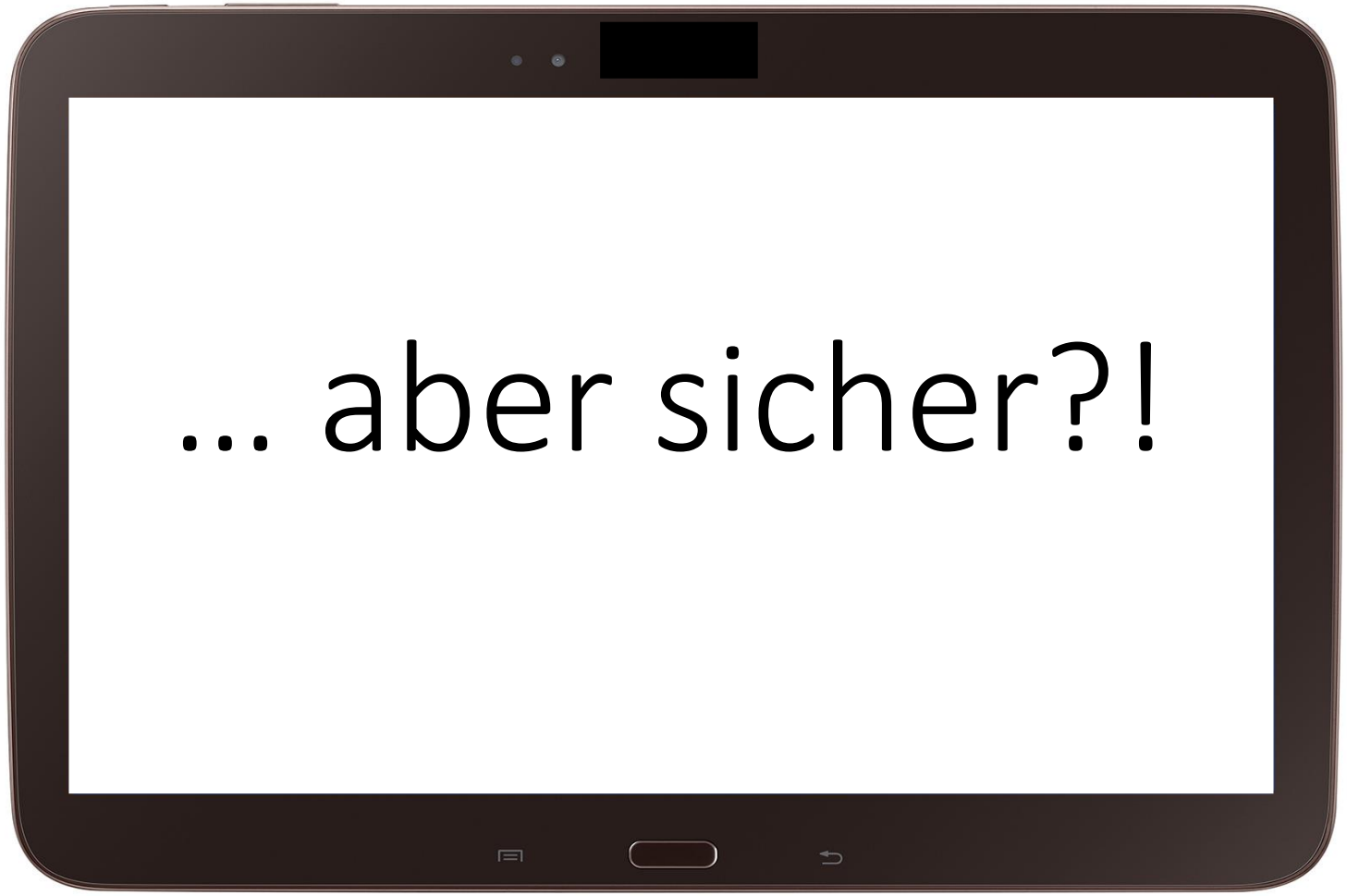
Mit dem Tablet unterwegs…



Zugangsschutz

Zugangsdaten wie PINs und Passwörter immer geheim halten…

… und regelmäßig wechseln.

Und: Machen Sie Gebrauch von Tastensperre und Gerätesperrcode!

PIN

Visueller Code

WLAN, Bluetooth und öffentliche Hotspots

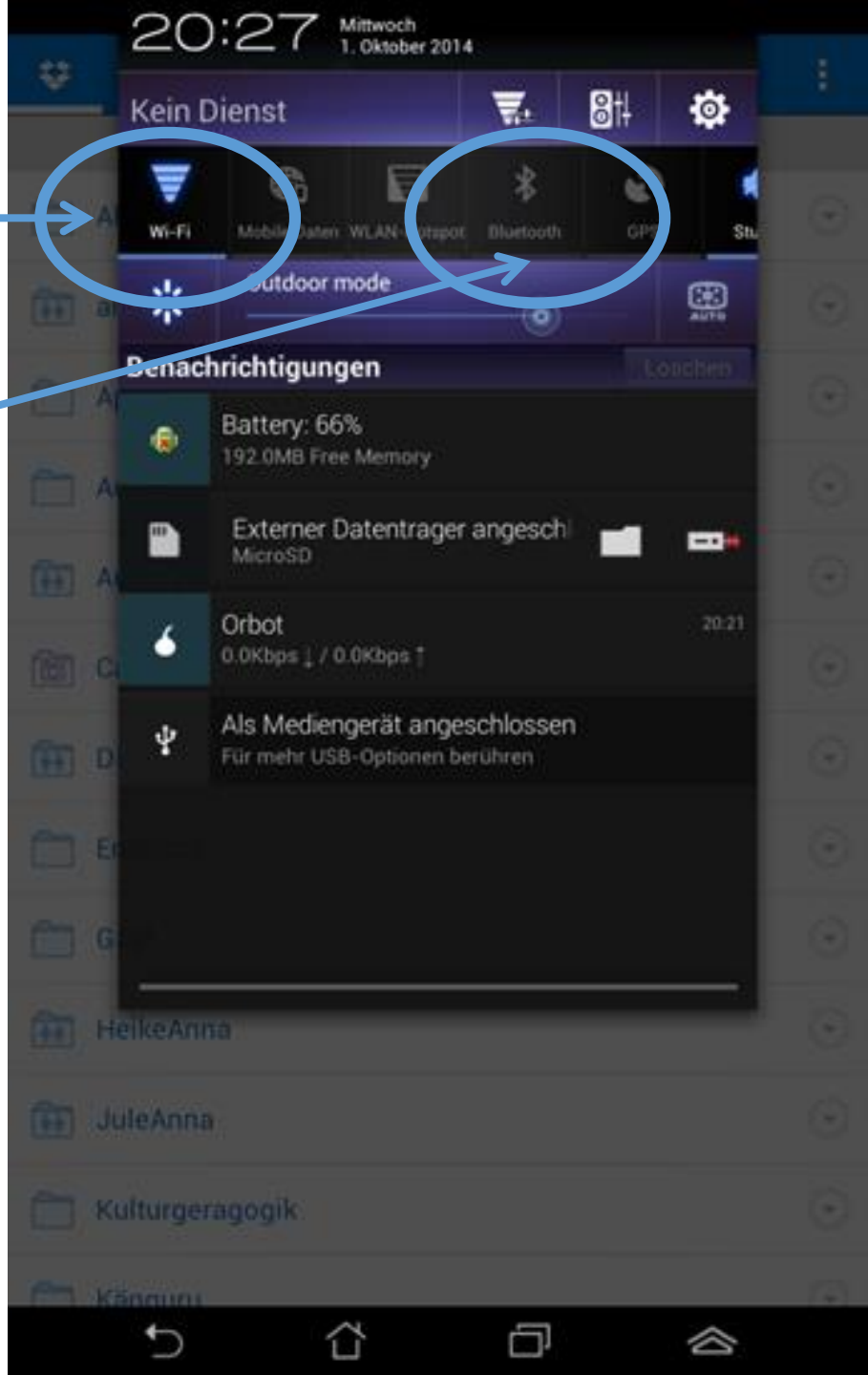
Egal, ob Sie übers WLAN oder den Mobilfunkanbieter ins Netz gehen: Die Datenübertragung ist i.d.R. durch eine Verschlüsselung seitens der Anbieter des jeweiligen Dienstes geschützt.

