheitsregeln auf den Geräten durchgesetzt und Notfallaktionen, wie z. B. die Fernlöschung gespeicherter Daten, ausgelöst werden. Dadurch lassen sich bestehende Risiken minimieren und die mobilen Endgeräte sicher in die IT-Infrastruktur des Landes integrieren.

Zum Zeitpunkt der Prüfung durch den Rechnungshof wurden mehr als 700 mobile Endgeräte nicht zentral, sondern außerhalb der MDM-Lösung betrieben. Ein großer Teil dieser Geräte war in die IT-Infrastruktur des Landes eingebunden und konnte z. B. auf dienstliche E-Mail-Postfächer zugreifen. Auf diese Geräte wurden dienstliche Daten übertragen, dort verarbeitet und gespeichert, ohne dass die mit der zentralen Verwaltung verbundenen Schutzfunktionen wirksam waren. Insbesondere konnten keine einheitlichen Sicherheitsstandards durchgesetzt und Notfallaktionen ausgelöst werden. Dem Stand der Technik entsprechende sicherheitsrelevante Ergänzungen des MDM, wie z. B. Container- bzw. Virtualisierungslösungen zur Trennung dienstlicher und privater Bereiche auf den Geräten, wurden bislang nicht eingesetzt.

Das Ministerium hat mitgeteilt, nach der VV Mobile Endgeräte dürften dienstliche Geräte ausschließlich zentral über ein MDM verwaltet werden. Dadurch ergebe sich auch die Gerätesicherung nach einheitlichen Vorgaben. Soweit in sensiblen Bereichen mobile Endgeräte außerhalb der MDM zu verwalten seien, verbiete der Mindeststandard die Anbindung an die IT-Infrastruktur des Landes. Im Übrigen werde die Einschätzung des Rechnungshofs geteilt, dass die MDM-Lösung unter Berücksichtigung des Wirtschaftlichkeitsgrundsatzes laufend dem Stand der Technik anzupassen und zu erweitern sei.

2.3 Konfiguration mobiler Endgeräte entsprach nicht immer dem Sicherheitsbedarf

Für die Verwaltung der einzelnen Geräte sowie die verwendeten Gerätekonfigurationen, insbesondere die Sicherheitseinstellungen, sind die jeweiligen Behörden und Einrichtungen verantwortlich. Bei der Konfiguration ist dem Schutzbedarf der verarbeiteten Informationen angemessen Rechnung zu tragen. Dafür muss eine passende Grundkonfiguration zusammengestellt und dokumentiert werden.

Zur Erleichterung der Konfiguration werden den mobilen Endgeräten in der MDM-Lösung über sogenannte Profile Einstellungen, Richtlinien und Einschränkungen zugewiesen. Damit werden für Nutzergruppen einheitliche Einstellungen umgesetzt, ohne dass jedes Gerät einzeln konfiguriert werden muss.

---

[3] Bundesamt für Sicherheit in der Informationstechnik (BSI): ISO 27001 Zertifikat auf der Basis von IT-Grundschutz, Zertifikatsnummer BSI-IGZ-0236-2016, gültig bis 29. August 2019.

Die Konfiguration des überwiegenden Teils der mobilen Endgeräte entsprach nicht den Anforderungen des Bundesamts für Sicherheit in der Informationstechnik für normalen Schutzbedarf. Beispiele:

- Die im Profil „Passcode“ der MDM-Lösung hinterlegten Passwortrichtlinien waren nicht einheitlich. Bei 70 % aller Geräte war der Passwortschutz nicht ausreichend.
- Der Zeitraum bis zum Sperren des Bildschirms bei Inaktivität (Gerätesperre) entsprach häufig nicht dem Schutzbedarf. Die Anzeige von vertraulichen Informationen auf dem Sperrbildschirm war oft nicht deaktiviert.
- Bei 200 Geräten mit dem Betriebssystem iOS konnten sicherheitsrelevante Einstellungen durch den Benutzer geändert werden.
- Häufig war das Speichern in der iCloud, also auf Servern des Betriebssystemherstellers und außerhalb der EU, zumindest teilweise zugelassen. So können vertrauliche Daten an unbefugte Dritte gelangen.
- Fast alle Geräte konnten mit fremden W-LAN-Netzen verbunden werden. Dadurch war die Vertraulichkeit der Datenübermittlung nicht gewährleistet und es bestand die Gefahr der Infektion mit Schadsoftware.

