dsb
datenschutzbeauftragte
des kantons zürich

Leitfaden

Einsatz von mobilen Geräten in der Verwaltung

Inhalt

Datenschutzbeauftragte des Kantons Zürich
Postfach, 8090 Zürich, +41 43 259 39 99
datenschutz@dsb.zh.ch, datenschutz.ch, twitter: @dsb_zh

1 Einleitung

Dieser Leitfaden richtet sich an die IT-Verantwortlichen der öffentlichen Organe des Kantons Zürich, die mobile Geräte wie Notebooks, Smartphones oder Tablet-PCs einsetzen.

Insbesondere Smartphones und Tablet-PCs zeichnen sich aufgrund der Kombination von zahlreichen Schnittstellen und Sensoren sowie einer nahezu unbegrenzten Anzahl von Anwendungen (Apps) durch erhöhte Risiken für die Persönlichkeitsrechte der Betroffenen aus. Diesen Risiken ist mit zusätzlichen Informationssicherheitsmassnahmen zu begegnen.

Im Folgenden werden die Informationssicherheitsmassnahmen thematisiert, die beim Einsatz von mobilen Geräten und Datenträgern notwendig sind.

2 Mobile Geräte und Datenträger

2.1 Gefahrenbereiche beim Einsatz von mobilen Geräten und Datenträgern

Die grössten Gefahren beim Einsatz von mobilen Geräten und Datenträgern sind:

- Anbindung der mobilen Geräte im gesicherten Netz der Verwaltung oder über das Internet (auch über Funknetzwerke wie WLAN oder Anbindung über gesicherte Verbindungen wie VPN)
- Abruf und Synchronisation von Kalender, Kontakten und E-Mail (teilweise auf verwaltungsfremden Geräten oder via Webinterface)
- Bearbeiten von Daten mit Programmen und Anwendungen, die vom öffentlichen Organ nicht autorisiert sind
- Installation und Verwendung von Programmen für den privaten Gebrauch
- Verwendung von Datenträgern für den Transport von Daten zwischen der Verwaltung und dem privaten Arbeitsplatz
- Bearbeiten der Daten ausserhalb der Räumlichkeiten der Verwaltung
- Anschlussmöglichkeiten von privaten Geräten (Kamera usw.), meistens über USB-Schnittstelle
- Verlust oder Diebstahl des Geräts und den auf dem Gerät gespeicherten Daten

2.2 Allgemeine Informationssicherheitsmassnahmen

Die wichtigsten Informationssicherheitsmassnahmen sind:

- Auswahl von mobilen Geräten und Datenträgern sowie Anwendungen, die die geforderten Sicherheitsmassnahmen wirkungsvoll umsetzen und innerhalb ihrer Verwendungsdauer unterstützen
- Einrichten der Geräte mit den angemessenen Sicherheitsmassnahmen nach dem aktuellen Stand der Technik
- Entfernen nicht benötigter Dienste, Schnittstellen und Anwendungen (beispielsweise Ausschalten der Standortdienste)
- Strikte Kontrolle der installierten Software (beispielsweise Apps) durch entsprechende Managementanwendungen (beispielsweise sofortige Meldung an das Supportpersonal bei der Installation von Anwendungen), Einsatz eines Mobile Device Managements (MDM)
- Sofortige Intervention durch das Supportpersonal und Anwendung der entsprechenden Prozesse bei Vorfällen wie Befall mit Malware oder Verlust durch Diebstahl (Zugänge zu den Anwendungen sperren, Passwörter ändern, Daten aus der Ferne sperren oder löschen, Sperren der SIM Karte)
- Erstellen einer Weisung mit klaren Handlungsanweisungen für die Benutzerinnen und Benutzer, inklusive der Beschreibung des Zwecks der Sicherheitsmassnahmen sowie der Sanktionen, falls das Verhalten nicht den Vorgaben entspricht (unabhängig von der Hierarchiestufe)
- Anlaufstellen sind bei Problemen der Benutzerinnen und der Benutzer verfügbar und können die notwendigen Massnahmen sofort einleiten (wie 7x24-Stunden-Hotline)
- Sichere Entsorgung der mobilen Geräte und Datenträger (Zusatzspeicher) durch die beschaffende Stelle oder das Supportpersonal