ABER: **Vorsicht bei der Nutzung öffentlicher Hotspots!** (besser kein Online-Banking…)

Außerdem: WLAN und Bluetooth ruhig auch mal deaktivieren, wenn es gerade nicht gebraucht wird. – Schont auch den Akku.

WLAN/Wi-Fi
ist aktuell aktiviert.

Bluetooth ist aktuell
nicht aktiviert.



Symbole für diese Funktionen sehen unterschiedlich aus, z.B. so:

WLAN/Wi-Fi:

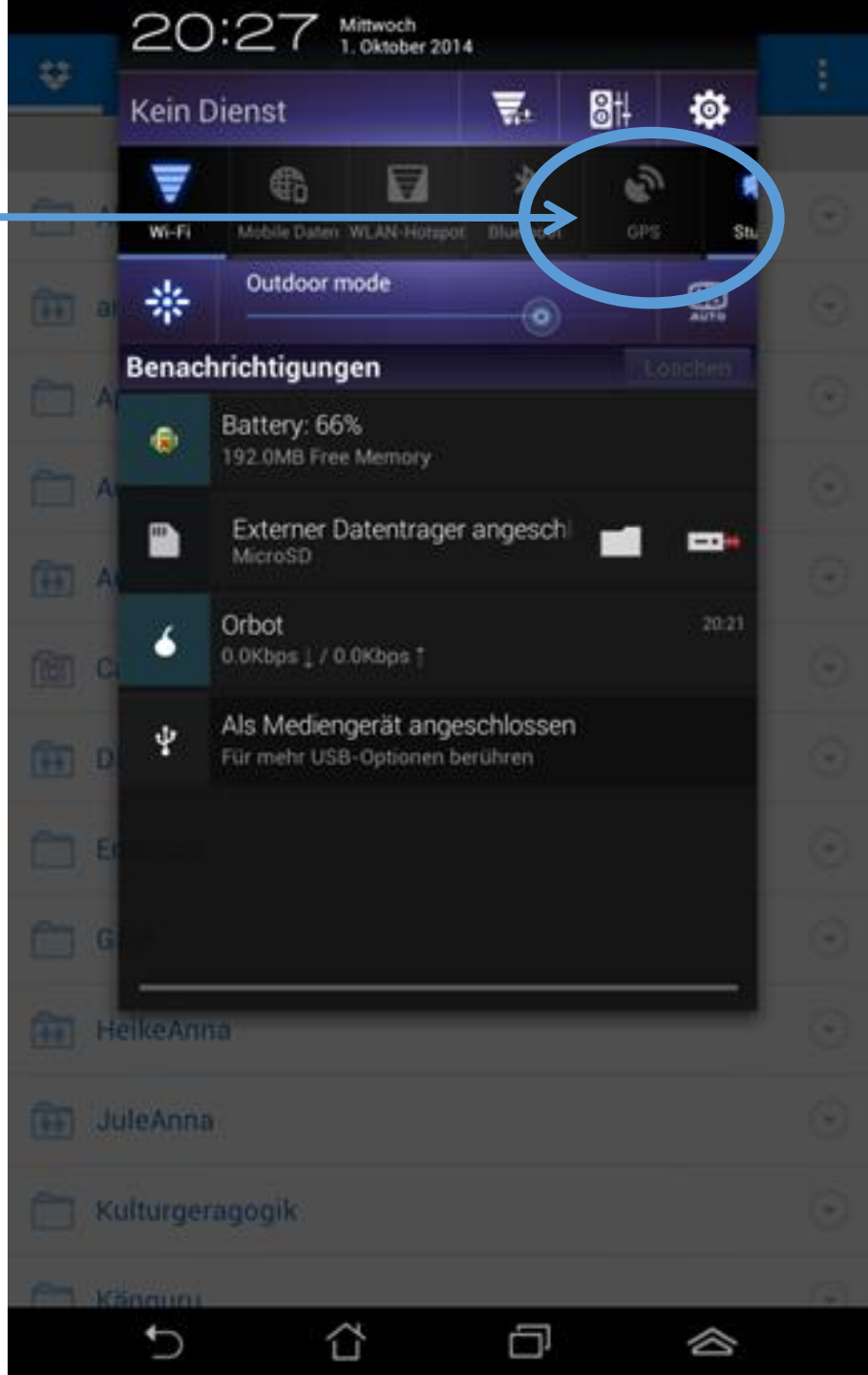
Bluetooth:

Automatische Standortdaten

Um zu verhindern, dass z.B. Bewegungsprofile von Ihnen erstellt werden können, sollten Sie die Ortungsfunktion Ihres Gerätes ausschalten bzw. nur dann aktivieren, während Sie die Navigationsfunktion oder ähnliche Dienste (Apps) tatsächlich nutzen.