Das Ministerium hat erklärt, in der VV Mobile Endgeräte würden entsprechende Sicherheitseinstellungen festgesetzt. Die Schutzziele „Vertraulichkeit“ sowie „Integrität“ könnten bei der Nutzung fremder W-LAN-Netze auch durch Maßnahmen, wie z. B. verschlüsselte Verbindungen, sichergestellt werden.

2.4 Konformitätsrichtlinien nicht ausreichend

Für den sicheren Einsatz von mobilen Endgeräten müssen Prozesse eingerichtet sein, damit auf Sicherheitsvorfälle umgehend mit angemessenen Maßnahmen reagiert werden kann. Bei einer zentralen Verwaltung in AirWatch können solche Prozesse als sogenannte Konformitätsrichtlinien hinterlegt werden. Diese gewährleisten eine regelmäßige automatisierte Überwachung der Sicherheit der Geräte und die einheitliche, automatisierte Umsetzung der Regelungen zum Umgang mit Sicherheitsvorfällen. Wird ein Sicherheitsvorfall registriert, ermöglichen vordefinierte Prozessabläufe umgehende Schutzmaßnahmen, wie z. B. die Fernlöschung von Daten bei Verlust oder Diebstahl des Gerätes.

Die bestehenden Konformitätsrichtlinien waren nicht ausreichend, um die Mindeststandards für einen sicheren Einsatz mobiler Endgeräte zu gewährleisten. Einheitliche Vorgaben, auf welche Sicherheitsvorfälle bei welchem Schutzbedarf mit welchen Prozessen und konkreten Maßnahmen reagiert wird, fehlten.

Das Ministerium hat mitgeteilt, in der VV Mobile Endgeräte seien entsprechende Vorgaben zum Umgang mit Sicherheitsfällen vorgesehen. Danach müsse jede Behörde die Anwender für mögliche Sicherheitsvorfälle sensibilisieren. Sämtliche Daten des Geräts müssten von der Ferne gelöscht werden können. Die spezifischen Prozesse zur Behandlung von Sicherheitsvorfällen seien zu dokumentieren.

2.5 Nutzung von Apps ohne angemessene Sicherheitsanforderungen

Apps können von Vertriebsplattformen im Internet, sogenannten App Stores, heruntergeladen werden. Apps nutzen regelmäßig die Sensoren und Schnittstellen der Geräte und haben damit auf deren Ressourcen und Funktionen Zugriff. Dies bietet potenziellen Angreifern eine Vielzahl von Infiltrationsmöglichkeiten.[4]

---

[4] „Infiltration“ bedeutet, dass ein unbefugter Dritter unbemerkt z. B. die Kontrolle über Kamera, Mikrofon übernehmen und/oder über Bluetooth- oder W-LAN-Schnittstellen einen Schadcode in das mobile Endgerät einschleusen kann.

Allein auf den mit der MDM-Lösung zentral verwalteten Geräten waren zum Zeitpunkt der Prüfung durch den Rechnungshof fast 700 verschiedene Apps installiert. Lediglich fünf Behörden hatten die Installation von Apps mithilfe einer Whitelist[5] oder einer Blacklist[6] eingeschränkt. In keinem Fall waren die mit den Apps verbundenen Risiken für die Informationssicherheit im Rahmen eines Freigabeprozesses durch die Verantwortlichen bewertet worden.

