KOMPETENZZENTRUM
DIGITALES HANDWERK

BFE
OLDENBURG

Mittelstand-
Digital

Gefördert durch:
Bundesministerium
für Wirtschaft
und Energie
aufgrund eines Beschlusses
des Deutschen Bundestages

Smartphones im Geschäftsalltag nutzen – aber sicher

BFE Oldenburg
Bundestechnologiezentrum für
Elektro- und Informationstechnik e.V.

Dipl.-Ing. Werner Schmit
Dozent und IT-Security-Beauftragter (TÜV)

Kurzvorstellung: Dipl.-Ing. Werner Schmit

- Dozent am Bundestechnologiezentrum für Elektro- und Informationstechnik (BFE Oldenburg)
- Arbeitsschwerpunkte
  - Informationssicherheit
  - Datennetzwerktechnik
  - GNU/Linux
  - Systempflege E-Learning-Server
- IT-Security-Beauftragter (TÜV)

- Kontakt
  E-Mail: w.schmit@bfe.de
  Tel.: 0441-34092458

Inhalte

1. Einführung
2. Bedrohungen und Schwachstellen bei mobilen Endgeräten
3. Bestandsaufnahme - Iststand zur Informationssicherheit im Unternehmen
4. Sicherheitsmaßnahmen für mobile Endgeräte

KOMPETENZZENTRUM
DIGITALES HANDWERK
BFE OLDENBURG
Mittelstand-Digital
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

1. Einführung

Betriebsmodelle für mobile Endgeräte 1(2)

- **Zwei Betriebsmodelle oder eine Kombination beider Modelle stehen zur Verfügung**
  - Endgeräte des Unternehmens = An die Mitarbeiter ausgegebene Geräte
  - Private Endgeräte = Bring Your Own Device (BYOD)

- **An die Mitarbeiter ausgegebene Geräte**
  - Das Unternehmen beschafft selbst die Geräte und stellt sie den Benutzern zur Verfügung
  - Entweder als personalisierte Einzelgeräte oder gemeinsam genutzte Endgeräte
  - Eigentum des Unternehmens
  - **Personalisierte Endgeräte, Corporate owned – business only (COBO)** bzw. **Corporate owned – personally enabled (COPE)**
  - **Nicht personalisierte Endgeräte – gemeinsam genutzte Endgeräte**

Betriebsmodelle für mobile Endgeräte 2(2)

- **Private Endgeräte**
  - **Bring Your Own Device (BYOD)**
  - Die Mitarbeiter (Endanwender) nutzen bereits vorhandene private mobile Endgeräte, um auf Informationen des Unternehmens zuzugreifen.
  - Die Endanwender erwarten …
    - dass sie die Unternehmensinfrastruktur wie WLAN-Zugang und Netzwerkfreigaben mit ihrem mobilen Gerät nutzen können.
    - dass die E-Mail-Serverkonfiguration den Fernzugriff über ihr mobiles Gerät gestattet.

Wozu werden die mobilen Endgeräte eingesetzt?

Nutzungsszenarien für mobile Endgeräte

Szenario 1: (erfordert die geringsten Sicherheitsmaßnahmen)

- Die Benutzer telefonieren hauptsächlich mit ihren Geräten und versenden E-Mail.
- Die Benutzer können nicht auf interne Kollaborations- und Dokumentenmanagementsysteme zugreifen.
- Die Informationen sind nicht als vertraulich klassifiziert

Szenario 2:

- Die Benutzer telefonieren mit ihren Geräten, versenden E-Mails und bearbeiten geschäftliche Dokumente.
- Die Benutzer können auf interne Kollaborations- und Dokumentenmanagementsysteme zugreifen.
- Teilweise sind die Informationen als vertraulich klassifiziert.

Fortsetzung Nutzungsszenarien

Szenario 3:

- Die Benutzer telefonieren mit ihren Geräten, versenden E-Mail und bearbeiten geschäftliche Dokumente.
- Die Benutzer können auf interne Kollaborations- und Dokumentenmanagementsysteme, Finanzdaten oder kritische Systeme des Unternehmens zugreifen.
- Teilweise sind Informationen als streng vertraulich eingestuft

- **Fazit**: Das Nutzungsszenario bestimmt den **Schutzbedarf**. Für einen Handwerksbetrieb spielen Nutzungsszenario 1 und 2 eine Rolle

Lösungen …

- **Mobile Device Management** (MDM) → Gerätemanagement ist die Basis
- **Mobile Application Management** (MAM) → Anwendungsmanagement
- **Mobile Content Management** (MCM) → Datenmanagement

KOMPETENZZENTRUM
DIGITALES HANDWERK
BFE OLDENBURG
Mittelstand-Digital
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

2. Bedrohungen und Schwachstellen bei mobilen Endgeräten

Welche Schäden können überhaupt entstehen?

- **Verlust von Vertraulichkeit, Integrität und Verfügbarkeit**

- **Informationen (Daten)**
  Schaden durch Spionage, Sabotage und Datendiebstahl

- **IT-Systeme, Produktions- oder Betriebsabläufe**
  Schaden durch Ausfall, Diebstahl oder Schädigung von IT-Systemen, Produktions- oder Betriebsabläufe

- → finanzieller Schaden, Imageverlust, rechtliche Konsequenzen und Existenzverlust

Auszug BSI Cyber-Sicherheits-Umfrage 2015

- 59% der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) befragten Institutionen waren in den letzten zwei Jahren Ziel von Cyber-Angriffen.

- 54% der von erfolgreichen Cyber-Angriffen betroffenen Unternehmen geben als Ursache das unbeabsichtigte Fehlverhalten von Mitarbeitern an.

- 36% führen den Erfolg der Angriffe auf nicht eingespielte Patches zurück.

Bewertung der Umfrage

- Cyberkriminelle dringen nicht ausschließlich über das Internet in IT-Infrastrukturen ein
- In jedem zweiten der betroffenen Unternehmen liegt die Ursache bei aktuellen oder ehemaligen Mitarbeitern, die die Schadsoftware in das System einschleusen – bewusst oder unbewusst.
- Beispiel: Mitarbeiter finden und nutzen USB-Sticks, die von Angreifern manipuliert und extra platziert wurden.
- Beispiel Diebstahl: Mitarbeiter speichern sensible Daten auf externe Datenträger und nehmen sie an sich

Fazit:

- Im Unternehmen werden klare Vorgaben, Regelungen, Sicherheitsrichtlinien (engl. Security Policies), benötigt, deren Einhaltung zu kontrollieren ist.
- Beispiele: Richtlinien für Mitarbeiter, Patch-Management, Umgang mit mobilen Datenträgern, usw.

Gefahren (Risiken) bei mobilen Geräten

- Zunächst etwas Mathematik
  Gefahr = Bedrohung + Schwachstelle

- Mobile Systeme bergen sowohl bei der Speicherung und Übertragung von Daten als auch bei der Sprachkommunikation besondere Risiken
  → **Vertraulichkeitsrisiken**

- Gefahr durch **Verlust** des mobilen Endgeräts
  Jedes Jahr gehen 70 Mio. Smartphones verloren und nur 7 Prozent der Besitzer erhalten ihr Telefon zurück.
- Gefahren durch **Schadsoftware** (Malware) → *separate Folie*

- Gefahren durch **private Nutzung** mobiler Endgeräte

- Gefahren durch Bring Your Own Device (**BYOD**)

Risiken mobiler Geräte durch Schadsoftware

- Ausspähen von Daten wie z. B. E-Mails, Anmeldedaten und vertrauliche Dokumente
- Verursachung hoher Kosten durch den Versand von SMS-Nachrichten an (ausländische) Telefonnummern von Premiumdiensten
- Ausspähen mobiler Banking-Apps
- Sperren von Geräten, um Lösegeld zu erpressen (Ransomware)

Gefahren (Risiken) bei mobilen Endgeräten

- **Gefahren beim Surfen im Internet**
  Phishing-Webseiten versuchen, den Benutzer dazu verleiten, persönliche Daten in ein scheinbar harmloses Formular einzugeben.