Welche Ortungsmöglichkeiten bestehen, erfahren Sie beim jeweiligen Anbieter von Netz, Gerät oder App.

GPS ist aktuell
nicht aktiviert.



Symbole für GPS-Funktion sehen unterschiedlich aus, z.B. so:

Datenspeicherung in der „Cloud“ (engl. Wolke)

Cloud-Dienste, z.B.: Web-Mail, Online-Speicher

Beispiele für Web-Mail-Anbieter:

GMX, Web.de, T-Online

Beispiele für Online-Speicher:

„Cloud Computing“ =

„Rechenleistung aus der Wolke“

Geräte sind nicht auf ihren eigenen Gerätespeicher begrenzt. Daten können ebenso „in der Cloud“ abgespeichert werden.

Der Zugriff auf die Daten in der Cloud erfolgt übers Internet. Der Zugang ist (i.d.R. passwortgeschützt) damit über alle internetfähigen Geräte möglich.

Bildquelle:
http://allaboutcloud.info/wp-content/uploads/2014/01/Cloud-Storage.jpg

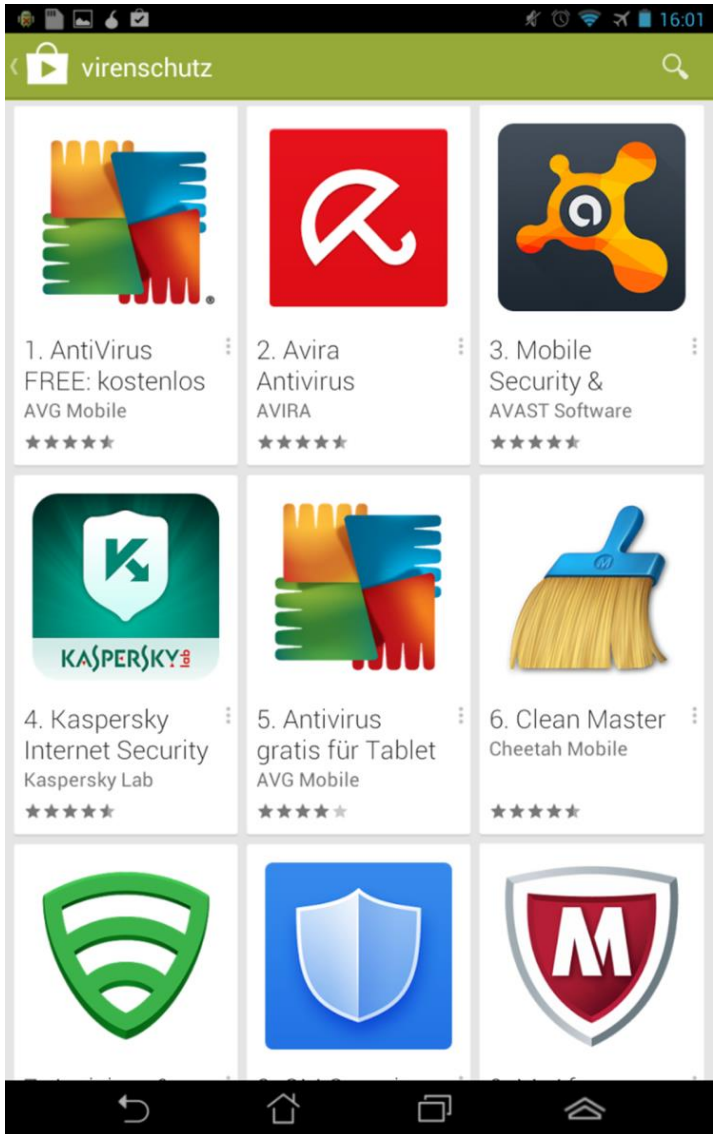
Literaturempfehlung zu „Sicher in der Cloud“