Außerdem war nicht geprüft worden, ob ein dienstlicher Bedarf für die Nutzung der Apps besteht und welcher Schutzbedarf für die verarbeiteten Daten und Informationen zu berücksichtigen ist. Somit war nicht sichergestellt, dass nur Apps installiert wurden, die angemessene Sicherheitsanforderungen erfüllen.

Nach dem Ergebnis einer stichprobenartigen Prüfung von 100 installierten Apps war deren Einsatz mit erheblichen Sicherheitsrisiken verbunden.[7] Beispiele:

- 82 % der Apps griffen auf Ortungsdaten zu. Dadurch können die Benutzer lokalisiert und Bewegungsprofile erstellt werden.
- 82 % der Apps übermittelten das Benutzerverhalten an Tracking[8]- und/oder Werbe-Netzwerke.
- 66 % der Apps sendeten Daten unverschlüsselt an den Betreiber oder an Dritte.
- 63 % der Apps konnten auf das Mikrofon des mobilen Endgerätes zugreifen. Ein Viertel dieser Apps verfügte zudem über die Möglichkeit der Spracherkennung oder einer Diktatfunktion. Die Spracheingaben werden aufgezeichnet und an einen Server des Betriebssystemherstellers übermittelt.

Das Ministerium hat erklärt, in der VV Mobile Endgeräte werde ein App-Freigabeprozess definiert und umgesetzt. Alle Apps, die in dem vom MDM verwalteten Bereich installiert werden sollten, müssten diesen Prozess erfolgreich durchlaufen. Der im Mindeststandard beschriebene App-Freigabeprozess umfasse die Informationssicherheit, die Feststellung des dienstlichen Bedarfs und die behördenspezifische Ermittlung des Schutzbedarfs der Daten. In dem nicht vom MDM verwalteten Bereich dürften nur Apps installiert werden, die nicht auf einer Blacklist aufgeführt seien. Es liege im Ermessen der Behörde, die Nutzung von Apps für Zielgruppen mit höherem Schutzbedarf zur Minimierung von Restrisiken zu verbieten.

2.6 Einheitliche Regelungen zum sicheren Einsatz mobiler Endgeräte fehlen

Die von den Dienststellen vorgelegten Dienstanweisungen und die sonstigen Regelungen zur Nutzung mobiler Endgeräte waren nicht geeignet, die IT-Sicherheit und den Datenschutz ausreichend zu gewährleisten. Eine Musterdienstanweisung zum Einsatz mobiler Endgeräte war noch nicht erarbeitet.

Sicherheitsrichtlinien, in denen die für den Einsatz mobiler Endgeräte angemessenen Sicherheitsmaßnahmen festgelegt und dokumentiert sind, wurden von keiner Dienststelle vorgelegt. Insgesamt fehlten einheitliche und verbindliche Mindeststandards für technische und organisatorische Sicherheitsmaßnahmen.

Das Ministerium hat mitgeteilt, der Ministerrat habe den Entwurf einer Musterdienstanweisung im Grundsatz gebilligt. Er habe das Ministerium des Innern und für Sport

---

5 Eine Whitelist beinhaltet Apps, die vom Benutzer aus dem App Store heruntergeladen werden können. Apps, die sich nicht auf der Whitelist befinden, können vom Benutzer nicht installiert werden.

6 Eine Blacklist enthält Apps, die auf den mobilen Endgeräten nicht installiert werden dürfen. Alle Apps, die sich nicht auf der Blacklist befinden, können aus den App Stores heruntergeladen werden.

