# Mindestsicherheitsstandards beim Einsatz der dienstlichen Geräte

Beim Einsatz der dienstlichen Geräte sind die nachfolgend aufgeführten Mindestsicherheitsstandards zu beachten, um sicherzustellen, dass

- dienstliche Daten vertraulich behandelt werden und
- dienstliche Daten besonders geschützt sind

## 1. Nutzung eines sicheren Endgeräts und eines sicheren Betriebssystems

Voraussetzung für ein sicheres Endgerät ist, dass das Endgerät von einem vertrauenswürdigen Hersteller stammt und dass alle Tätigkeiten vom Vertrieb bis zur Einrichtung des Endgeräts von vertrauenswürdigen Personen oder Institutionen durchgeführt wurde.

Sicherheitsfunktionen sind heute üblicherweise im Betriebssystem integriert. Dies können restriktive Berechtigungen sein, eigene Schutzprogramme, aber auch App-Stores, die nur das Installieren geprüfter Software ermöglichen. Software sollte nur von anerkannt sicheren Quellen bezogen werden. Unter Windows sind in den Standardeinstellungen eine Firewall und ein Virenscanner aktiv, unter Android können die Berechtigungen der einzelnen Programme auf die Ressourcen eingestellt werden und ein iPad lässt nur die Installation aus dem eigenen App-Store zu.

Werden diese Sicherheitseinstellungen beachtet und die Betriebssysteme sowie Programme regelmäßig (automatisch) aktualisiert, ist ein guter Grundschutz gegeben. Aktuelle Betriebssysteme, die vom jeweiligen Anbieter gepflegt werden, können als sicher betrachtet werden, solange die Sicherheitseinstellungen (vgl. BSI) beachtet bzw. nicht bewusst deaktiviert werden.

## *2.* Sichere Softwareauswahl/-einsatz

### 2.1 Software aus anerkannt sicheren Quellen

Beim Download und bei der Installation von Software ist generell Vorsicht geboten, da dieser Weg die einfachste Methode darstellt, um Schadsoftware oder unerwünschte Software (z.B. Adware) auf einem Endgerät zu bringen.

Sichere Anbieter von Software sind insbesondere

- Softwareportale der Betriebssysteme (Apple Appstore, Google Playstore, Microsoft Store)
- Webseiten des Herstellers der Hard- oder Software
- vertrauenswürdige Softwareportale, z. B. Heise oder Snapfiles.

*Bei vielen Softwareportalen wird allerdings oft zusätzlich Adware mitinstalliert.*

### 2.2 Installation der Software

Die Software ist nur mit dem geringsten notwendigen Funktionsumfang zu installieren und auszuführen.

### 2.3 Software zur Verarbeitung personenbezogener Daten

Vor dem Erwerb der Software, durch die personenbezogene Daten verarbeitet werden, hat eine Freigabe durch die Schulleitung zu erfolgen.

*[Hinweis:*

*Die Schulleitung kann im Rahmen ihrer organisatorischen Befugnisse den Datenschutzbeauftragten mit der Überprüfung beauftragen.*

## 3. Betrieb des Endgeräts in einer sicheren Netzwerkumgebung

In einem schulischen Netzwerk (z. B. Lehrernetz) mit Zugangsbeschränkungen, kann davon ausgegangen werden, dass das Netzwerk sicher ist und dass aus dem Netzwerk heraus keine Angriffe

auf einem Endgerät erfolgen. Entsprechendes gilt auch für das Heimnetzwerk, wenn man ein sicheres WLAN-Passwort gesetzt und am Heimrouter keine Verbindungen von außen ins Heimnetz geöffnet hat. Einschränkungen gelten gegebenenfalls, wenn schlecht abgesicherte Smart-Home-Geräte im Heimnetz betrieben werden, die von sich aus einer Internetverbindung öffnen.

### Betrieb des Endgeräts in unterschiedlichen Umgebungen

Wenn dienstliche Endgeräte in unterschiedlichen Umgebungen genutzt werden, fehlt der Schutz der schulischen oder häuslichen Umgebung und des lokalen Netzwerks. Deshalb muss in besonderer Weise sichergestellt sein, dass

- das Endgerät vor unberechtigten physischen Zugriffen geschützt ist und
- das Endgerät vor Angriffen bzw. unberechtigten Zugriffen aus dem lokalen Netzwerk und aus dem Internet geschützt ist.

Hier ist in besonderer Weise auf sichere Einstellungen am Endgerät zu achten (Updates, Firewall, Virenscanner, keine Freigaben nach außen) sowie auf eine verschlüsselte Verbindung ins Internet.

## 4. Zugriff auf das Endgerät nur durch die jeweilige Lehrkraft

Der Zugriff auf das Endgerät darf nur durch die jeweilige Lehrkraft erfolgen. Ist die Nutzerin bzw. der Nutzer an einem Endgerät mit persönlichen Zugangsdaten angemeldet (z. B. mit Benutzernamen und starkem Passwort), ist der Zugriff von fremden Personen zumindest erschwert. Beim Verlassen des Arbeitsplatzes sollte sich die Lehrkraft abmelden oder das Endgerät sperren. Bei zu langer Inaktivität kann auch eine automatische Sperrung des Endgeräts erfolgen.

Wie strikt diese Maßnahmen durchgeführt werden sollten, ist auch von der jeweiligen Umgebung abhängig. Wenn der Zugangsschutz zum persönlichen Endgerät durch andere Maßnahmen erfolgt (z. B. in einem ausschließlich selbst genutzten Büro) können auch einfachere Schutzmaßnahmen am Endgerät genügen.

## 5. Verschlüsselte Ablage von dienstlichen Daten

Die verschlüsselte Ablage von Dateien oder Dokumenten bietet auch dann noch Schutz, wenn diese in die falschen Hände geraten. Bei der Verschlüsselung von Daten steht die Vertraulichkeit im Vordergrund. Es soll gewährleistet sein, dass ohne den zugehörigen Schlüssel bzw. ohne das Passwort die Dokumente nicht lesbar sind. Der zugehörige Schlüssel muss an einem sicheren Ort aufbewahrt werden.

Möglich ist die Verschlüsselung einzelner Dokumente, die Ablage der Dokumente in verschlüsselten Containern oder die Verschlüsselung ganzer Partitionen bzw. Dateisysteme.

## 6. Speicherfristen

Die gesetzlichen Aufbewahrungsfristen sind einzuhalten.

## 7. Backup der dienstlichen Daten

Sofern ein Backup erstellt wird, muss auf den Zugriffsschutz und auf eine Verschlüsselung geachtet werden. Um einem Verlust der Daten vorzubeugen, empfiehlt es sich, regelmäßig Sicherungskopien der wichtigen Daten anzufertigen und diese an einem sicheren Ort aufzubewahren. Bei Backups sind ebenfalls die unter Ziffer 6 genannten Aufbewahrungsfristen einzuhalten.

## 8. Sicheres Löschen von Datenträgern

Bei ausgemusterten Geräten müssen die Datenträger vor der Entsorgung oder Weitergabe an Dritte sicher gelöscht oder vernichtet werden.