Als Übersicht dient beispielsweise die Empfehlung des BSI zum IT Grundschutz, Kapitel 3.1 bis 3.4.
- SYS.3.1 Laptops
- SYS.3.2.1 Allgemeine Smartphones und Tablets
- SYS.3.2.2 Mobile Device Management (MDM)
- SYS.3.2.3 iOS (for Enterprise)
- SYS.3.2.4 Android
- SYS.3.3 Mobiltelefon
- SYS.4.5 Wechseldatenträger

2.3 Informationssicherheitsmassnahmen bei der Bearbeitung besonderer Personendaten

Bei der Bearbeitung von besonderen Personendaten sind zusätzliche Informationssicherheitsmassnahmen umzusetzen:
- Massnahmen zur Einhaltung der Vertraulichkeit auf dem gesamten Transportweg sowie auch bei der Aufbewahrung: Verschlüsselung der Informationen bei der Speicherung auf dem Gerät, wobei die Verwaltung der Schlüssel (Key-Management) beim öffentlichen Organ verbleiben muss
- Einsatz einer Zwei-Faktor-Authentisierung für den Zugriff auf die Informationen
- Abgleich der Änderungen der Informationen auf den mobilen Geräten mit den Geschäftssystemen, um die Datensicherung (Back-up) sowie die Nachvollziehbarkeit der Veränderungen zu gewährleisten
- Permanenter Schutz vor Malware und anderen Bedrohungen
- Vollständige Protokollierung sämtlicher Aktionen

3 Smartphone und Tablet-PC

3.1 Erhöhte Risiken bei Smartphones und Tablet-PCs

Smartphones und Tablet-PCs zeichnen sich durch erhöhte Risiken aus:
- Offene Schnittstellen (API), die eine Verwendung von Anwendungen (Apps) von beliebigen Anbietern mit beinahe unbeschränktem Funktionsumfang ermöglichen
- Mobile Datenträger mit grosser Speicherkapazität, welche die Ablage von grossen Informationsmengen wie auch die Speicherung einer grossen Menge von Trackingdaten wie Standortdaten zulassen
- Sensoren und Schnittstellen, auf die Anwendungen aller Art je nach Rechtevergabe zugreifen können (lesen und/oder schreiben), wie:
  - Berührungs-, Bewegungs-, Beschleunigungs- und Lagesensor
  - Standort- und Ortungsdienste (GPS)
  - Kamera und Lichtsensor
  - Mikrofon, Lautsprecher, Anschluss für Kopfhörer (Ton)
  - Funkschnittstellen für die Netzwerkkommunikation wie Mobilfunk, Bluetooth, WLAN, Near Field Communication (NFC)
  - USB oder proprietäre externe Anbindungsmöglichkeiten (weitere Geräte / Datenträger)

3.2 Organisatorische Informationssicherheitsmassnahmen

Beim Einsatz von Smartphones und Tablet-PCs sind insbesondere folgende Informationssicherheitsmassnahmen zu berücksichtigen:
- Erstellen einer Weisung zur Verwendung von Smartphones und Tablet-PCs
- Sensibilisierung der Benutzerinnen und Benutzer
- Ergänzung und Erweiterung der Betriebsprozesse mit Blick auf die Nutzung von Smartphones und Tablet-PCs

3.2.1 Weisung zur Verwendung von Smartphones und Tablet-PCs

Vor dem Einsatz von Smartphones und Tablet-PCs ist die Weisung für die Nutzung elektronischer Geräte mit folgenden Punkten zu erweitern:

