Mindestsicherheitsstandards bei der dienstlichen Nutzung von privaten Endgeräten

Beim Einsatz von privaten Endgeräten zur dienstlichen Aufgabenerfüllung hat die Nutzerin bzw. der Nutzer die Mindestsicherheitsstandards zu beachten.

1. Nutzung eines sicheren Endgerätes 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 Endgerätes 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 (Microsoft Defender) aktiv.
- Bei Apple MacOS ist die Firewall und der Virenscanner integriert und aktiv.
- Unter Android können die Berechtigungen der einzelnen Programme auf die Ressourcen eingestellt werden, ein iPad lässt nur die Installation aus dem eigenen App-Store zu.
- Bei Tablets ist der Schutz in der Systemsicherheit integriert.

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 beachtet bzw. nicht bewusst deaktiviert werden.

2. 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.

3. Betrieb des Endgerätes in einer sicheren Netzwerkumgebung

Hat man ein sicheres WLAN-Passwort gesetzt und am Heimrouter keine Verbindungen von außen ins Heimnetz geöffnet, kann man davon ausgehen, dass das Heimnetz sicher ist. Einschränkungen gelten gegebenenfalls, wenn schlecht abgesicherte Smart-Home-Geräte im Heimnetz betrieben werden, die von sich aus einer Internetverbindung öffnen.

Im Allgemeinen kann man davon ausgehen, dass ein lokales Netz zu Hause sicher ist, solange kein Zugriff von außen möglich ist und innerhalb des Heimnetzes nur sichere Geräte betrieben werden.

4. Internetverbindungen in einer unsicheren Umgebung

In potenziell unsicheren Netzwerkumgebungen (z. B. in einem öffentlichen WLAN) muss man auf Internetverbindungen nicht grundsätzlich verzichten. Voraussetzung ist, dass man an einem sicheren

Endgerät (z. B. eigenes Notebook oder eigenes Tablet) arbeitet, das nicht manipuliert wurde, dass man in besonderer Weise auf sichere Einstellungen an seinem Endgerät achtet (Updates, Firewall, Virenscanner, keine Freigaben nach außen) sowie auf eine verschlüsselte Verbindung ins Internet – sobald persönliche oder vertrauliche Daten übertragen werden.

5. Zugriff auf das Endgerät nur durch die jeweilige Lehrkraft

Wenn man an einem Endgerät mit persönlichen Zugangsdaten angemeldet ist (**z. B. mit Benutzername und Passwort**) ist der Zugriff von fremden Personen zumindest erschwert. Beim Verlassen des Arbeitsplatzes sollte man sich **abmelden oder das Endgerät sperren**. Bei zu langer Inaktivität sollte eine **automatische Sperrung** des Endgerätes erfolgen.

Weitere Informationen:
Broschüre: https://schulnetz.alp.dillingen.de/materialien/Passwoerter.pdf;
Selbstlernkurs: https://alp.dillingen.de/lehrgangs-suche/?event_id=285492

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

6. Ablage von dienstlichen Daten

Die dienstlichen Daten sollten **logisch und organisatorisch** von den privaten Daten und den Systemdaten getrennt sein (z. B. in unterschiedlichen Verzeichnissen). 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**.

Möglich sind die Verschlüsselung einzelner Dokumente, die Ablage der Dokumente in verschlüsselten Containern oder die Verschlüsselung ganzer Partitionen bzw. Dateisysteme (Festplattenverschlüsselung). **Bei mobilen Endgeräten sollte die Festplatte verschlüsselt werden**.

Weitere Informationen:
Datensicherheit durch Verschlüsselung: https://schulnetz.alp.dillingen.de/materialien/Verschluesselung.pdf
Selbstlernkurs: Datensicherheit durch Verschlüsselung: https://alp.dillingen.de/lehrgangs-suche/?event_id=285645

7. Löschfristen

Die **gesetzlichen Aufbewahrungsfristen** sind einzuhalten.

8. Backup der dienstlichen Daten

Um einem Verlust der Daten vorzubeugen, empfiehlt es sich, regelmäßig Sicherungskopien der wichtigen Daten anzufertigen und diese an einem sicheren Ort aufzubewahren. Auch bei einem Backup muss auf den Zugriffsschutz und ggf. auf eine Verschlüsselung geachtet werden. Die unter Ziffer 7 genannten Löschfristen sind einzuhalten.

Sofern das Backup in der Cloud außerhalb des EWR/EU-Raums erfolgt, ist darauf zu achten, dass die personenbeziehbaren Daten Dritter nicht ohne weitere Sicherheitsmaßnahmen (z.B. angemessene und geeignete Verschlüsselung) abgelegt werden.

Weitere Informationen:
Backup in der Cloud: https://schulnetz.alp.dillingen.de/materialien/Handreichung_Cloud-Backup.pdf

9. Entsorgung des Endgerätes

Vor der Entsorgung oder Weitergabe des Endgerätes ist dafür zu sorgen, dass die dienstlichen Daten zuverlässig gelöscht sind.

Stand: 26.07.2022