7 Grundlage waren Prüfprotokolle des TÜV Austria zu Apps, die auch in der Landesverwaltung verwendet wurden.

8 Beim Tracking werden Verbraucher von Trackern verfolgt, wenn sie die Apps nutzen. Diese Tracker können erkennen, welche Funktionen der App genutzt werden. Mit diesen Daten können Benutzerprofile erstellt und das Nutzerverhalten analysiert werden.

gebeten, hierzu eine Beteiligung der Arbeitsgemeinschaft der Hauptpersonalräte sowie des Landesbeauftragten für den Datenschutz und die Informationsfreiheit durchzuführen und die abschließende Fassung der Musterdienstanweisung der Konferenz der Staatssekretäre zur Entscheidung vorzulegen. In der VV Mobile Endgeräte sei bestimmt, dass jedes Ressort bzw. jede Behörde in eigener Zuständigkeit auf Basis der Musterdienstanweisung behördenspezifische Dienstanweisungen erlassen solle. Ferner würden Maßnahmen zum sicheren Betrieb von mobilen Endgeräten verbindlich geregelt, die von allen Dienststellen mindestens anzuwenden seien.

2.7 Private Nutzung unzureichend geregelt

Bei einem großen Teil der dienstlichen mobilen Endgeräte war die private Nutzung zugelassen oder geduldet. Allerdings fehlten in allen Fällen Einwilligungserklärungen der Benutzer, die es den Dienststellen gestatten, die erforderlichen Maßnahmen zu ergreifen, um die Vertraulichkeit, Integrität und Verfügbarkeit der dienstlichen Daten zu gewährleisten. Für die IT-Sicherheit und den Datenschutz erforderliche Zugriffe, Kontrollen und sonstige Maßnahmen waren dadurch nicht möglich.

Geeignete technische Möglichkeiten zur Trennung privater und dienstlicher Daten auf den mobilen Endgeräten wurden nicht genutzt.

Das Ministerium hat erklärt, eine private Nutzung dienstlicher mobiler Endgeräte solle grundsätzlich unterbleiben. Falls in begründeten Fällen eine private Nutzung zugelassen werde, sei eine qualifizierte Einwilligungserklärung des Nutzers einzuholen. In der VV Mobile Endgeräte und dem Entwurf der Musterdienstanweisung seien technische Maßnahmen zur Trennung dienstlicher und privater Daten vorgesehen. Konkrete technische Lösungen zur Gewährleistung einer sicheren Systemumgebung und einer sicheren Datentrennung würden erarbeitet.

3 Folgerungen

3.1 Zu den nachstehenden Forderungen wurden die gebotenen Folgerungen bereits gezogen oder eingeleitet:

Der Rechnungshof hatte gefordert,

a) für die Beschaffung mobiler Endgeräte eine ressortübergreifende Produktstrategie basierend auf einer angemessenen Wirtschaftlichkeitsuntersuchung zu entwickeln,

b) sicherzustellen, dass die Betriebssysteme der mobilen Endgeräte auf einem aktuellen Stand gehalten werden,

c) alle mobilen Endgeräte, die in die IT-Infrastruktur des Landes eingebunden sind, mithilfe einer Mobile Device Management-Lösung zentral zu verwalten und nach einheitlichen Vorgaben zu sichern,

d) dem Stand der Technik entsprechende, sicherheitsrelevante Ergänzungen der Mobile Device Management-Lösung unter Beachtung des Grundsatzes der Wirtschaftlichkeit vorzunehmen,

e) sicherzustellen, dass nur sicherheitsgeprüfte Apps installiert werden können und hierzu ein definiertes Freigabeverfahren mit geeigneten Bewertungskriterien einzuführen,

f) für den Einsatz mobiler Endgeräte einheitliche und verbindliche Mindeststandards für die technischen und organisatorischen Sicherheitsmaßnahmen zu setzen sowie eine Musterdienstanweisung und eine IT-Sicherheitsrichtlinie zu erarbeiten,

g) bei auch privater Nutzung der mobilen Endgeräte sicherzustellen, dass die erforderlichen technischen und organisatorischen Maßnahmen ergriffen werden können, um die Vertraulichkeit, Integrität und Verfügbarkeit der dienstlichen Daten zu gewährleisten.

3.2 Folgende Forderung ist nicht erledigt:

Der Rechnungshof hat gefordert, über die Ergebnisse der eingeleiteten Maßnahmen zu Nr. 3.1 zu berichten.