- Umfang und Art der zu bearbeitenden Informationen
- Erlaubte Mitnahme und Orte der Verwendung
- Private Nutzung am Arbeitsplatz
- Anforderungen an die persönlichen Geräte bei betrieblicher Verwendung
- Administration und Verwaltung der Geräte
- Bedingungen des Zugriffs auf die Informationen der öffentlichen Organe
- Datensynchronisation
- Datensicherung (Back-up)
- Nutzung von Cloud-Diensten
- Verwendung von zusätzlichen Geräten (zur Datenspeicherung)
- Verwendung als Netzwerkkomponente (WLAN-Hotspot)
- Sicherung gegen Diebstahl
- Vorgehen bei Verlust, Diebstahl und Entsorgung
- Verhaltensregeln in Bezug auf unbefugte Nutzung und Modifikationen wie Jailbreaking oder Rooting
- Verhaltensregeln in Bezug auf den Gebrauch des Geräts
- Sicherstellung der Vertraulichkeit
- Verhaltensregeln betreffend die Behandlung und Benützung von Zertifikaten
- Sicherstellung der Verfügbarkeit
- Verhaltensregeln für die Nutzung des Internets
- Benutzung der Schnittstellen und der zur Verfügung gestellten Dienste
- Sachlicher und persönlicher Geltungsbereich
- Massnahmen zur Überwachung der Umsetzung der Weisung
- Hinweise auf die Verpflichtung zur Einhaltung der Weisung und die möglichen Sanktionen
- Verweis auf weitere Dokumente
- Datum des Inkrafttretens, verantwortliche Stelle

Eine Liste der zugelassenen Anwendungen ist zu publizieren. Bei nicht erlaubten Anwendungen ist die Ablehnung zu begründen, damit der Entscheid transparent und nachvollziehbar ist.

3.2.2 Sensibilisierung der Benutzerinnen und der Benutzer

Folgende Verhaltensregeln dienen der Sensibilisierung der Benutzerinnen und Benutzer:

- Nutzung und Geheimhaltung des PIN, Passworts, Gerätesperrcodes und Zugangscodes
- Strikte Beachtung der Liste der zugelassenen Anwendungen und ausschliessliche Verwendung eines internen Stores für mobile Applikationen
- Unverzügliche Meldung von Vorfällen, Verlust oder Diebstahl an den Support
- Bei Verlust des Smartphones oder Tablet-PCs unverzügliche Löschung der Daten aus der Ferne auf dem Gerät (und den Speicherkarten sofern verwendet) durch den Support, danach Sperrung der SIM-Karte beim Anbieter
- Unverzügliche Sperrung (Revokation) von Zertifikaten bei Verlust des Smartphones oder Tablet-PCs
- Aktivierung von WLAN, NFC und Bluetooth nur, wenn diese effektiv benötigt werden
- Keine Ausschaltung der Sicherheitseinstellungen sowie strikte Befolgung der Anweisungen des Supportpersonals
- Nutzung von öffentlichen WLAN-Hotspots nur wenn nötig
- Keine Rückrufe an unbekannte Mehrwertdienste-Rufnummern
- Vorgängige Prüfung der benötigten Berechtigungen von Anwendungen (zum Beispiel die Verwendung von Kamera, Mikrofon oder von Standortdiensten)

3.2.3 Ergänzung und Erweiterung der Betriebsprozesse mit Blick auf die Nutzung von Smartphones und Tablet-PCs

Die bisherigen Betriebsprozesse müssen mit den Massnahmen für eine effiziente und effektive Bewirtschaftung der Geräte (meist durch ein Mobile Device Management (MDM)) ergänzt und im Detail ausgearbeitet werden. Diese Massnahmen sind beispielsweise in den Prozessbausteinen des IT-Grundschutz-Kompendiums (Edition 2021) im Kapitel Konzeption und Vorgehensweise (CON) und Betrieb (OPS) des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) zusammengefasst.