- **Gefahren beim Zugriff auf Unternehmensdokumente**
  Es muss sichergestellt werden, dass keine vertraulichen Informationen nach außen dringen können, sei es versehentlich (z. B. durch Hochladen der betreffenden Dateien auf einen Filesharing-Dienst) oder absichtlich (Insider-Bedrohung)

- **„Gefahren“ der Unproduktivität des Mitarbeiters**
  Ablenkung durch zu viele installierte Apps, viel Arbeitszeit mit Spielen und anderen Freizeitbeschäftigungen vergeudet.

Bedrohungen und Schwachstellen im Kontext MDM

- Nicht ausreichende Synchronisation mit dem MDM
- Fehlerhafte Administration des MDM
- Ungeeignetes Rechtemanagement im MDM
- Keine oder schwache Verschlüsselung der Kommunikation zwischen MDM und Endgerät
- Unberechtigte Erstellung von Bewegungsprofilen durch das MDM

KOMPETENZZENTRUM
DIGITALES HANDWERK
BFE OLDENBURG
Mittelstand-Digital
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

3. Bestandsaufnahme – Iststand zur Informationssicherheit im Unternehmen

Iststand zur IT-Sicherheit im Unternehmen 1(5)

- Klar ist: 100-prozentige Sicherheit gibt es nicht
- Allerdings wäre es ein Irrtum, deshalb zu resignieren
- Gelebte Realität in vielen Unternehmen: Resignation, Hackern und Cyber-Kriminellen wird verteidigungslos das Feld überlassen
- Cyber Security ist – trotz der wachsenden Bedrohungslage – in deutschen Unternehmen oft wenig mehr als ein Lippenbekenntnis
- Firmenlenker handhaben das Thema Informationssicherheit sehr unterschiedlich

Iststand zur IT-Sicherheit im Unternehmen 2(5)

- Unternehmen sind sich bewusst, dass ihr Business vor allem auf einer sicheren IT basiert

- Unternehmen vertrauen darauf, dass die organisatorischen und technischen Maßnahmen, die sie bereits ergriffen haben „schon reichen werden“ und „das wir gar nicht interessant genug sind für einen Hacker-Angriff“

- Empfehlungen vom Informationssicherheitsbeauftragten (ISB) oder IT-Admins gelten eher als Kosten denn als Investition in die Zukunftssicherung des Unternehmens und sterben den schnellen Tod auf der nächsten Streichliste

- Selten schätzen Unternehmen das tatsächliche Bedrohungspotenzial realistisch ein

Iststand zur IT-Sicherheit im Unternehmen 3(5)

- Neuartige Bedrohungen wie gezielte komplexe Angriffe sind oft gar nicht im Vorsorge-Fokus

- Es fehlt an personellen Ressourcen und Know-how

- **Fazit**: Informationssicherheit ist mehr als die Summe von Einzelmaßnahmen. Aus professioneller Sicht ist Informationssicherheit idealerweise ein zentral gesteuertes und in das Unternehmen integrierte Managementsystem. Dieses fehlt noch häufig im Unternehmen.
  Das zielorientierte **Informations-Sicherheits-Management-System (ISMS)** verfolgt einen ganzheitlichen, prozessorientierten Ansatz, da der Schutz essentiell wichtiger Informationen über alle Bereiche der Wertschöpfungskette im Fokus steht. Das Thema Informationssicherheit kann nur sinnvoll über das Management initiiert werden.

Ursachenforschung für den Iststand

- Viele Unternehmen betrachten Informationssicherheit nicht als Chefsache, sondern als Teildisziplin ihrer IT. Diese ist oft nicht angemessen an die Geschäftsbereiche angebunden und erhält keine konkreten Anforderungen von der Business-Seite

- Die Geschäftsführung / das Management hat kein Verständnis für die Erfordernisse der Informationssicherheit

- Für die Unternehmensführung / das Management ist es schwer verständlich, dass die IT ein Stützprozess und damit ein wirklicher Businesstreiber ist und das das Thema Informationssicherheit weit über den Aktionsradius der IT hinausgeht

- Der Unternehmensführung fehlt es häufig an fachlichem Verständnis für relevante Fragen der IT-Sicherheit, da dies nur selten zu den Kernaufgaben des Managements gehört

Gründe bei den angegriffenen Unternehmen

- Updates / Patches wurden nicht (zeitnah) eingespielt
- Mangelhaftes Backupkonzept
- Mangelhaftes Benutzer- / Rechtekonzept
- Mangelhafte Schulung der Benutzer
- Fehlende Netzwerksegmentierung
- Sicherheitssysteme nicht vorhanden oder fehlerhaft konfiguriert

KOMPETENZZENTRUM DIGITALES HANDWERK
BFE OLDENBURG
Mittelstand-Digital
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

4. Sicherheitsmaßnahmen für mobile Endgeräte

4.1 Anforderungen des Unternehmens

4.2 Basisschutz von Smartphones und Tablets

Übersicht der Maßnahmen 1(2)

Allgemeines:

- Für Smartphones und Tablets gelten mindestens die gleichen Sicherheitsanforderungen wie für stationäre Computer
- Zusätzliches Gefahrenpotenzial, durch die Möglichkeit, die Geräte immer und überall dabei zu haben und sie ständig mit dem Internet zu verbinden

Sicherheitsmaßnahmen:

- **Anforderungen des Unternehmens**

- **Maßnahmen zum Basisschutz für Smartphones und Tablets**
  - Empfehlungen von der Polizei
  - Empfehlungen vom Bundesamt für Sicherheit in der Informationstechnik (BSI)

- **Aufbau eines Informationssicherheits-Managementsystems (ISMS)**

Übersicht der Maßnahmen 2(2)

- **Sicherheitsrichtlinien (Regelungen) für Mitarbeiter im Umgang mit Daten und IT-Systemen speziell für mobile Endgeräte**
  - Regelungen für IT-Anwender
  - Regelungen für IT-Personal

- **Mobile Device Management (MDM)**

Mobile Device Security. 1(2)

- **Mobile Device Security beschreibt die Richtlinien, Verfahren und Tools zum Schutz mobiler Geräte.**

- Angriffe auf mobile Geräte haben zugenommen und werden weiterhin zunehmen, da mobile Geräte in unserem Alltag eine immer größere Rolle spielen.
- Der Schutz mobiler Geräte und der auf ihnen gespeicherten Daten sollte in Ihrem Unternehmen deshalb eine hohe Priorität genießen.
- Sorgen Sie dafür, dass ihre Richtlinien und Verfahren mobile Geräte berücksichtigen. Die Sicherheitsempfehlungen für PCs gelten gleichermaßen für Smartphones und Tablets („Kleintierzoo“).

Mobile Device Security - 2(2)

- Halten Sie Software auf dem aktuellen Stand.
- lassen Sie bei der Installation neuer Apps Vorsicht walten.
- Nutzen Sie aktuelle Sicherheitssoftware.
- Gehen Sie verdächtigen Aktivitäten nach.
- Mit **Mobile-Device-Management-Systemen** können Unternehmen viele dieser Funktionen zentral steuern und verwalten

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

4.1 Anforderungen des Unternehmens

Anforderungen des Unternehmens 1(2)

Ziel:

- Festlegen allgemeiner Anforderungen für das Sicherheitskonzept auch hinsichtlich eines Mobile Device Management (MDM).
- Es geht um die Erfüllung **datenschutzrechtlicher, sicherheitstechnischer und betrieblicher Anforderungen**.

Maßnahmen:

- **Strategie festlegen für das Mobile Device Management**
  - Wie Mitarbeiter mobile Endgeräte benutzen dürfen und müssen (eigene Apps installieren, Zuständigkeit der Systempflege, etc.).
  - Wie die Geräte in die IT-Struktur des Unternehmens integriert sind.
  - Müssen private und geschäftliche Bereiche strikt getrennt werden?
  - Wenn ja, über welche Lösung (z. B. Containerlösung, Betriebssystem-mechanismen wie Managed Apps und Managed Open-In oder virtualisierte Benutzerumgebungen)

Anforderungen des Unternehmens 2(2)

- **Festlegen erlaubter mobiler Endgeräte**
  - Welche mobilen Geräte und welche Betriebssysteme sollen unterstützt werden?
- **Festlegung des Betriebsmodells für mobile Endgeräte**
  - private Endgeräte, personalisierte Endgeräte oder nicht pers. Endgeräte
- **Festlegen sichere Grundkonfiguration mobiler Endgeräte**
- **Auswahl und Freigabe von Apps**
- **Festlegung erlaubter Informationen auf mobilen Endgeräten**
- **Auswahl von Sicherheits-Apps**
- **Sichere Anbindung der mobilen Endgeräte an das Unternehmen**

BYOD – Tipp: vermeiden

Quelle: BSI

Ob BYOD innerhalb des Unternehmens freigegeben werden kann, sollte anhand nachfolgender Fragen hinsichtlich eine akzeptablen Risikos beantwortet und bewertet werden:

- Sind die rechtlichen Konflikte bei der dienstlichen Nutzung von privaten mobilen Endgeräten bezüglich des Softwarelizenzrechts geklärt oder ausgeräumt? (z. B. dienstliche Nutzung privater Lizenzen oder private und dienstliche Nutzung von dienstlichen Lizenzen?)

- Sind im Rahmen des Notfallmanagements Maßnahmen hinsichtlich der Löschung des gesamten Datenbestands mit den Besitzern der mobilen Endgeräte vereinbart worden?

- Sind die Verantwortlichen der IT-Abteilung in der Lage, jedes einzelne private Gerät daraufhin zu prüfen, ob es geeignet ist, im Unternehmensumfeld eingesetzt zu werden?

Fortsetzung BYOD – Tipp vermeiden

- Sind Möglichkeiten evaluiert, wie interne Datenschutz- und Sicherheitsanforderungen ausreichend umgesetzt werden können?

- Ist sichergestellt, dass bei Reparatur- und Wartungsarbeiten an privaten mobilen Endgeräten unberechtigte Dritte nicht auf Informationen des Unternehmens zugreifen können?

- Ist sichergestellt, dass nachdem ein Arbeitsverhältnis beendet wurde, der ehemalige Mitarbeiter nicht mehr auf Informationen des Unternehmens zugreifen kann und alle dienstlichen Informationen auf dem mobilen Endgerät gelöscht werden können?

- Ist sichergestellt, dass jederzeit genug Ressourcen für die Benutzerunterstützung vorhanden sind?

Vom Einsatz von BYOD ist abzuraten, wenn eine der Fragen mit Nein beantwortet wird!

Auswahl und Freigabe von Apps - Prüfkriterien

1. Wird durch die App unberechtigt auf Informationen des Benutzers zugegriffen?
2. Versucht die App unberechtigt, die Kommunikationsverbindungen umzuleiten?
3. Werden App-Anwendungsdaten außerhalb des deutschen bzw. europäischen Datenschutzraums gespeichert?
4. Werden App-Anwendungsdaten automatisiert oder ungefragt auf Servern außerhalb der Hoheit des Unternehmens gespeichert?
5. Besteht durch nicht werbefreie Apps die Gefahr des Benutzer-Profilings?
6. Werden die Daten innerhalb einer App, die auf wesentliche Informationen oder Geschäftsprozesse des Unternehmens zugreift, automatisch beim Entsperren des Geräts entschlüsselt oder gibt es eine zusätzliche Zugriffsbeschränkung (muss der Benutzer z. B. zusätzlich ein Passwort zum Entschlüsseln eingeben)?
7. Werden durch die App eigene Sharing-Dienste oder Netzschnittstellen angeboten?
8. Stellt der App-Entwickler regelmäßig Aktualisierungen bereit?
9. Setzt der App-Entwickler die aktuellsten Schnittstellen und Richtlinien des Betriebssystemherstellers um?

Quelle: BSI

Auswahl von Sicherheits-Apps

- Die wichtigste Sicherheits-App: **Der Client für das Mobile-Device-Management-System**

- Weitere (Funktion kann auch Bestandteil des MDM-Clients sein):
  - **Apps zur Lokalisierung des Gerätes im Falle des Verlusts**
  - **Antiviren-App**
  - **Apps für die kryptografische Absicherung von einzelnen Daten und Ordnern**
  - **Apps für die Bereitstellung von Arbeitsumgebungen mittels einer Container-Isolierungstechnik**
  - **Apps, die den Zugriff auf andere Apps regeln**

KOMPETENZZENTRUM
DIGITALES HANDWERK
BFE OLDENBURG
Mittelstand-Digital
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

4.2 Basisschutz von Smartphones und Tablets

Empfehlungen vom BSI

Bundesamt für Sicherheit in der Informationstechnik

BSI FÜR BÜRGER
INS INTERNET - MIT SICHERHEIT

Risiken | **Empfehlungen** | Digitale Gesellschaft | Service

Basisschutz für Computer & Smartphone

Sichere Einrichtung Ihres Computers, Tablets und Smartphones

Inhaltsverzeichnis
- Ihren Computer sicher einrichten
- Schutz für Smartphone & Co.

Quelle: © *baloon111 / Fotolia.com*

Schaffen Sie für die sichere Nutzung Ihres › Computers oder Ihres › mobilen Gerätes eine solide Grundlage, indem Sie Ihr Gerät sicher konfigurieren. Viele Geräte, die "aus dem Karton" heraus in Benutzung gehen, sind das nicht, was Kriminelle ausnutzen.

Auch wenn das Betriebssystem Ihres Gerätes nicht exakt dem vorgestellten entspricht, werden Sie dennoch wichtige Hinweise finden.
Der Begriff "Basisschutz" zeigt aber auch, dass es einen hundertprozentigen Schutz leider nicht gibt, auch keinen hundertprozentigen Geräteschutz.

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/BasisschutzGeraet/BasisschutzGeraet_node.html

BSI-Sicherheitshinweise für Smartphone & Tablet 1(2)

- Gesunder **Menschenverstand**
- Installieren Sie **Apps** nur aus vertrauenswürdigen Quellen
- Deaktivieren Sie **drahtlose Schnittstellen**
- Führen Sie regelmäßig **Sicherheitsupdates** durch
- Nutzen Sie **öffentliche Hotspots** mit erhöhter Vorsicht
- Sorgfältiger Umgang mit **Zugangsdaten**
- Lassen Sie bei **Verlust Ihres mobilen Gerätes** die SIM-Karte unverzüglich sperren

BSI-Sicherheitshinweise für Smartphone & Tablet 2(2)

- **Verkauf** und **Entsorgung**
- **Bewegungsprofile**
- Prüfen Sie unbekannte Rufnummern vor Rückruf
- Führen Sie **Gespräche mit vertraulichem Inhalt** nicht über das Mobiltelefon
- Halten Sie **mobile Geräte** stets unter Aufsicht
- **Backup**