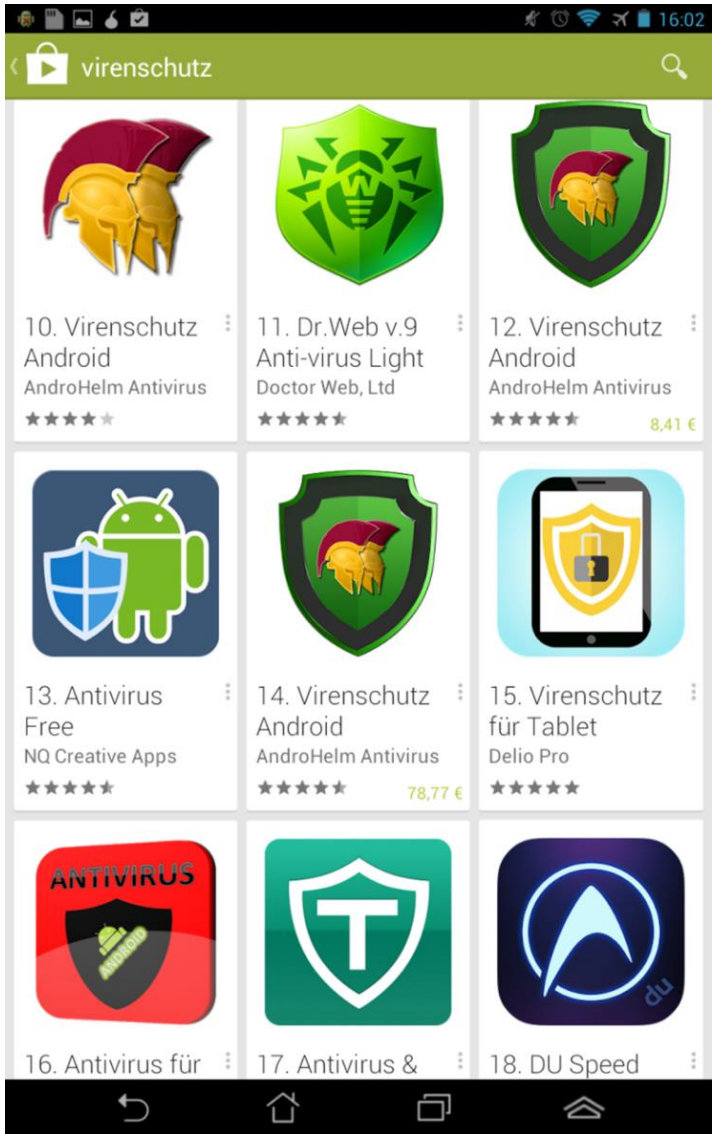
Broschüre des Bundesamtes für Sicherheit in der Informationstechnik (BSI):

„In die Cloud – aber sicher!“

Kostenlos abrufbar unter: www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSIFB/Broschueren/Brosch_A6_Cloud_Computing.pdf?__blob=publicationFile