Folgende Prozesse sind zu spezifizieren oder allenfalls zu ergänzen:

- Planung des Einsatzes in der Verwaltung
- Auswahl und Beschaffung
- Konfiguration von Diensten und Schnittstellen
- Installation von Anwendungen
- Betriebliche Prozesse
  - Rechtemanagement (-vergabe), Regelung der Rollen und Zugriffe
  - Einsatz und Wartung von allgemeinen Anwendungen wie E-Mail, Kalender, Kontakt- und Adressverzeichnis, Aufgaben, Internetzugriff (Browser), VPN-Anbindung, interne WLAN-Anbindung, Verteilen und Verwalten von Zertifikaten
  - Einsatz und Wartung von Zusatzanwendungen wie Fahrplan-, Wetter-, Bildbearbeitungsanwendungen, soziale Netzwerke, Medienplayer, VOIP (zum Beispiel Skype) oder PDF Reader
  - Einsatz und Wartung von fachspezifischen Anwendungen (zum Beispiel SAP)
  - Back-up von Daten, Programmen (Apps) und Einstellungen
  - Speicherung von Dateien bei einem Service Provider (Cloud-Dienste)
  - Einsatz der Dienste und Schnittstellen
  - Vergabe von PIN, Benutzer-ID und Passwörtern sowie Zertifikaten
  - Unterstützung bei Problemen und Fehlersuche, Anlaufstelle bei Sicherheitsvorfällen
- Erster Einsatz des Geräts
- Folgeprozesse bei defekten und blockierten Geräten
- Vorgehen bei Verlust oder Diebstahl des Geräts
- Austausch oder Weitergabe des Geräts
- Entsorgung des Geräts

3.3 Technische Informationssicherheitsmassnahmen

Dieses Kapitel erläutert die technischen Informationssicherheitsmassnahmen bei der Verwendung von mobilen Geräten.

3.3.1 Einsatz einer Managementsoftware

Der Einsatz einer Managementsoftware für mobile Geräte (Mobile Device Management (MDM)) muss an die internen Betriebsprozesse angepasst und in diese eingebettet werden. Die Anpassungen ergeben sich aus:

- der meist hohen Anzahl Geräte, die bei der Neubeschaffung oder beim Ersatz verwaltet werden müssen
- der Vielzahl der notwendigen Einstellungen (Policies und Installationsparameter)
- der notwendigen Verwaltung (Rollout, Back-up) einer grossen Zahl von Anwendungen (meist im internen Store für mobile Applikationen)
- der Aktualisierung von Anwendungen und Erkennungsmustern (Anti-Viren-Updates)
- des hohen Bedarfs an die Standardisierung der Prozesse (bei allen Geräten gleiche oder ähnliche Funktionalitäten)
- dem fehlenden Know-how für die Spezialisierung nach Gerätetyp (iOS, Android oder Windows Phone)

Zentrale Funktionalitäten von MDM-Software sind:
- Geräteregistrierung (über zentrales Benutzerportal)
- Einbinden der Benutzerverwaltung über ein zentrales Benutzerverzeichnis (zum Beispiel Microsoft Active Directory)
- Geräte- und Softwareinventar
- Zentrale Bereitstellung und Verteilung von Policies
- Zentrale Bereitstellung und Verteilung von Patches und Updates
- Zentrale Verteilung und Löschung von Zertifikaten
- Internen Store für mobile Applikationen (Authentisierung über Zertifikate, nur für registrierte Geräte)
- Verwaltung der Datensicherung (Back-up)
- Gerätesperrung und Löschung von Daten, Anwendungen und Zertifikaten bei Austritt, Verlust, Diebstahl, Defekt oder Austausch
- Überprüfung von spezifischen Geräteeinstellungen und Alarmierung bei unzulässigen Modifikationen

3.3.2 Verwendung eines internen Stores für mobile Applikationen

Eine interne Plattform für Anwendungen oder ein interner Store für mobile Applikationen dient folgenden Zwecken:
- einfache Verwaltung des Bestands der Fachanwendungen und genehmigten Apps
- Informationsbasis für das MDM oder andere Managementsysteme

4 Weiterführende Informationen

Datenschutzbeauftragte des Kantons Zürich
- Checkliste Smartphone-Sicherheit
- Merkblatt Softwarelösungen für IT-Verantwortliche

Weitere Informationen
- Mindeststandard des BSI für Mobile Device Management – Bundesamt für Sicherheit in der Informationstechnik (BSI, Deutschland)
- Smartphone und Tablet effektiv schützen – BSI (Deutschland)

V 1.5 / März 2021