Auch die Polizei hilft durch Aufklärung

Quelle: www.polizei-beratung.de

Empfehlungen der Polizei 1(3)

Sie sind hier: Themen und Tipps / Gefahren im Internet / Smartphone-Sicherheit

Ganz sicher mobil unterwegs

Die Sicherheitsanforderungen an mobile Geräte haben sich verändert. Mit ihrer zunehmenden Verbreitung muss auch verstärkt auf die **Sicherheit der Daten**, die auf solchen Geräten gespeichert sind, geachtet werden. Hinzu kommt, dass darauf inzwischen nicht nur private Daten, sondern auch immer mehr geschäftliche Informationen abgelegt werden. Damit sind Smartphones und Tablets **denselben Risiken ausgesetzt wie stationäre und tragbare PCs**.
Gerade weil man mit Smartphones und Tablets kinderleicht im Internet surfen kann, bieten sie **Angriffspunkte für Schadsoftware** oder Phishing. Die Angriffsmöglichkeiten unterscheiden sich bei Smartphones und Tablet-PC und auch je nach verwendetem Betriebssystem. Die Arbeitsweisen der Täter verändern sich ebenso rasant wie die technische Entwicklung dieser Geräte.

Tipps der Polizei: 2(3)

- Lassen Sie Ihr Smartphone oder Tablet **nie unbeaufsichtigt** liegen lassen.
- Nutzen Sie den **Gerätesperrcode**, die automatische **Displaysperre** und aktivieren Sie stets die **SIM/USIM-PIN.**
- Löschen Sie alle **sensiblen Daten**, wenn Sie das Gerät verkaufen. Stellen Sie das Gerät auf **Werkseinstellungen** zurück.
- Laden Sie **keine Daten aus unsicheren Quellen** herunter.
- Aktivieren Sie **drahtlose Schnittstellen** (WLAN, Bluetooth, etc.) nur bei Bedarf
- Nutzen Sie **fremde WLAN**, z. B. öffentliche Hotspots an Flughäfen oder in Cafes nur mit einem VPN (Virtual Private Network)

Tipps der Polizei 3(3)

- Nutzen Sie **bei Verlust oder Diebstahl** mögliche Ortungs-, Fernsperr- oder Löschdienste. Lassen Sie das Gerät sofort bei Ihrem Anbieter sperren.
- Nutzen sie **Antivirenprogramme** und **Überwachungs-Apps**, die Ihnen die Berechtigungen von anderen Apps (z. B. Zugriff auf das Telefonbuch) anzeigen.
- Verwenden Sie **Online-Banking-Apps nicht auf dem gleichen Gerät**, auf dem Sie auch die **mobilen TAN** empfangen.
- Hinterfragen Sie **Provider-Updates**, die Sie per SMS, MMS oder als Link erhalten – es kann sich um Schadsoftware handeln.
- Lesen Sie vor Kauf und Nutzung der Apps die **Bewertungen in den App-Stores**.

Maßnahme: Schutzsoftware für Smartphone & Tablet

- Mobile Internet Security: Preis: ab 15,-
- Tipp: deutsche Sicherheitsprodukte wählen
- Funktionsumfang:
  - **Virenscanner** - Schutz vor Viren
  - **App-Kontrolle -** überprüft die Berechtigungen der Apps
  - **Geräte wieder finden**
  - **Kindersicherung**
  - **Diebstahlschutz**
  - **Sichere Kontakte -** verhindert nervige Werbeanrufe und Spam-SMS, nur ausgewählte Kontakte zulassen, unliebsame Nummern sperren
  - **Integrierte Browser -** Schutz vor Phishing-Attacken, gefährlichen und gefälschten Webseiten
  - **Schutz am Hotspot (öffentliches WLAN) durch VPN -** sorgt für Privatsphäre und Sicherheit im WLAN und Internet

Vielen Dank für Ihre Aufmerksamkeit