Anti Virus Programme



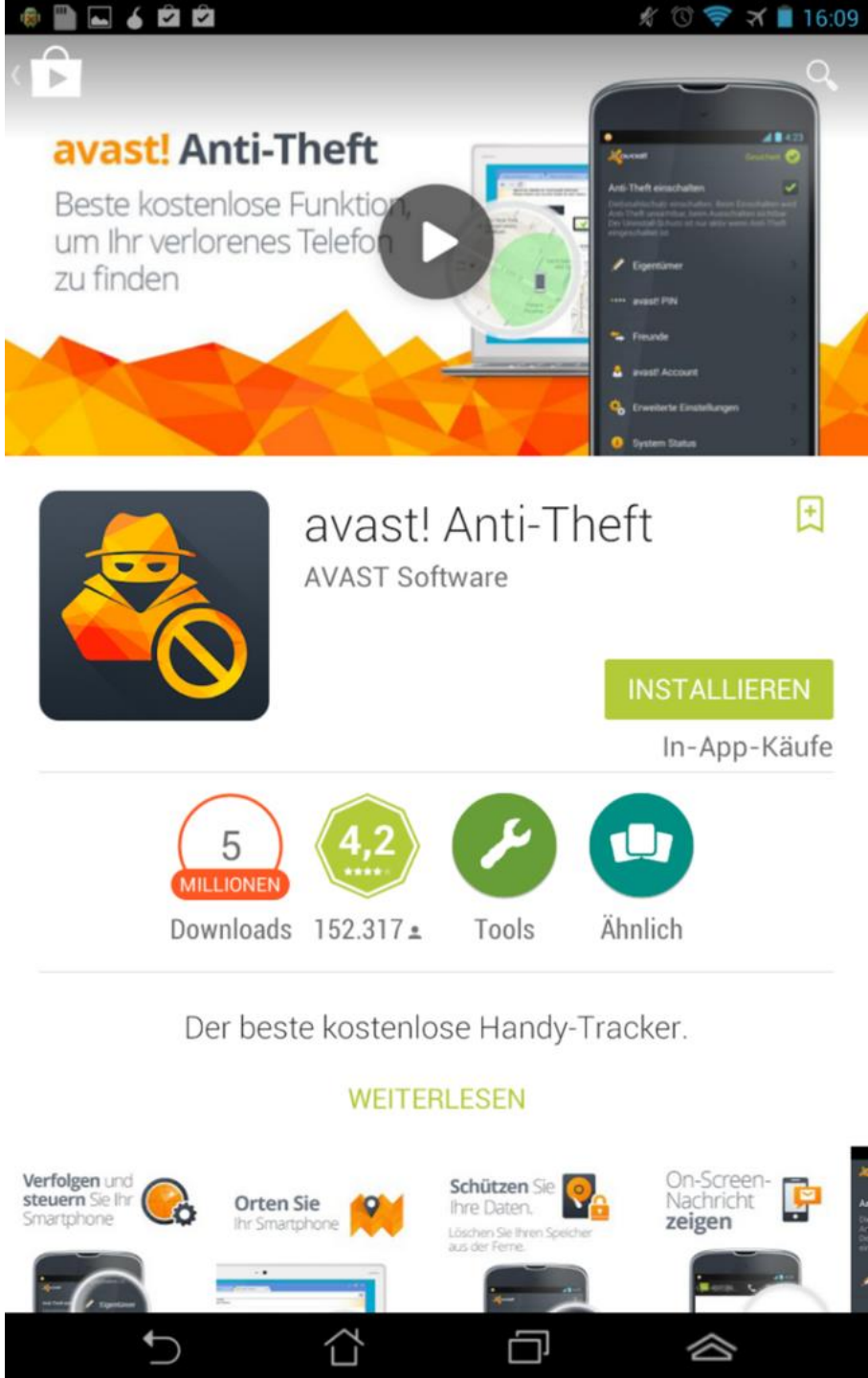


Beispiele für Anti-Virus-Apps

Diebstahlschutz

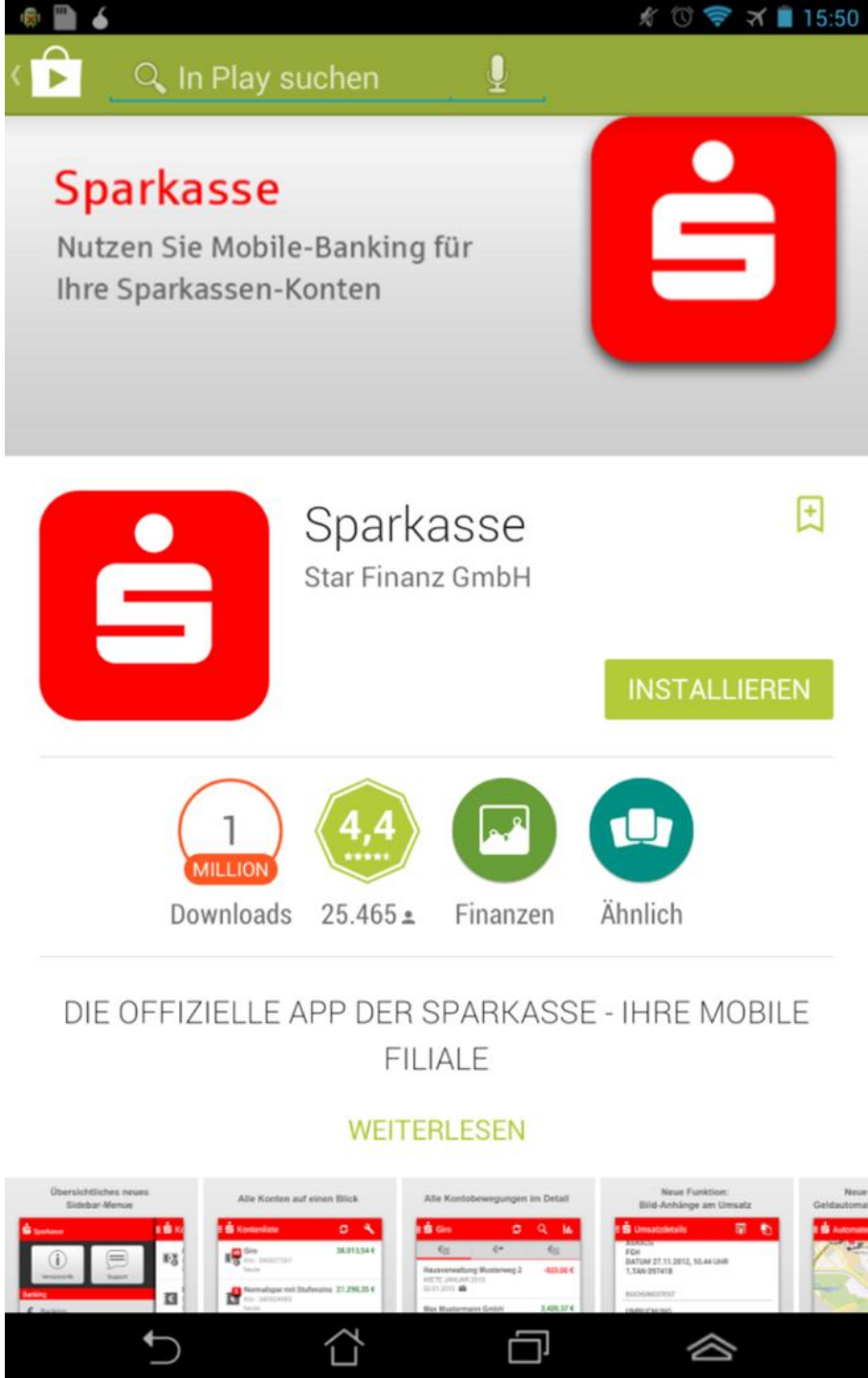
- Über Mobilfunkanbieter sofort SIM-Karte sperren lassen!
- Fernlöschung (Remote Wipe) evtl. über Gerätehersteller möglich
- Evtl. Ortung des Gerätes über Diebstahl-App

Beispiel für Datenschutz-App



Mobile Banking

- Birgt die gleichen Gefahren wie Online-Banking.
- Auf „https://“ achten!
- Adresszeile immer wieder neu eintippen, nicht speichern!
- Nicht an dem Gerät, welches den mTAN empfängt, auch einkaufen!
- mTAN niemals außerhalb der Bankmaske oder Bank-App eintragen!
- Konto regelmäßig kontrollieren!



Beispiel für Online-Banking-App

Bezahlen mit dem Tablet – Varianten:

Über den Anbieter:

- Anruf/SMS
- (Prepaid-) Kreditkarte
- Rechnung
- Nachnahme
- Vorkasse
- Bankeinzug (SSL!!!)

Über eine App, z.B.:

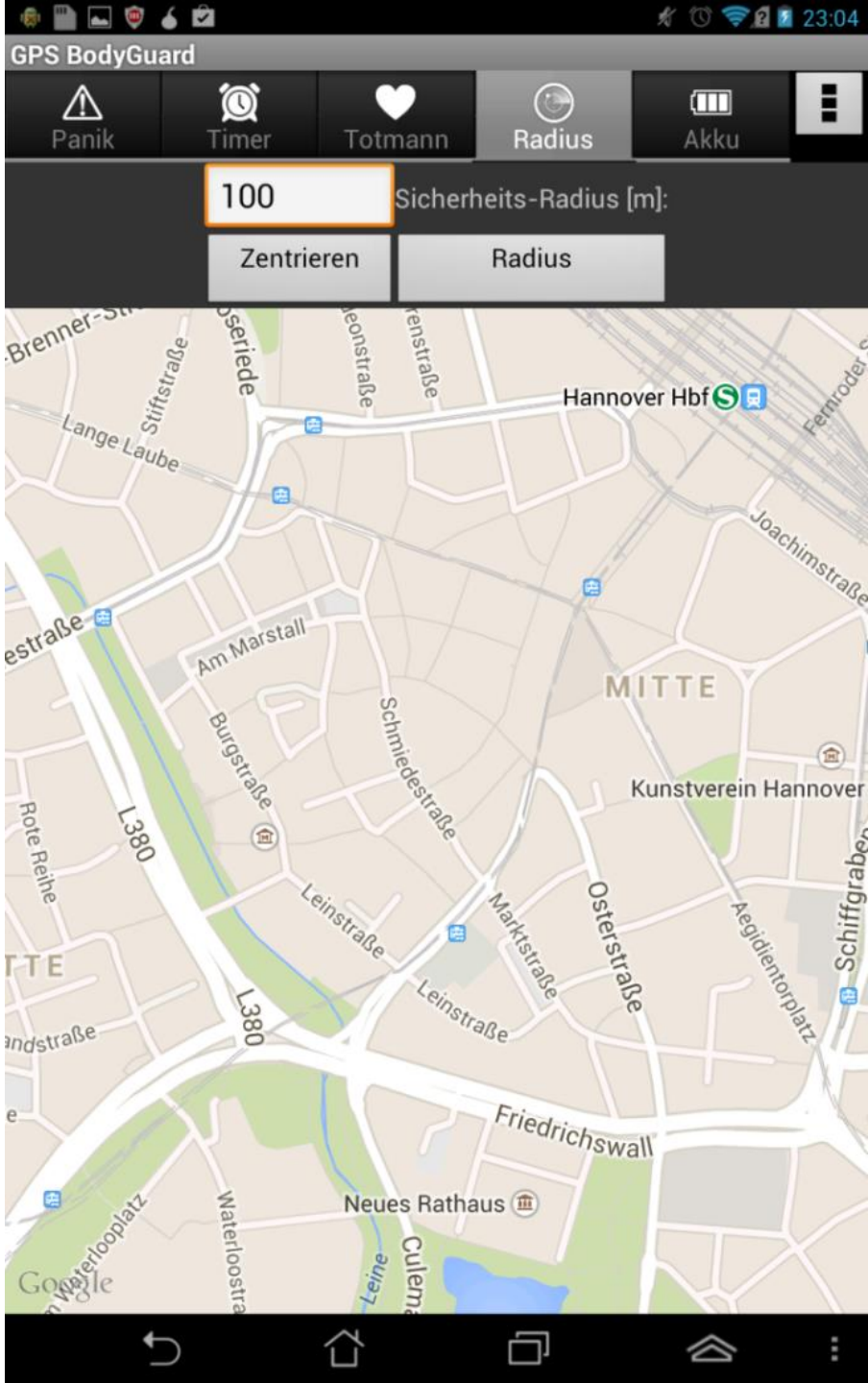
- PayPal
- Click and Buy
- Moneybookers
- Giropay
- Sofort-Überweisung

In einer App, z.B.:

- easyGo (Mobilfunk)
- DB Navigator (Kreditkarte)

Bezahlsystemanbieter, z.B.:

Personen-sicherheit



Literaturempfehlungen

Diverse Broschüren und Tipps des Bundesamtes für Sicherheit in der Informationstechnik (BSI):

Kostenlos abrufbar unter:
https://www.bsi-fuer-buerger.de/BSIFB/DE/Wissenswertes_Hilfreiches/Service/Broschueren/broschueren_node.html
und
https://www.bsi-fuer-buerger.de/BSIFB/DE/Wissenswertes_Hilfreiches/Service/Checklisten/checklisten_node.html

„Das Internet sicher nutzen – Informationen und Tipps für Senior/innen“

Kostenlos abrufbar unter:
http://www.saferinternet.at/uploads/tx_simaterials/Das_Internet_sicher_nutzen_01.pdf

Kontakt zu A. Feineis und C. Kuttner

Anna Feineis afeineis@htwk-leipzig.de
0314-30768808

Claudia Kuttner claudia.kuttner@htwk-leipzig.de
01578-5501557