KOMPETENZZENTRUM
DIGITALES HANDWERK

BFE
OLDENBURG

Mittelstand-
Digital

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

Smartphones im Geschäftsalltag des Handwerks nutzen, aber sicher!

Teil 2: Webinar

am 02. Mai 2018

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

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

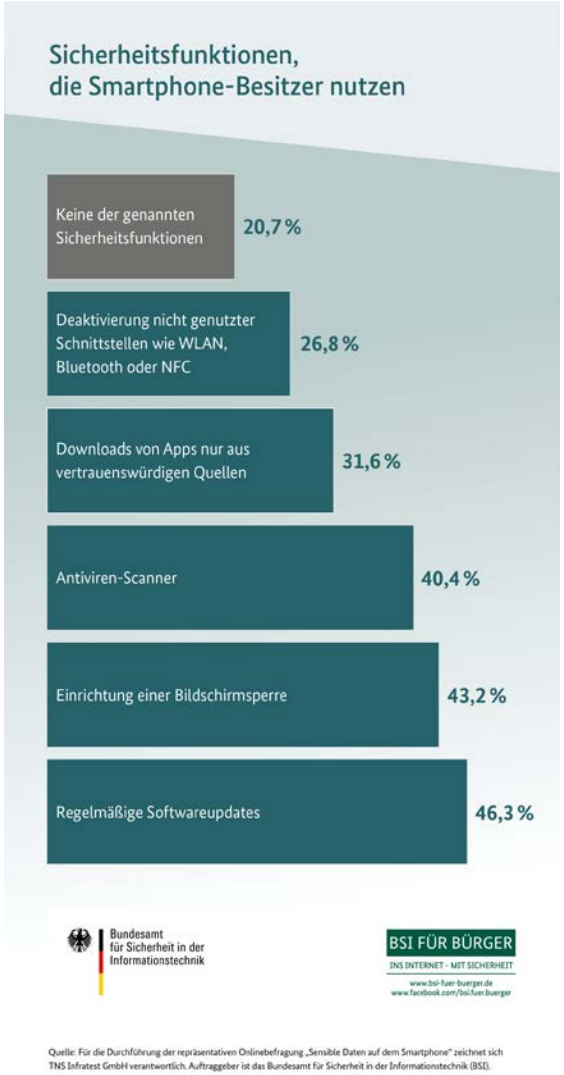
Bisher

- Gefahren beim Einsatz mobiler Endgeräte
- Datenschutzprobleme – Erhebliche Risiken für den Datenschutz
- Sicherheitskonzept für mobile Endgeräte
- NoGo → Bring Your Own Device im Handwerksbetrieb
- Faktor Mensch - größte Schwachstelle

Webinar

5. Schutzmaßnahmen nach Lebenszyklus
6. Einsatz von Security-Suiten
7. Fazit

Die meist genutzten Sicherheitsfunktionen



Wirkungsvolle Schutzmaßnahmen

- **Organisatorische Maßnahmen**
  - Klare Regelungen für dienstliche Nutzung von mobilen Endgeräten
  - Einsatz eines Mobile Device Management (MDM), ...
- **Technische Maßnahmen**
  - Backup, Verschlüsselung, sicheres Passwort, Anbindung über VPN, ...
- **Permanente Sensibilisierung der Mitarbeiter für das Thema Informationssicherheit**
  - Regelmäßige Unterweisungen, ...
- **Notfallvorsorge**
  - Notfallpläne für Diebstahl und Verlust, ...

Schutzmaßnahmen nach Lebenszyklus

- **Erstinbetriebnahme**
- **Systempflege (Wartung)**
- **Nutzung**
- **Abgabe zur Reparatur**
- **Notfallvorsorge**
  - Verlust oder Diebstahl
- **Aussonderung**
  - Verkauf oder Entsorgung

KOMPETENZZENTRUM
DIGITALES HANDWERK

BFE
OLDENBURG

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Erstinbetriebnahme

Erstinbetriebnahme für die sichere Nutzung

- Ersteinrichtung (Konfiguration) des Smartphones für die sichere Nutzung
  - Viele Geräte, die „aus dem Karton“ heraus in Benutzung gehen, sind das nicht

- Umfasst:
  - Aktivieren der vorhandenen Sicherheitseinstellungen
  - automatische Software-Updates aktivieren
  - ...

Geräteverschlüsselung aktivieren

- **Speichern Sie keine vertraulichen Daten unverschlüsselt auf Ihrem IT-Gerät. Bei Verlust kann somit nur ein materieller Schaden entstehen.**

- Aktivieren Sie die systemeigene Verschlüsselung des mobilen Endgerätes. Schützenswerte Daten auf externen Speichermedien (z. B. SD-Karten) sind auch zu verschlüsseln.

- Einfach bei iOS: per Default Datenverschlüsselung aktiviert
- Unterschiedlich bei Android: teilweise ab Werk vorhanden bzw. muss aktiviert werden
  - Abhängig von Android-Version
  - Abhängig vom Smartphone-Hersteller
  - Neue Android-Geräte mit Vollverschlüsselung

Schnittstellen und Funktionen einschränken

- Lassen Sie **nur kontrollierte Datenübertragungen** zu!!!
- **Schnittstellen**: *WLAN, Bluetooth, Infrarot, NFC, USB, SMS, MMS, GPS*
  - Deaktivieren Sie **drahtlose Schnittstellen**
  - Aktivieren Sie **drahtlose Schnittstellen** nur bei Bedarf
    - Weniger anfällig für Cyber-Angriffe
    - WLAN-, Bluetooth- und NFC-Schnittstellen sind offene Einfallstore für Cyber-Kriminelle und schädliche Software.
  - Vertrauenswürdige **USB-Verbindung**
    - mobiles Gerät nur an vertrauenswürdige Rechner anschließen
    - Gefahr der Malwareübertragung
    - Gilt auch für die Stromzufuhr
- **Funktionen**: z. B. *Kamera, Mikrofon, Sprachsteuerung* und *Ortungsdienst*
- **Koppeln und Verbinden mit anderen Geräten** (z. B. via *Apple AirPlay* oder *AirDrop*) zum Datenaustausch oder zur Datenweitergabe unterbinden.

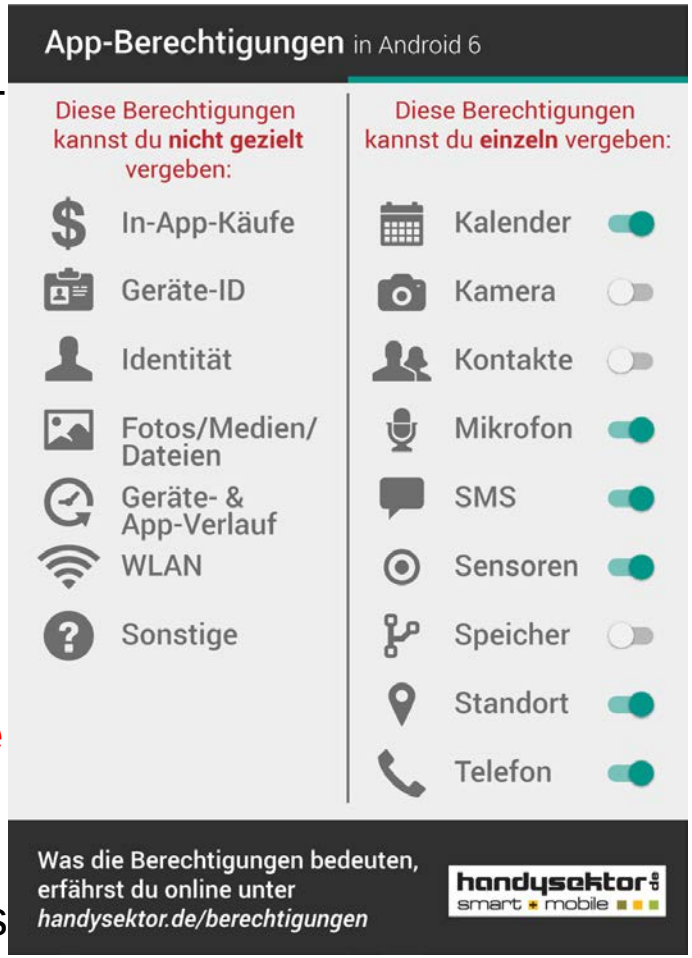
Installation von Apps

- Installieren Sie Apps nur aus vertrauens-würdigen Quellen
- Lesen Sie vor Kauf und Nutzung der Apps die **Bewertungen in den App-Stores**, wenn Ihnen der Anbieter nicht bekannt ist.
- Prüfen Sie kritisch die **Zugriffs-berechtigungen vor der Installation**.
  - das **Einräumen von Zugriffsrechten auf Daten**.
  - sind die eingeforderten Zugriffsrechte erforderlich für deren Funktionalität?
  - Hinweis: Auch durch Update kann Änderung oder Erweiterung der Zugriffsrechte erfolgen

Quelle: Handysektor,www.handysektor.de

App-Berechtigungen

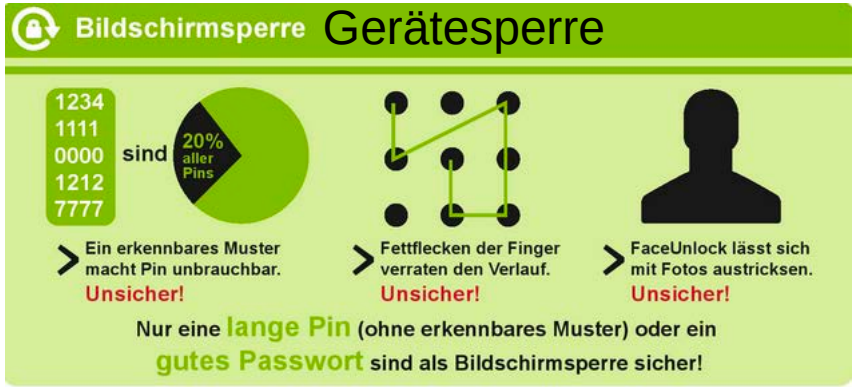
- Zugriffsberechtigungen auf bestimmte Smartphone-Funktionen und persönliche Daten auf dem Gerät vergeben
- Persönliche Daten vor App schützen
- Berechtigungen überprüfen
  - iOS: *Einstellungen → Datenschutz*
  - Android: *Einstellungen → Anwendungen → Anwendungen verwalten*
- 0-Euro-Apps sind beim Thema Datenschutz oft mangelhaft!
- Merke: **Ist etwas kostenlos, „bezahlt“ der Kunde häufig mit privaten Daten!**
- Android-Tipp: https://CluefulApp.com von Bitdefender entschlüsselt Berechtigungen von Apps



Darum sind App-Rechte gefährlich!!!

Zugangsschutz einrichten

- umfasst
  - **Gerätesperre**,
  - **Bildschirmsperre** (Displaysperre)
  - **Tastatursperre**
  - **sperren sensibler Anwendungen**
    - Beispiel Online-Banking
  - **SIM-Karte**
- mittels
  - Passwort
    oder
  - Code,
    - per PIN (Zahlencode)
    - per Wischmuster
    - per Fingerabdruck.



Quelle: Handysektor,www.handysektor.de

Kennwörter und Gerätecodes

- **Einrichtung und Durchsetzung komplexer Kennwörter und Gerätecodes. Vorgabe, nach wie vielen Fehleingaben das Endgerät gesperrt oder gelöscht wird.**
- Die mobilen Endgeräte müssen durch Kennwörter oder Gerätecodes geschützt sein.
- Die Stärke von Kennwörtern und Gerätecodes (minimale Länge, Beschaffenheit, Komplexität und Gültigkeitsdauer) muss der IT-Sicherheitsrichtlinie des Unternehmens entsprechen.
- Die Anzahl der maximal möglichen Fehlversuche für die Eingabe des Gerätecodes muss festgelegt und technisch umgesetzt werden. BSI: **Die Anzahl der möglichen Fehlversuche darf 10 nicht überschreiten.**
- Nach Überschreitung der Grenze müssen alle auf dem Gerät gespeicherten Daten automatisch gelöscht werden.

Automatische Sperre und Gerätesperrung

- **Einrichtung automatische Sperre und Gerätesperrung (Remote-Lock)**
- Die automatische Sperre des mobilen Endgerätes muss genutzt werden.
- Die Gerätesperrung muss sich bereits nach einer angemessenen Phase von Inaktivität einschalten. Die Frist muss den Sicherheitsrichtlinien des Unternehmens entsprechen.
- BSI: **Die Frist sollte aber einen Zeitraum von 10 Minuten nicht überschreiten**.

Virenschutz einrichten

- **Virenscanner**
  - wichtig bei Android-Systemen
- Android-Produkte
  - Avira Mobile Security
  - Eset Mobile Security & Antivirus
  - Avast Free Antivirus
  - Antivirus & Sicherheit Lookout
  - AVAST Security & Booster
  - AVG AntiVirus
  - GData
- Antiviren-App für iOS?
  (nach BSI nicht erforderlich)
- **Firewall -** Ist noch nicht zwingend erforderlich

Quelle: Handysektor,www.handysektor.de

KOMPETENZZENTRUM
DIGITALES HANDWERK

BFE
OLDENBURG

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Systempflege (Wartung)

Aktualität Betriebssystem und Apps

- **Auf Aktualität des Betriebssystems und der Anwendungen (Apps) achten**
  - **Regelmäßige** und **zeitnahe** Aktualisierung von Betriebssystem und Programmen (genutzten Apps), um Sicherheitslücken zu schließen.

Regelmäßiges Smartphone-Backup

- **Smartphone-Konfiguration und -Daten**

- **Lösungen für die Datensicherung**
  - Allgemein: Es gibt App- und PC-Lösungen
  - Verwaltungsprogramme der Smartphone-Hersteller
  - Spezielles Sicherungsprogramm für den Desktop-PC
  - Apps zum Sichern der Daten
  - Manuelles Sichern der Daten ohne zusätzliche Softwareunterstützung

- Nicht vergessen: Restore-Funktion überprüfen

Motivation für Backup

Regelmäßige Backups sind der einzige Weg, mit dem Anwender ihre persönlichen Daten schützen und im Notfall retten können

Beispiele

- **Backup Apple iOS**:
  PC mit iPhone verbinden → ***iTunes*** → erstellt verschlüsseltes Backup auf dem PC bzw. in **iCloud**

- **Backup unter Android**:
  - jeder Hersteller stellt eigenes Tool (App) zur Verfügung, nicht einheitlich.
  - PC mit Android-Smartphone verbinden
  - Samsung mit Android: ***Kies*** (bzw. Nachfolger ***Smart Switch***)
  - LG mit Android: ***LG Backup***

- Alternative für Android: Freeware PC-Anwendung ***MyPhoneExplorer*** und die dazugehörige Android-App ***MyPhoneExplorer-Client***

Backup in der Cloud

- Backups in der **Cloud** sollten grundsätzlich verschlüsselt werden.
- Der „Schlüssel“ liegt bei mir und nicht in der Cloud
- Spezialfall: Verschlüsselungstrojaner – Probleme beim automatisiertem Backup (in Cloudspeicher)
- **Datenschutzrechtliche Anforderungen**
  Wenn Cloud-Dienste eingesetzt werden, sind immer dann rechtliche Aspekte zu beachten, wenn personenbezogene Daten im Sinne des Bundesdatenschutzgesetzes (BDSG, §3 Absatz 1) übergeben werden. Eine solche Auftragsdatenverarbeitung ist, abhängig vom tatsächlichen Speicherort der Daten, nur unter bestimmten Voraussetzungen möglich (§ 11 BDSG) und zudem an einen schriftlichen Auftrag gebunden. Halten sich Unternehmen nicht daran, verstoßen sie gegen bestehendes Recht.

KOMPETENZZENTRUM
DIGITALES HANDWERK

BFE
OLDENBURG

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Nutzung

Lassen Sie Ihr Gerät nicht aus den Augen

- Lassen Sie Ihr Smartphone oder Tablet **nie unbeaufsichtigt** liegen.
- Halten Sie **mobile Geräte** stets unter Aufsicht
  - Um das Gerät vor unbefugtem Zugriff und Manipulation zu schützen, sollten Sie Ihr Smartphone niemals unbeobachtet lassen oder verleihen.

Arbeiten Sie mit gesundem Menschenverstand

- **Gesunder Menschenverstand anwenden**
  - Hinterfragen Sie **Provider-Updates**, die Sie per SMS, MMS oder als Link erhalten – es kann sich um Schadsoftware handeln.
  - Surfen mit gesundem Menschenverstand

Berufliche E-Mail-Adresse nur für berufliche Zwecke

- Dienstliche E-Mail-Adressen sollten von der privaten Nutzung ausgeschlossen sein.
- Regelung gehört mit in die Sicherheitsrichtlinie bzw. Dienstvereinbarung
- Berufliche E-Mail-Adressen dürfen nicht zur Registrierung bei privat genutzten Internetdiensten (z. B. Ebay, Amazon, etc.) oder für den privaten E-Mail-Verkehr verwendet werden.
- Grund: mögliche Kontrollrechte des Arbeitsgebers

Sichere Passwörter verwenden

- Sicher heißt schwer zu erraten
- So sieht ein gutes Passwort aus:
  - Mindestens 12 Zeichen
  - Buchstaben (große und kleine), Zahlen und Sonderzeichen verwenden
  - Keine Begriffe oder Informationen verwenden, die mit mir zu tun haben! Also kein Geburtsdatum, keinen Namen – auch nicht vom Haustier

Quelle: Handysektor,www.handysektor.de

- **Passwörter wie eigene Zahnbürste behandeln: Nicht mit anderen teilen und regelmäßig wechseln**
- Je länger ein Passwort ist, desto sicherer ist es auch.
- Es ist mit steigender Länge aber auch schwerer, sich das Passwort zu merken
- Passwörter merken mit dem Satz-Trick
- Je mehr Passwörter, desto besser

Was taugt mein Passwort? Mach den Test!

- Überprüfung der Passwörter z. B. auf https://checkdeinpasswort.de

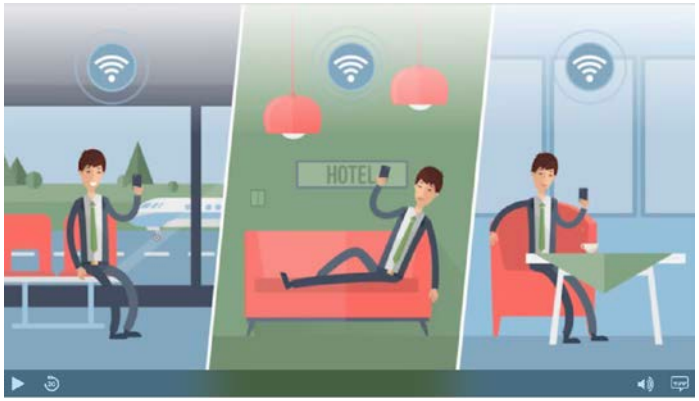
Erstellung von Bewegungsprofilen vermeiden

- Der Aufenthaltsort von Mobilfunkgeräten kann von den Betreibern der Funknetzwerke und zum Teil auch von den App-Anbietern jederzeit ermittelt werden.
- Bei Android: Standortverlauf aktiviert (sendet regelmäßig aktuellen Standort an Google)
- Aber auch mit deaktiviertem Standortverlauf kann ein Smartphone über die Mobilfunkmasten lokalisiert werden.
- **Prinzipiell sollten Sie mit der Weitergabe ihrer Ortsangaben sehr zurückhaltend sein** – also etwa Lokalisierungsdienste meiden und keine Ortsangaben in Fotos speichern, die Sie ins Internet laden.
- **Schalten Sie die GPS-Funktion aus.**
  - Dadurch wird die Positionsbestimmung zumindest ungenauer**.**

Quelle: Handysektor,www.handysektor.de

Vorsicht bei öffentlichen Hotspots (fremde WLAN-Netze)

- Nutzen Sie **öffentliche Hotspots** bzw. **fremde WLANs** mit erhöhter Vorsicht.
- Kein Online-Banking in offenen Netzwerken.
- nur mit einem **VPN** (Virtual Private Network) nutzen.
  - Unterwegs freuen sich die meisten über kostenloses WLAN. In öffentlichen -Netzen im Café oder am Flughafen ist der Zugang meist unverschlüsselt. Hier ist erhöhte Vorsicht geboten. Nutzen Sie, sofern möglich, eine gesicherte https-Verbindung, die Sie am Kürzel in der Adresszeile erkennen. http://multimedia.gsb.bund.de/BSI/Video/Sicher_im_Internet/WLAN.mp4
- Besser: über eigenen Provider ins Internet



Daten schützen durch Backup und Verschlüsselung

Backup

- Erstellen Sie regelmäßig **Backups** der Daten
- **Wichtig bei Backup sind Aktualität der gesicherten Daten und der Speicherort.**
- Viele Backup-Programme nutzen Cloud-Speicher als automatisches Backupmedium.
- Der sicherste Speicherort ist ein externer Datenträger, der nach einem manuellen Backupprozess aus dem Geräte entfernt wird.

Quelle: Handysektor,www.handysektor.de

Verschlüsselung

- Nutzen Sie die Funktionen zur **Datenverschlüsselung**, wenn vorhanden, oder verschlüsseln Sie sensible Daten selbst mit einer Verschlüsselungssoftware.

Verschlüsseln Sie vertrauliche Gespräche

- Mobiles Telefonieren ist nicht abhörsicher.
- Führen Sie **Gespräche mit vertraulichem Inhalt** nicht über das Mobiltelefon (Tipp der Polizei)
- **Verschlüsseln Sie vertrauliche Gespräche**
  - Wenn Sie vermehrt schützenswerte oder gar geheime Informationen austauschen wollen, weichen Sie besser auf verschlüsselte Kommunikation aus.
- Beachten Sie auch Vorgaben Ihres Arbeitgebers bei der privaten Nutzung eines dienstlichen Gerätes oder der dienstlichen Nutzung eines privaten Gerätes.

Prüfen Sie unbekannte Rufnummern vor dem Rückruf

- Unbekannte Rufnummern nicht zurückrufen
- Lassen Sie bei Bedarf unerwünschte Rufnummern zu Mehrwertdiensten von Ihrem Netzbetreiber sperren
- Weitere aktuelle Informationen zu missbräuchlich genutzten Rufnummern finden Sie auf der Webseite der Bundesnetzagentur.
  www.bundesnetzagentur.de/Rufnummernmissbrauch

KOMPETENZZENTRUM
DIGITALES HANDWERK

BFE
OLDENBURG

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Abgabe zur Reparatur

Abgabe zur Reparatur

- Systemkonfiguration und Daten sichern
- Gerät auf Werkseinstellungen zurücksetzen
- Sicherstellen, dass keine sensiblen Daten auf dem mobilen Endgerät oder eingebundenen Speichermedien verbleiben

KOMPETENZZENTRUM
DIGITALES HANDWERK

BFE
OLDENBURG

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Notfallvorsorge (Verlust oder Diebstahl)

Diebstahlschutz

- IMEI-Nummer notieren
- Lokalisierungsfunktion und Fern-löschung der Daten im Betriebssystem aktivieren
  - Nutzen Sie **bei Verlust oder Diebstahl** mögliche Ortungs-, Fernsperr- oder Löschdienste.
  - Alternativ Sicherheits-App mit diesem Funktionsumfang installieren.

Quelle: Handysektor,www.handysektor.de

- Bei Verlust Smartphone orten
  - Android-Gerätemanager bzw. App „Mein iPhone suchen“

Aktionen bei Geräteverlust

- SIM-Karte vom Netzbetreiber sofort sperren lassen
  - Zentralen Kartensperrdienst 116 116 anrufen
  - Aus dem Ausland: 0049 30 4050 4050
- Umgehend den Betrieb informieren
- Mobilgerät per Sicherheitsfunktion bzw. Sicherheits-App lokalisieren
- Gegebenenfalls die Daten aus der Ferne löschen bzw. das Gerät aus der Ferne sperren
- Bei Diebstahl: Anzeige bei der Polizei erstatten und die IMEI-Nummer angeben

- **Melden Sie den Verlust Ihres Mobilgerätes, auch wenn es kurze Zeit später wieder gefunden wurde**. Anschließend sollte die Integrität des Gerätes von vertrauenswürdiger Stelle sichergestellt werden.

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

Aussonderung (Verkauf oder Entsorgung)

Verkauf und Entsorgung

- Löschen Sie **alle Speicher** (**sensiblen Daten)**, bevor Sie das Gerät verkaufen oder entsorgen.
  - Sicheres Löschen → Infos auf Internetseite des Herstellers, Service-Portale, etc.
- Stellen Sie das Gerät auf **Werkseinstellungen** zurück.
- Stellen Sie sicher, dass keine sensiblen Daten auf dem mobilen Endgerät oder eingebundenen Speichermedien verbleiben.
- Entfernen Sie die SIM-Karte.
- Zusammenfassung:
  „Wenn Sie ein Mobilgerät außer Betrieb nehmen, sollte sichergestellt sein, dass alle darauf gespeicherten Daten gelöscht bzw. unbrauchbar gemacht sind und das Gerät auch keine geschützten Unternehmensressourcen mehr nutzen kann.“

KOMPETENZZENTRUM
DIGITALES HANDWERK

BFE
OLDENBURG

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Einsatz von Mobile Security-Suiten

Schutzsoftware für Smartphone & Tablet

- **Gilt für Android-Betriebssysteme**
  Android steht in Verruf, besonders einfach angreifbar zu sein.
- Die Polizei rät: Nutzen sie **Antivirenprogramme** und **Überwachungs-Apps**, die Ihnen die Berechtigungen von anderen Apps (z. B. Zugriff auf das Telefonbuch) anzeigen.
- **Mobile Internet Security-Suite**
  Preis: ab 10,- €
- Tipp: deutsche Sicherheitsprodukte wählen
- Bedürfnisse festlegen
- **Anbieter von Sicherheits-Apps:**
  Avast, Avira, Eset, GData, Kaspersky, McAfee, Norton, Sophos, etc.

Funktionsumfang Schutzsoftware

- **Virenscanner** - Schutz vor Viren
- **Web-Filter / Firewall**
- **App-Kontrolle**
  - Berechtigungen der App anzeigen / verwalten / App sperren
- **Geräte wieder finden**
  - orten / sperren / löschen
- **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

Bewertung Schutzumfang der Security-Suites

- Perfekten Rundum-sorglos-Schutz bietet kein Produkt!!!
- Die Oberflächen vieler Produkte wirken überladen
- Viele Funktionen überflüssig, da sie über die Schutzmechanismen des Android-Systems (Android-Bordmittel) und die Kontrollen im Play Store erreicht werden können.
  - Orten über den Android-Gerätemanager
  - Seit Android 6 lassen sich die Rechte einer App anzeigen und bei Bedarf einzelne entziehen
- Empfehlenswerte Produkte: (Quelle: Sonderheft c‘t Android 2017)
  - **Mobile Security von Eset**, 10,- € jährlich
  - **Internet Security Light von G Data**, 19,- € jährlich

Bewertung Schutzumfang der Security-Suites

- **Größtes Einfallstor unter Android bleiben Bugs im Betriebssystem oder in installierten Apps. Das können Security-Suites auch nicht verhindern.**
  - Hier hilft nur, dass der Software-Hersteller zeitnah Updates und Patches liefert
- **Gesunder Menschenverstand ist immer gut**: Vorsicht bei der Installation von Apps
  - Keine Apps aus Drittquellen (unbekannten Quellen)
    - Haupteinfallstor für Schädlinge
  - Vor der Installation die eingeforderten Rechte anschauen
  - Vorabunterstützung gibt es durch Kontrollen im Play Store
- Zum „Surfen“ im Internet ist in jedem Fall ein Virenscanner erforderlich

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Fazit

Fazit

- Mobile Endgeräte benötigen einen höheren Schutzbedarf als stationäre PCs.
- Für den sicheren Einsatz sind organisatorische und technische Maßnahmen, Notfallpläne sowie eine permanente Sensibilisierung der Mitarbeiter für das Thema Informationssicherheit erforderlich.
- Für die dienstliche Nutzung von mobilen Endgeräten sollten im Unternehmen klare Regelungen und Vorgaben in Form von Sicherheitsrichtlinien (Anwendungsrichtlinien) existieren.
- Die Mitarbeiter müssen die Richtlinien als ihr „persönliches Schutzschild“ empfinden.
- BYOD ist für den Handwerksbetrieb nicht geeignet
- Bevor mobile Endgeräte im Unternehmen eingesetzt werden können, sind noch einige technische Maßnahmen erforderlich. Grund: Smartphones werden für den Consumer-Bereich entwickelt und müssen erst für den Unternehmenseinsatz vorbereitet werden.

Auch bei YouTube

Smartphones im Geschäftsalltag nutzen? Aber sicher!

Vielen Dank für Ihre Aufmerksamkeit