Gerade die Eigenschaften, die mobile Datenspeicher so nützlich machen, bergen Risiken, die bei ihrem Einsatz beachtet werden müssen.

Dienstlich bereitgestellte USB-Sticks und externe Festplatten sind praktische Helfer im Büroalltag und werden deshalb häufig verwendet – leider öfter, als es sinnvoll wäre. Sie dienen häufig als Datendauerparkplatz, zuweilen werden auch private Inhalte auf den dienstlichen mobilen Datenspeichern gesichert. Ein sorgloser Umgang mit den kleinen Helfern birgt große Risiken für die Sicherheit der Behörde und die Vertraulichkeit der dienstlichen Verfahren.

Das eigentliche Problem bei der Verwendung von USB-Sticks und externen Festplatten liegt darin, dass vielen Bediensteten die Regeln für den korrekten Umgang damit nicht bekannt sind. Nehmen Sie sich bitte die Zeit, diese Regeln kennenzulernen.

Ausführliche Informationen dazu finden Sie beim Bundesamt für Sicherheit in der Informationstechnik BSI. Geben Sie in Ihren Browser die Suchwortkombination „BSI“ und „Wecheldatenträger“ ein, und Sie werden auf die aktuellen Veröffentlichungen des BSI zu diesem Thema geführt.

www.thueringen.de

digitale Services
verwaltung.thueringen.de

Herausgeber:
Thüringer Finanzministerium
Informationssicherheitsbeauftragter des Freistaats
Ludwig-Erhard-Ring 7
99099 Erfurt

Bilder:
Rogge GmbH, Bildmontagen unter Verwendung von Motiven aus AdobeStock, ©Daniel CHETRONI (Titel), © PheelingsMedia (innen oben), ©moquai86 (innen unten), ©Nomad_Soul (S. 5)
Text und Layout:
Rogge GmbH, Weimar

Freistaat Thüringen

Sicher unterwegs

Der richtige Umgang mit mobilen Datenspeichern

Informationssicherheit

Die Verwendung mobiler Datenspeicher bringt diese Risiken mit sich:

Verbreitung von Schadsoftware
Die Verwendung der mobilen USB-Datenspeicher erhöht grundsätzlich die Gefahr, von Schadprogrammen befallen zu werden. Grund dafür ist die Möglichkeit, sie mit mehreren unterschiedlichen IT-Geräten verbinden zu können.

Kopplung in fremden Netzen
Durch die Verbindung der Speichermedien mit behördenfremden IT-Geräten oder Netzwerken können unter Umständen unberechtigte Dritte vertrauliche Daten auslesen.

Physische Defekte
Die Hardware mobiler Datenspeicher kann beim Transport, zum Beispiel auf Dienstreisen oder bei dienstlichen Gängen, beschädigt werden. Dabei können auch die abgelegten Daten verloren gehen.

Physischer Diebstahl
Beim Transport von Datenspeichern und bei ihrem Einsatz außerhalb der Behörde droht der Diebstahl des Geräts und damit der gespeicherten Daten.

Verlust besonders vertraulicher Informationen
Das Risiko von Diebstahl oder Verlust mobiler Geräte ist so groß, dass auf diesen grundsätzlich nur Daten, die keinen besonderen Schutz oder keine besondere Vertraulichkeit erfordern, unverschlüsselt gespeichert werden dürfen.

Das können Sie tun, um einen sicheren Umgang mit mobilen Datenspeichern zu gewährleisten:

1. Vermeide den Stick
Prüfen Sie, bevor Sie Daten aus dem gesicherten dienstlichen System herunterladen müssen, ob der Download auf ein externes Speichermedium wirklich notwendig ist. Besser ist es, die Daten über die ThDAP zu tauschen.

2. Im Dienst nur Dienstgeräte
Speichern Sie behördliche Informationen und Dateien immer auf den dienstlich zur Verfügung gestellten USB-Sticks, nicht auf privaten Geräten. Private Inhalte dürfen auf keinen Fall auf Dienstgeräten verwahrt werden oder erst recht nicht vermischt werden.

3. Nicht „fremdgehen“
Nutzen Sie keine dienstlichen Datenspeicher in fremden oder Ihnen unbekannten IT-Geräten oder Netzwerken.

4. Datenspeicher verschlüsseln
Nutzen Sie grundsätzlich verschlüsselte Datenspeicher, insbesondere dann wenn sensible Daten gespeichert werden.

5. Nicht dauerparken
Mobile Speichermedien sind nur für einzelne konkrete Aktionen gedacht und nicht für eine langfristige Datenspeicherung. Löschen Sie alle Informationen nach ihrer Verwendung.

6. Sicher transportieren
Schützen Sie mobile Datenträger bei Dienstreisen und Dienstgängen vor Beschädigung, Verlust und Diebstahl. Rucksäcke und Hosentaschen sind kein sicherer Ort beim Transport.

Kampagne SECURITY AWARENESS
Eine Handreichung des
Thüringer Finanzministeriums
für die Arbeit mit digitalen Medien

Ansprechpartner/
IT-Sicherheitsbeauftragte(r):

Name:

Dienststelle:

Telefon:

E-Mail: