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!

Vortrag am 11. April 2018 in der HWK Oldenburg

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
  - Programmierung (C/C++, Java, PHP)

- IT-Security-Beauftragter (TÜV)
- IT-Security-Auditor

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

Agenda

Vortrag

1. Einführung - Bestandsaufnahme und Fakten
2. Gefahren beim Einsatz mobiler Endgeräte
3. Das Sicherheitskonzept – Strategische Gedanken und Organisatorisches
4. Erstes Fazit

Webinar

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

Einladung per E-Mail zum Webinar

Webinar, Demonstration der Konferenz

Holtz Rainer
An: Schmit Werner

Sehr geehrte Teilnehmer und Teilnehmerinnen,

Der Videokonferenzraum wir mit folgender URL erreicht:

URL: http://bfe.adobeconnect.com/webinar-demo/

Anfangszeit: 11.04.2018, 17:00 Uhr

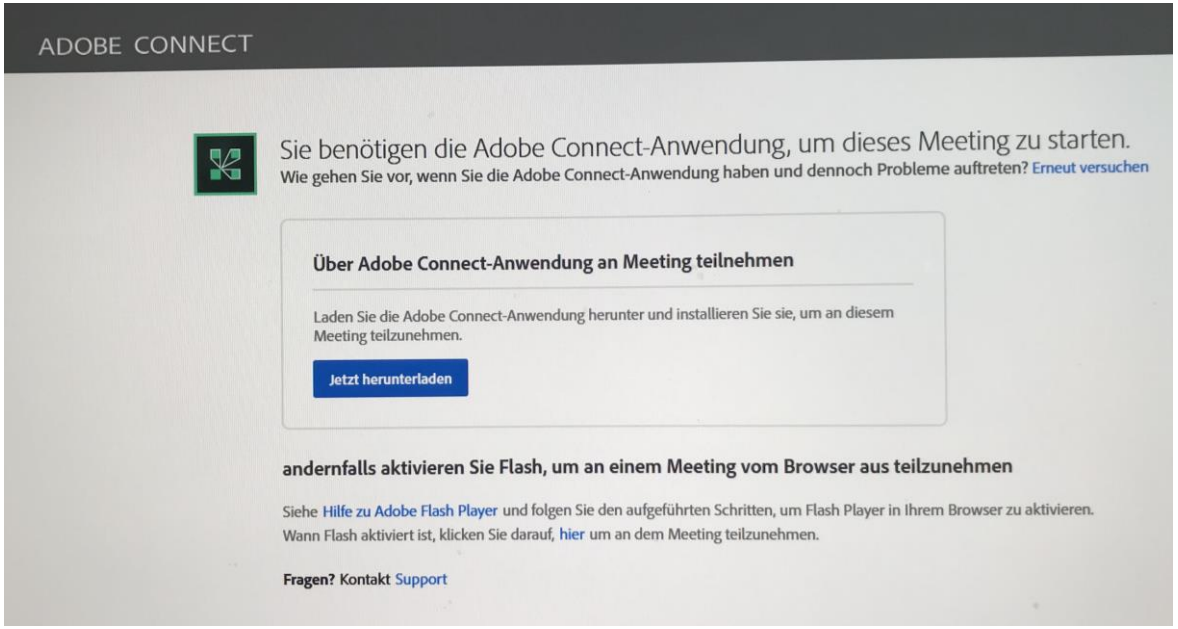
Dauer: 2h

Zugriff: Alle Personen, die die URL für das Meeting haben, dürfen den Raum betreten.

Freundliche Grüße aus dem BFE-Oldenburg

Rainer Holtz
Bereichsleiter Entwicklung und Technologietransfer

Bundestechnologiezentrum für
Elektro- und Informationstechnik e.V.
Donnerschweer Str. 184
26123 Oldenburg
Tel: +49 (0)441 34092-280
Fax: +49 (0)441 34092-259
Mailto: r.holtz@BFE.de



1. Einführung
- Bestandsaufnahme und Fakten

Mobile Endgeräte – Die Lösung für alle Fälle mit Risiken

Die erste technische Revolution war die Einführung des PC, die zweite Revolution die Einführung des mobilen Telefons, die dritte Revolution war das Internet und jetzt wachsen alle Techniken zur Digitalwirtschaft zusammen. Dadurch ergeben sich neue Nutzungs- und Anwendungsmöglichkeiten, aber auch zahlreiche, zusätzliche Herausforderungen. Über mobile Endgeräte ist der Zugang zur IT-Infrastruktur eines Unternehmens ortsunabhängig möglich. Weil ein Smartphone immer und überall verfügbar ist, kann es aber auch immer und überall angegriffen werden.

Viele Unternehmer sind sich auch selten der erheblichen Risiken für den Datenschutz bewusst, die der Einsatz mobiler Endgeräte in der Praxis mit sich bringt.

Smartphones: Komfortable Alleskönner ... - Digitale Helfer für das Handwerk

- Das Smartphone als Allrounder hat längst den Weg in unseren Alltag gefunden und wird in Unternehmen zunehmend als klassisches Endgerät eingesetzt.
  - E-Mails einschließlich sensibler Anhänge versenden und empfangen, Termine verwalten, Kontaktdaten pflegen, ...
- Die kleinen Applikationen (Apps) bieten vielfältige Anwendungsmöglichkeiten
- Grenzen zwischen beruflicher und privater Nutzung verschwinden
- Auch im Handwerk erfreuen sich die digitalen Helfer immer größer werdender Beliebtheit.
- Beispiele:
  - Baustellen-Apps,
  - Fernwartungs-Apps für das SHK-Handwerk
- Auch „Wischen gehört zum Handwerk“

Smartphones: ... aber unsicher (1)

- Primär für den privaten Bereich (Consumer-Bereich) und nicht für den Einsatz in Unternehmen konzipiert
- auf einfache Benutzung ausgelegt
- Teilen von Informationen und Bildern spielt eine wichtige Rolle
- Die Nutzung im gewerblichen Umfeld fordert das genaue Gegenteil. Nur Informationen, die speziell vom Unternehmen freigegeben sind, dürfen mit der Öffentlichkeit geteilt werden
- nur rudimentäre Sicherheitsfeatures
- Die Nutzung von Smartphones birgt erhöhte Sicherheitsrisiken:
  - **Verlust oder Diebstahl des Gerätes** und dadurch unter Umständen Zugriff auf vertrauliche Daten durch Unbefugte
    - Sofern das Gerät vorher nicht entsprechend abgesichert worden ist, hat der neue Besitzer anschließend Zugriff auf alle sensiblen Informationen und kann unter Umständen sogar auf das Firmennetzwerk zugreifen.

Smartphones: ... aber unsicher (2)

- **Manipulation des Gerätes durch bösartige Apps**
- **Unbeabsichtigter, automatischer Datenabfluss an externe Cloud-Dienste**
  - Apps haben Zugriff auf Kontaktdaten, Fotos, Videos, Standortdaten oder Informationen auf der Speicherkarte
  - Apps greifen Informationen ab und verteilen diese über Clouddienste
  - Betrifft nicht nur klassische Malware, sondern auch reguläre Apps

Smartphoneeinsatz: Sicherheitskonzept benötigt!

- **ToDo: Sicherheitskonzept für den Einsatz von Smartphones im Unternehmen erstellen und umsetzen**
- Einige zu klärende Fragen:
  - Sollen im Unternehmen überhaupt private Geräte zum Einsatz kommen? (Thema Bring Your Own Device = BYOD)
  - Welche Unternehmensdaten dürfen wie gespeichert werden?
  - Muss die App-Installation reglementiert werden?
  - Wer ist für die Absicherung und Systempflege zuständig?
  - Welche technischen Maßnahmen zur Absicherung sind erforderlich?
  - Welche weiteren Maßnahmen sind erforderlich?
  - Wie kann ein sicherer Zugriff auf das Unternehmensnetzwerk erfolgen?
  - Wie werden die Mitarbeiter sinnvoll in das Sicherheitskonzept eingebunden?
  - Benötige ich ein Mobile Device Management-System (MDM)?
  - Wer hilft mir bei der Erstellung und Umsetzung?
- Tipp: **„Machen Sie den Einsatz von Smartphones zu einer sicheren Sache!“**

Regelungsbedarf: Abgrenzung mobile Endgeräte

- **Nicht intelligente mobile Endgeräte**
  - Beispiele: Externe Datenträger und Speichermedien (USB-Festplatte, USB-Stick)
  - Sicherheitsrisiken durch technische Maßnahmen gut kontrollierbar
  - Z. B. Maßnahmen: Sperrung USB-Port, Virenscanner, Verschlüsselung
- **Intelligente mobile Endgeräte**
  - Gruppe Notebooks und Laptops
  - Gruppe „Kleingerätezoo“ (Tablets, Phablets und Smartphones)
  - Mehr Sicherheitsmaßnahmen erforderlich
  - Technische und organisatorische Maßnahmen
  - Für Notebook und „Kleingerätezoo“ eigene Nutzungsrichtlinien erforderlich

- **Unser Thema:** Der **„Kleingerätezoo“**

Unsere mobilen Endgeräte

- **Mobile Endgeräte** sind **Smartphones**, Tablets und Phablets, die mit einem für den mobilen Einsatz angepassten Betriebssystem ausgestattet sind (z. B. Android, iOS, Windows Phone oder BlackBerryOS). Tragbare Computer mit Betriebssystemen für den Desktopbereich (Notebooks) liegen außerhalb der Betrachtung

Klassischer Client

- **Arbeitsplatzrechner = PC** und **Notebook**
- Nach Hardwarekauf kann beliebiges Betriebssystem installiert werden. Gerät durch Administrator vollständig anpassbar.
- Anwender entscheidet, wann Betriebssystemupdates installiert werden.
- Meist homogene Gruppe von Client-Geräten, z. B. Windows Desktop-PC.
- Vorhersehbare Gegebenheiten → (möglichst) einheitliche Client-Hardware und Anwendungen
- Einheitlichkeit der Netzwerkgeräte
  - Zentraler Zugang über Unternehmensfirewall zum Internet
  - Arbeitsplatzrechner hat nur Netzzugang über LAN
- Einsatz im Firmennetz

Der “Kleingerätezoo“ = Smartphone,Tablet,Phablet

- Hardware wird zusammen mit dem Betriebssystem erworben
  - Nur das vom Hersteller gelieferte Betriebssystem funktioniert
- Kontrolle
  - Hersteller des Betriebssystems hat gewisse Kontrolle über das Gerät, da er das Betriebssystem kontrolliert
- Updates
  - Anwender allein entscheidet nicht über die Durchführung von Updates, da der Hersteller diesen Prozess kontrolliert. Bei android-basierten Geräten ist auch häufig der Mobilfunkanbieter eingebunden, da er die Updates des Herstellers noch anpasst und danach erst an seine Kunden weitergibt.
- Breitgefächerter Zugang zu Ressourcen möglich
  - WLAN, UMTS, LTE, Bluetooth
- Einsatz an unterschiedlichsten Orten
- Vielzahl unterschiedlicher Geräte
- Benutzerfreundliche Consumer-Technologie → Steigerung der Produktivität

Vergleich mobiles Endgerät – klassischer Arbeitsplatzrechner (1)

- **Mobile Endgeräte sind grundlegend anders** in ...
  - Beschaffung
  - Betrieb
  - Benutzung und
  - Systempflege

... als ein klassischer Arbeitsplatzrechner.

Vergleich mobiles Endgerät - klassischer Arbeitsplatzrechner (2)

- **Mobile Endgeräte bergen zusätzliches Gefahrenpotential** durch ...
  - die Möglichkeit, die Geräte immer und überall dabei zu haben
  - die ständige Verbindung mit dem Internet
  - die ständige Verbindung mit dem Firmennetzwerk
  - viele Schnittstellen
  - die sensiblen Unternehmensdaten, die auf dem Smartphone gespeichert sind (besonders hohes Risiko)

- **Fazit**: Mobile IT-Geräte haben einen höheren Schutzbedarf als stationäre Computer, insbesondere wenn darauf vertrauliche Informationen gespeichert werden.

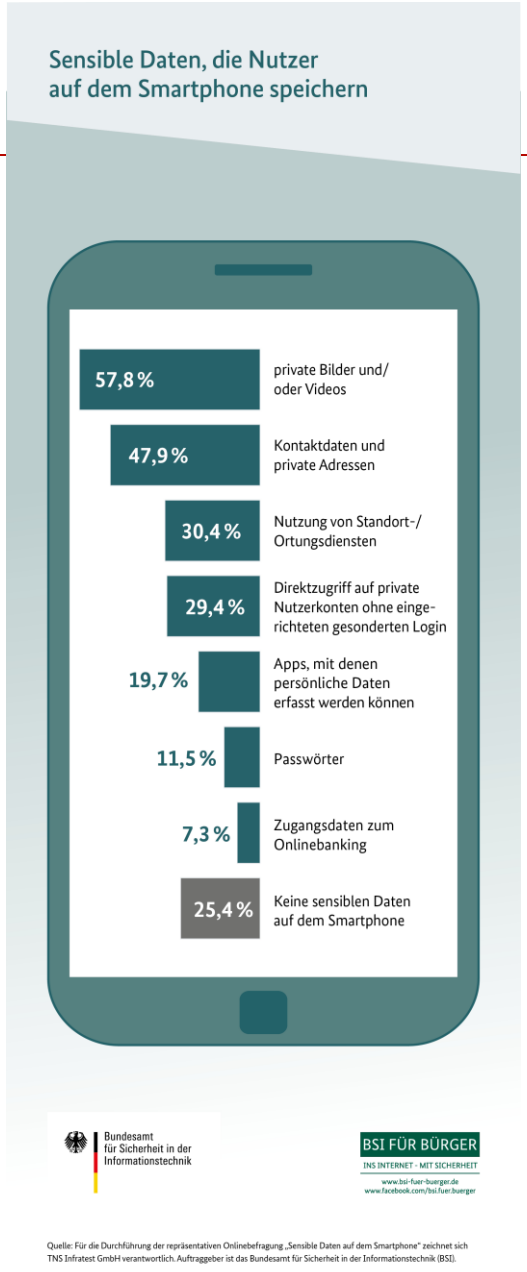
- Spezielle Herausforderung für den Handwerksbetrieb:
  „**Und wie geht das ohne IT-Abteilung und Administrator?**“

Herausforderungen beim Einsatz mobiler Endgeräte

- Produktvielfalt im Betriebseinsatz (Heterogenes Betriebsumfeld)
  - IT-Abteilungen müssen mobile Geräte in vielen unterschiedlichen Ausführungen (Geräte unterschiedlicher Hersteller und mit verschiedenen Betriebssystemen) bereitstellen, pflegen und dabei gleichzeitig für eine angemessene Sicherheit sorgen.
- Erhöhte Gefährdungen
- Die Administration unterscheidet sich in grundlegenden Punkten von anderen IT-Systemen.
- BYOD
- Consumerization der IT

Anmerkung: Consumerization der IT = Einfluss privat genutzter Consumer-Geräte auf IT-Lösungen im Unternehmen

Das Smartphone und seine Datenschätze



BSI-Umfrage in 2016

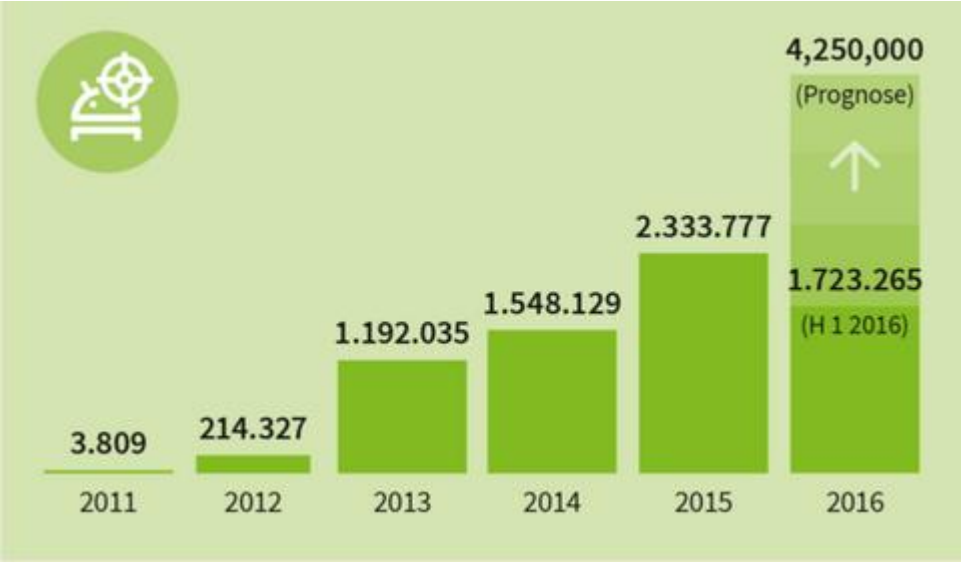
Fakten (1)

- **Googles Android dominiert mit 80%-Marktanteil den Smartphone-Markt**

- **Veraltete Betriebssysteme**
  87 % der Android-Nutzer hatten im Juni 2016 ein veraltetes Betriebssystem auf ihrem Smartphone oder Tablet. Bedenklich sind die **ausbleibenden Sicherheitsupdates**.

- Laut Google: **25 %** der genutzten **Android-**Geräte laufen noch mit **Version 4.4**.

- **Entwicklung Schaddateien**
  Bereits **1.723.265 neue Android-Schaddateien** im ersten Halbjahr 2016



Quelle und Bild: GDATA

Fakten (2)

- In Sachen Sicherheit eilt **Android** ein **schlechter Ruf** voraus – manchmal zu Recht.
  - **Sicherheits-Patches** (z. B. regelmäßige Sicherheitsupdates nur für Top-Geräte)
  - **Updates** (keine für ältere und / oder preiswerte Geräte)
  - **Zwei-Klassen-Gesellschaft**

- Nie zuvor waren **Daten** und **Mitarbeiter** so **mobil** und **losgelöst von Standort** und **Gerät**.

- Nie zuvor waren die **Grenzen** zwischen Unternehmensnetzwerk und dem Rest der Welt so **durchlässig**.

- Die Gefahren beim Einsatz mobiler Endgeräte werden oft unterschätzt.

Fakten (3)

- Der mobil arbeitende Mitarbeiter, der lediglich rudimentäre Sicherheitsmechanismen nutzt und hochbrisante Firmeninformationen auf seinem Mobilgerät gespeichert hat, ist natürlich für professionelle Datendiebe ein extrem lohnendes Angriffsziel.

- Trotz alledem: Die Nutzung mobiler Endgeräte im Unternehmen bringt Vorteile. Beispiele: mobiler Zugriff auf Unternehmensressourcen weltweit, E-Mails, Kalender und Benachrichtigungen abrufen.

- **Wir müssen uns aber auch immer die Frage stellen, ob der hohe Grad der Vernetzung in allen Bereichen des Lebens sinnvoll ist.**

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

- Es ist nicht die Frage, **ob** Sie angegriffen werden können, sondern **wann** Sie gehackt werden.

- Cyberkriminelle dringen nicht ausschließlich über das Internet in IT-Infrastrukturen ein. → Gefahr geht von Innen aus

- In jedem zweiten der betroffenen Unternehmen liegt die Ursache bei aktuellen oder ehemaligen Mitarbeitern, die die Schadsoftware in das System einschleusen – bewusst oder unbewusst.
  → Faktor Mensch: größte Gefährdung durch den (ehemaligen) Mitarbeiter

- Beispiele:
  - Mitarbeiter finden und nutzen USB-Sticks, die von Angreifern manipuliert und extra platziert wurden.
  - Diebstahl: Mitarbeiter speichern sensible Daten auf externe Datenträger und nehmen sie an sich.

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

2. Gefahren beim Einsatz mobiler Endgeräte

Mögliche Schäden

- **Sabotage**
  - Verfälschung von Daten
  - Ausfall oder Einschränkung der Funktionsfähigkeit wichtiger IT-Systeme
  - Ausfall, Zerstörung bzw. Manipulation von (Produktions-) Maschinen
  - Störung der Betriebsabläufe
- **Verlust von Daten**
  - Datenklau (hier speziell Unternehmensdaten und private Daten)
- **Spionage**
  - Verlust der Vertraulichkeit wichtiger Unternehmensdaten
  - Kundendaten und andere sensible Unternehmensdaten
    - Forschungs- und Entwicklungsergebnisse, Strategiepapiere, Einzelheiten von Verträgen, Angebote und Preiskalkulationen, die Korrespondenz mit Geschäftspartnern, Informationen über die Besonderheiten der Unternehmens-IT, Zugangsdaten,...
- **Verletzung des Datenschutzes**

Mögliche Folgen

Produktionsverzögerung oder **Lieferverzögerungen**

Auftragsverlust

Kundenverlust

spürbare finanzielle Einbußen

Insolvenz

Jedes Smartphone lässt sich komplett übernehmen

Jedes Smartphone lässt sich komplett übernehmen. - YouTube

https://www.youtube.com/watch?v=9rkqoN_rspw

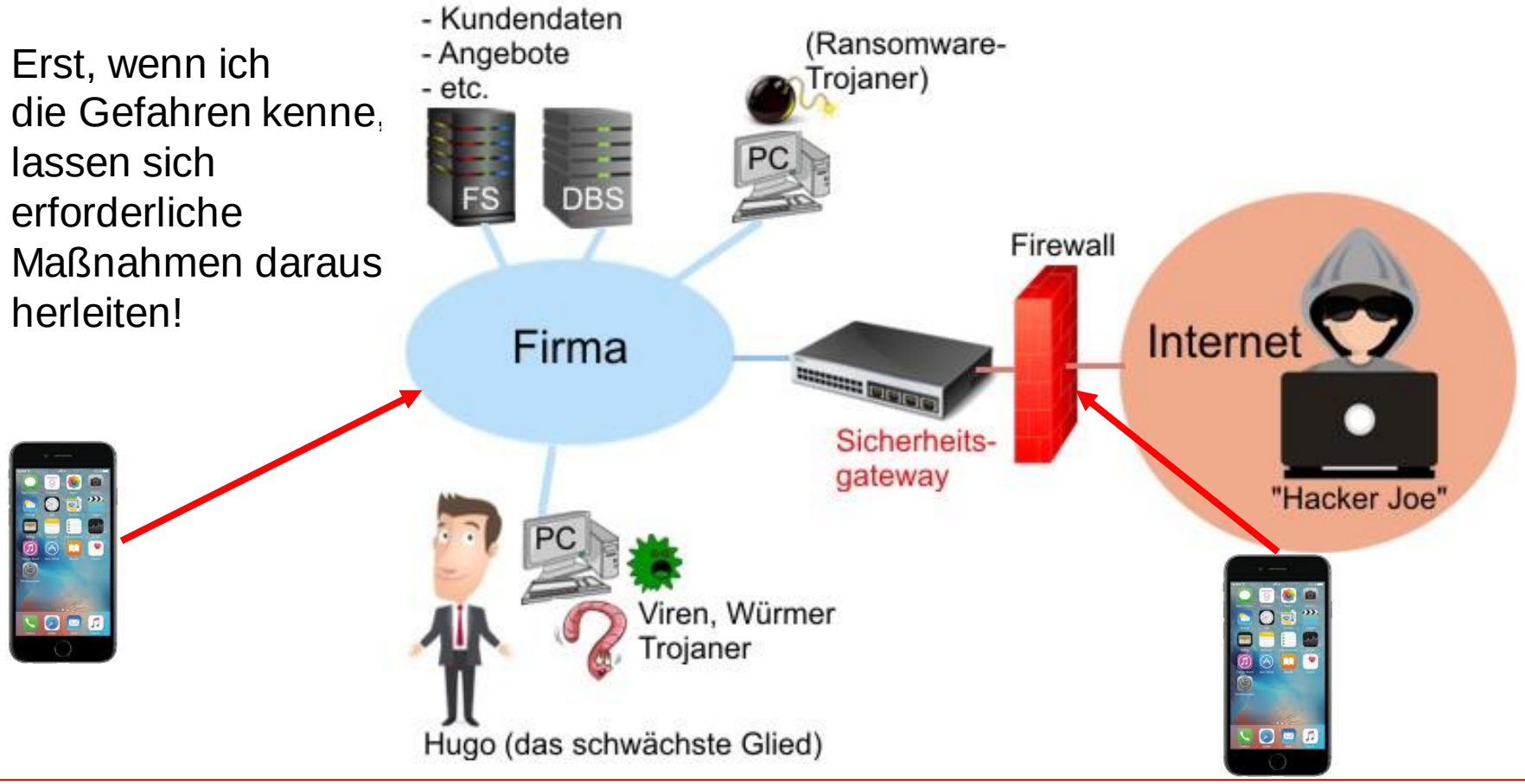
09.03.2017 - Hochgeladen von MrGogeln

For educational purposes only! Android-Hack: **Jedes Smartphone lässt sich komplett übernehmen** ...

Gefahren für Daten, IT-Systeme und Maschinen

- **Gefahrenpotentiale** = a)Bedrohungen und Sicherheitslücken b)Risiken

- Erst, wenn ich die Gefahren kenne, lassen sich erforderliche Maßnahmen daraus herleiten!



Die größte Gefahr: Schwachstelle Mensch

- **Social Engineering**
  - Cyberkriminelle setzen zunehmend auf Angriffe, bei denen nicht Schwachstellen in der Software ausgenutzt werden, sondern die Leichtgläubigkeit von Personen. Via Social Engineering können sich Bedrohungen, wie die so genannte Ransomware, rasant verbreiten.

Quelle: heise.de

Höhere Gefährdung im Vergleich zum stationärem PC

- Nutzung auch außerhalb des Firmengeländes
- Angriff auf das mobile Endgerät auch außerhalb des Firmengeländes möglich
  - Gerät ist immer und überall dabei und verfügbar
- ständig mit dem Internet verbunden
- sensible (vertrauliche) Daten gespeichert
- Opt. ständige Verbindung mit dem Firmennetzwerk
- Viele Schnittstellen
- Mobile Endgeräte sind nicht für den Unternehmenseinsatz sondern für den Consumer-Einsatz entwickelt

„Mittlerweile entsprechen die mobilen, internetfähigen Geräte kleinen Computern, auf denen gearbeitet, kommuniziert und vertrauliche Daten gespeichert werden. Dadurch gelten für sie mindestens die gleichen Sicherheitsanforderungen wie für stationäre Computer. Die Sicherheit spielt im Grunde sogar eine noch größere Rolle, denn die Möglichkeit, die Geräte immer und überall dabei zu haben und sie ständig mit dem Internet zu verbinden, birgt zusätzliches Gefahrenpotenzial.“

Gefahren beim Einsatz mobiler Endgeräte

- Gefahren durch **Überwachung**
  - Bewegungsprofile können erstellt werden
  - Problematisch: Datenschutz
  - Ständige Überwachung möglich (gewollt oder ungewollt)

- Gefahren durch **Datendiebstahl**

Quelle: Handysektor,www.handysektor.de

Gefahren durch **Schadsoftware (Malware)**

- **Ausspähen von Daten** wie z. B. E-Mails, Anmeldedaten und vertrauliche Dokumenten
- **Verursachung hoher Kosten** durch den Versand von SMS-Nachrichten an (ausländische) Telefonnummern von Premiumdiensten.
- **Ausspähen mobiler Banking-Apps**.
- **Sperren von Geräten, Verschlüsseln von Daten**, um Lösegeld zu erpressen (Ransomware).
- Woher kommt die Schadsoftware?
  - Eingeschleust über installierte Apps, bei Surfen über Browser, Mails inklusive Anhänge
  - Die schädlichen Apps sind schon beim Kauf vorinstalliert (China-Smartphones) oder werden durch mich (Benutzer) installiert

Gefahren durch **spionierende Apps**

- **Apps als Datensammler und Datenschutz-Risiko**
- Wodurch?
  - Nutzung von Apps, die automatisiert und vom Nutzer unentdeckt auf die Daten des Geräts zugreifen.
  - Sensible Daten verlassen das Unternehmen ungewollt, wenn mobile Geräte abhanden kommen.
  - Aber auch mit unserer Erlaubnis werden Daten gesammelt → siehe „fleißige Datensammler“
- Folge
  - Haftungsrisiken der Unternehmensleitung
- Wie vermeiden?
  - Regelungen im technischen und organisatorischen Bereich treffen
  - → *mehr bei Thema Basisschutz für Smartphones und Tablets*

Quelle: Handysektor, www.handysektor.de

Die „fleißigsten Datensammler“

Quelle: c‘t,heise

- **WhatsApp** (gehört zu Facebook)
  - Sendet Telefonbuch, Kontaktdaten, Termine, etc. an Hersteller.
  - Wir erlauben WhatsApp, z. B. die Bildergalerie zu durchsuchen oder das Kameralicht ein- und auszuschalten.
- **Betriebssysteme** (Android, iOS)
  - Android (Datenkrake Google)
  - Standortverlauf aktiviert → sendet regelmäßig Standort an Google (Bewegungsprofil)
  - Lokalisierung auch über die Mobilfunkmasten mit deaktiviertem Standortverlauf möglich
- **Google-Street-View**
- **Internetbrowser**
  - Cookies, Verlauf der besuchten Seiten

Gefahren durch **Verlust** oder **Diebstahl**

- Ärgerlich, wenn ein Smartphone verloren geht oder gestohlen wird
- Jedes Jahr gehen 70 Mio. Smartphones verloren und nur 7 Prozent der Besitzer erhalten ihr Telefon zurück.
- Smartphones sind viel Geld wert und speichern jede Menge privater Daten und evt. Unternehmens-daten

- Tipps: Dieben Zugang zu Daten erschweren.
  - Daten auf dem **Gerätespeicher verschlüsseln** (falls das Gerät das nicht als Werkseinstellung anbietet)
  - Ein **Backup** rettet Ihre Daten
  - **Fernlöschung** zum Schutz ihrer Daten

Quelle: Handysektor,www.handysektor.de

Gefahren beim Einsatz mobiler Endgeräte

- 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 wird mit Spielen und anderen Freizeitbeschäftigungen vergeudet.

- Gefahren durch **private Nutzung** mobiler Endgeräte

- Gefahren durch Bring Your Own Device (**BYOD**)
  oder: *„bring your own disaster“*

Gefahren beim Einsatz mobiler Endgeräte

- Gefahr der **Verletzung der Vertraulichkeit** *(siehe später bei Schutzbedarfsanalyse)*
  - Besondere Risiken sowohl bei der Speicherung und Übertragung von Daten als auch bei der Sprachkommunikation

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

- Gefahren durch **Smartphone-Bots**
  - Steigende Gefahr durch Android-Botnetze
  - https://www.security-insider.de/steigende-gefahr-durch-android-botnetze-a-700303/?cmp=nl-36&uuid=616DE35D-739E-4E51-A630115113B9EBE1

Gefahr der **Verletzung des Datenschutzes**

- Unternehmenseigene Daten, die dem Datenschutz unterliegen, werden Dritten unbefugt zur Kenntnis gebracht.

- Hervorgerufen durch
  - Unbedachten Umgang der Anwender
  - Root/Jailbreak-Malware
  - Normale Apps wie z. B. WhatsApp
  - Mit Malware infizierte Apps
  - (unerlaubte) private und dienstliche Nutzung von Endgeräten

Gefahren im Kontext Mobile Device Management (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

Mobile Device Management (MDM) - Systeme

- Verwaltung mobiler Endgeräte über eine Plattform
- Konfigurieren, Absichern und Bewachen
- Ermöglichen Mitarbeitern einfachen Zugriff auf Unternehmensressourcen wie E-Mail und Dokumente bei gleichzeitigem Schutz des Unternehmensnetzwerks und dessen Ressourcen
- Erledigen geräte- und betriebssystembezogene Aufgabenstellung
  - Entdeckung von Compliance-Verletzungen (Rooting, Jailbraik, Passwortstärke, etc.)
  - Erstellen von Bestandslisten
  - „wipen“ (sicheres Löschen)
  - Zurücksetzen auf Werkseinstellungen
  - Fernlöschung

Doch wie schützt man sich am besten vor Hackern und Datenklau?

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

3. Das Sicherheitskonzept - Strategische Gedanken und Organisatorisches

1. Organisation, Planung und Konzeption
2. Berufliches und Privates auf einem Gerät sicher voneinander trennen
3. Bring Your Own Device (BYOD)

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

3. Das Sicherheitskonzept - Strategische Gedanken und Organisatorisches

1. **Organisation, Planung und Konzeption**
2. Berufliches und Privates auf einem Gerät sicher voneinander trennen
3. Bring Your Own Device (BYOD)

Unkoordinierte „Insellösungen“ vermeiden

Ein ganzheitliches Sicherheits-konzept ist erforderlich!

Wichtigster Faktor und gleichzeitig größte Schwachstelle ist der Mensch!

Organisatorische Mängel lassen sich nicht mit Technik erschlagen!

Das schwächste Glied in der Kette bestimmt die IT-Sicherheit.

Smartphones haben höheren Schutzbedarf als stationäre Endgeräte.

Bild: privat

Ziel: Sensible Daten auf mobilen Geräten schützen

- Schon **einfache Maßnahmen erhöhen das Sicherheitsniveau**
- Sensible Daten („**Kronjuwelen**“) im Unternehmen **klassifizieren**
- Die Empfehlungen sollen das Risiko des ungewollten Abflusses von Daten an Dritte verhindern
- Zusätzliche Anforderungen bei BYOD

Wirkungsvolles Schutzschild

- **Organisatorische Maßnahmen**
  - Im Unternehmen werden klare Vorgaben, Regelungen, Sicherheitsrichtlinien (engl. Security Policies) zum Umgang mit mobilen Endgeräten benötigt, deren Einhaltung zu kontrollieren ist.
  - Anwenderrichtlinien (Dienstvereinbarungen) für mobile Endgeräte
    - Beispiele: Richtlinien für Mitarbeiter zum Umgang und Verhalten, Patch-Management Smartphones, Umgang mit mobilen Datenträgern, usw.
  - Datenklassifizierung. Welche Daten dürfen auf dem Mobilgerät gespeichert werden?
- **Technische Sicherheitsmaßnahmen** → siehe Lebenszyklus
- **Permanente Sensibilisierung der Mitarbeiter für das Thema Informations-sicherheit**
- **Notfallpläne**
  - Für Diebstahl und Verlust. → siehe Lebenszyklus

Zu klärende Fragen – relevante Fakten

- Welche Ziele sollen mit dem Smartphone-Einsatz erreicht werden?
- Daten welcher Klassifizierung liegen auf den Smartphones?
- Auf Daten welcher Klassifizierung wird extern zugegriffen?
- Welche Smartphones werden eingesetzt?
- Welche Gruppen im Unternehmen werden mit Smartphones ausgestattet?

Unternehmensdaten auf dem Smartphone

- oder Welche Daten dürfen auf dem Mobilgerät gespeichert werden?
- Wichtige Regel: **Prinzip der Datensparsamkeit**:
  - Auf dem Mobilgerät so wenig (dienstliche) Daten wie möglich speichern
- Vom Speichern von privaten Daten auf dienstlichen Geräten wird abgeraten
- **Klassifizierung der Unternehmensdaten in Bezug auf die Vertraulichkeit erforderlich = Schutzbedarfsanalyse**
  - Die Schutzbedarfsanalyse weist lediglich auf einen typischen Schutzbedarf hin, der tatsächliche Bedarf ist jedoch vom Inhalt der Daten abhängig und kann vom Empfohlenen abweichen
- Bestimmte Daten sind ungeeignet für die Speicherung zur mobilen Nutzung → Richtschnur bildet der Schutzbedarf

Datenklassifizierung=Schutzbedarf der Informationen ermitteln

Informationsbestand	Bewertung	Typischer Schutzbedarf
Personaldaten mit Gehaltsinfos, Fehlzeiten etc.	Sehr sensible Informationen mit sehr hohen Vertraulichkeitsanforderungen.	Sehr hoch
Leistungsverzeichnisse, Lagerinformationen	Geringe Vertraulichkeitsanforderungen, da sie teilweise öffentlich verfügbar sind. Dort, wo sie unternehmensspezifisch sind, würde bei unberechtigten Zugriffen kein Schaden entstehen.	Keiner
Kalkulationen	Sensible Informationen. Die Vertraulichkeitsanforderungen sind hoch, da die Informationen das Know-how der Firma repräsentieren und eine Konkurrenzvorteil bieten können.	Hoch
Kundendaten (Adressdaten, Angebote, erbrachte Leistung und Umsätze)	Dies sind sensible Informationen mit hohen Vertraulichkeitsanforderungen.	Hoch
Buchhalterische Daten	Die sind sehr sensible Informationen. Die Vertraulichkeitsan-forderungen sind sehr hoch	Sehr hoch
Private Daten	Gehören nicht auf das Dienstgerät!	Normal bis hoch

Eignung der Daten für mobile Nutzung (Speicherung)

- Für personenbezogene Daten (sowohl mit dienstlichem als auch privatem Bezug) gelten die Bestimmungen des Datenschutzes.
- Auch Daten ohne Personenbezug können einen sehr hohen Schutzbedarf haben (z. B. auf Grund von Geheimhaltungsvereinbarungen)
- Der Schutzbedarf der Daten wird grundsätzlich hinsichtlich der drei Schutzziele ***Verfügbarkeit***, ***Integrität*** und ***Vertraulichkeit*** differenziert bestimmt. Entsprechend differenziert müssen Vorkehrungen zur Sicherheit der Daten getroffen werden.
- Aus dem Schutzbedarf der Daten folgt zwingend die Eignung oder Nicht-Eignung zur Speicherung auf dem Mobilgerät
- Tipp: Möglichst alle Daten verschlüsseln, inklusive auf Zusatzspeicherkarte

Schutzbedarf	Eignung mobile Speicherung
Daten mit keinem bis normalen Schutzbedarf	Ja
Daten mit hohem Schutzbedarf	nur verschlüsselt
Daten mit sehr hohem Schutzbedarf	**nein**

Sicherheitsrichtlinien für mobile Endgeräte (1)

Quelle BSI:

„**Bevor mobile Endgeräte in eine Unternehmensstruktur eingebunden werden können, müssen klare Regeln für die Integration festgelegt werden**. Mit diesen **Sicherheitsrichtlinien**, den sogenannten Security Policies, werden u. a. die Rahmenbedingungen bezüglich Auswahl der Geräte, Auswahl der Daten, die auf den Geräten verarbeitet werden dürfen, Einschränkungen der Benutzer und Limitierung der Möglichkeiten der Geräte (Hardware wie Software) festgelegt.

Neben den Sicherheitsrichtlinien ist auch eine **Dienstvereinbarung** mit einer klaren Darstellung der Rahmenbedingungen für die Verwendung der mobilen Endgeräte notwendig.“

Sicherheitsrichtlinien für mobile Endgeräte (2)

- **Wir brauchen klare Regelungen für die dienstliche Nutzung von mobilen Endgeräten**
- **Sicherheitsrichtlinien** = Nutzungsrichtlinien für mobile Endgeräte
- Sinnvoll ist die gemeinsame zeitgleiche Einführung von Richtlinien und mobilen Endgeräten
- „Viele Nutzer mobiler Endgeräte sind keine IT-Spezialisten und müssen deshalb über Vorgaben zur sicheren Verwendung der mobilen Endgeräte angeleitet werden“
- Anwender sollen die Richtlinien als nützliche Unterstützung empfinden
- Herausforderung: Richtlinien entwickeln, die die Anwender akzeptieren
- Richtlinien können von anderen Unternehmen nicht exakt übernommen werden. Jedes Unternehmen muss seinen Regelungsbedarf im Rahmen seiner Unternehmenskultur ermitteln. Übernahme innerhalb einer Branche aber möglich
- **Dienstvereinbarung**: Rahmenbedingung für die Verwendung

Mögliche Themenbereiche für Richtlinien (1)

- **Verhalten** bei
  - Nutzung der Smartphones (allgemein)
    (Schutzfolien gegen unbefugte Einsichtnahme, Gerätesperre, usw.)
  - Nutzung im Inland
    (Verhalten bei öffentlichem WLAN, Umgang mit der Kamera, Verbot von Aufzeichnungen, Sperren von Rufnummern, usw.)
  - Nutzung im Ausland
  - Verlust des Smartphones
    (vorbeugende Maßnahmen, Verhaltensregeln bei Verlust)
  - Nutzung von Apps
    (Einschränkung der Nutzung oder verbotene Apps)
  - Privater Nutzung (falls erlaubt)
- Zulassung bzw. Verbot von Diensten *(z. B. keine Überweisungen)*
- Umgang mit sozialen Netzwerken (Social Media)

Mögliche Themenbereiche für Richtlinien (2)

- Festlegung von Nutzerprofilen
- Änderungen der vorgegebenen Konfiguration
- Einstellungen zum persönlichen Schutz der Anwender
  (Ausschaltung der Ortung, Verschlüsselung, Regelungen der Erreichbarkeit usw.)
- Regelung des Umgangs mit personen- und ortsabhängigen Daten
  - Auf den mobilen Endgeräten
  - Auf den IT-Systemen für Verwaltung und Betrieb der Geräte
- Regelungen zur Arbeitszeit
- Regelungen zur Gesundheitsvorsorge
- Spezielle Regelungen für Administratoren
- Gerätespezifische Regelungen
  - Rücknahme und datenschutzkonforme Vernichtung

Beispiel: Empfehlungen zum dienstlichen Umgang mit Mobilgeräten

Der Westfälischen Wilhelms-Universität Münster:

1. Absicherung des Gerätes gegen unbefugten Zugriff
2. Umgang mit Betriebssystem und Apps
3. Abruf von E-Mails, Kalender, Adressbuch
4. Nutzung von Cloud-Diensten
5. Verlust des Gerätes
6. Ausmusterung von nicht ausreichend abzusichernden Geräten

Absicherung des Gerätes gegen unbefugten Zugriff

Grundsätzlich sollten folgende Sicherheits-Regelungen beachtet werden:

- Sperrung des Gerätes mithilfe einer PIN bzw. eines Kennwortes
- Automatische Sperrung des Gerätes bei Inaktivität
- Festspeicher des Gerätes verschlüsseln, falls Daten mit hohem Schutzbedarf darauf gespeichert werden, ebenso Zusatzspeicherkarten
- Sichere Verwahrung des Gerätes und keine Weitergabe des entsperrten Gerätes an Dritte
- Nicht benötigte Schnittstellen bei Nichtbenutzung deaktivieren
- Gerät nicht über den USB-Anschluss an unbekannte Quellen anschließen; auch nicht um den Akku des Gerätes zu laden (z. B. öffentliche Ladestationen an Flughäfen)
- Bei Verwendung von öffentlichen, ungesicherten Netzen (z. B. WLAN-Hotspot) sichere verschlüsselte Verbindung nutzen (z. B. VPN)

Umgang mit Betriebssystem und Apps

Jeder Nutzer sollte bei der Installation und Verwendung von Betriebssystem und Apps folgendes beachten:

- Regelmäßiges Aktualisieren des Betriebssystems und aller installierten Apps
- Installation eines empfohlenen Virenschutzes
- Installation von Apps nur aus den offiziellen App-Stores (z. B. Google Play bei Android und App Store bei iOS)
- Überprüfung der Nutzungsbedingungen einer App
  - Apps, die nur für den Privatgebrauch kostenfrei zur Verfügung stehen, müssen für kommerzielle Nutzung und dienstliche Zwecke gegebenenfalls ordnungsgemäß lizenziert werden
- Überprüfung der Berechtigungen einer App bei Installation
  - Apps, die unnötigen Zugriff auf (dienstliche) E-Mails, Adressbuch oder Kalender erfordern, sollten vermieden werden
- Löschung von Apps, die nicht (mehr) benötigt werden
- Verzicht auf Jailbreak (iOS) oder Rooting (Android)

Abruf von E-Mails, Kalender, Adressbuch

- Um dienstliche E-Mails, Kalender und Adressbuch zu synchronisieren, sollte ausschließlich der betrieblich implementierte Weg (sicheres Verfahren) verwendet werden.
- Der Abruf der dienstlichen E-Mails über IMAP oder POP3 sollte vermieden werden

Nutzung von Cloud-Diensten

- Cloud-Dienste sollten entsprechend einer Cloud-Richtlinie verwendet werden
- Separates Thema

Verlust des Gerätes

- Umgehend den IT-Administrator oder für die im Betrieb für dienstliche Mobilgeräte zuständige Person informieren
- Der Nutzer sollte unmittelbar seine Passwörter von betrieblich verwendeten Kennungen ändern, um eine unberechtigte Nutzung auszuschließen
- Der Nutzer kann bei Bedarf selbständig sein Gerät aus der Ferne auf Werkseinstellungen zurücksetzen und damit sensible Daten auf dem Gerät löschen. Daten auf Zusatzspeicherkarten werden u. U. nicht bei jedem Gerät gelöscht.
- Eine Fernlöschung darf nur durch den Benutzer oder mit seiner Zustimmung erfolgen

Ausmusterung von nicht ausreichend abzusichernden Mobilgeräten

- Mobilgeräte, die nicht hinreichend abgesichert werden können, sollten nicht mehr zu dienstlichen Zwecken oder mit dienstlichen Daten genutzt werden und fachgerecht ausgemustert werden.

  → Sichere Löschung der darauf vorhandenen Daten

  → (Lebenszyklus) Entsorgung

Verantwortlichkeit

- Auszug aus „Empfehlung zum dienstlichen Umgang mit Mobilgeräten“:
  ... Alle Nutzer eines Mobilgerätes sind für die Absicherung ihres Gerätes und der darauf befindlichen Daten in der Regel selbst verantwortlich. Durch den Nutzer muss sichergestellt werden, dass eine qualifizierte Person die Verantwortung für sachgerechte Betreuung übernimmt. Dies kann grundsätzlich auch der Nutzer selbst sein, alternativ kann die Administration durch eine ausgewiesenen IT-Administrator der ihn DV-technisch betreuenden Einrichtung erfolgen.

  Für dienstlich genutzte Privatgeräte gelten zusätzlich alle allgemeinen Regelungen zu Datenschutz und Datensicherheit

  ??? Wie soll das im Handwerksbetrieb gelöst werden ???
- **Tipp: Zuständigkeiten klären und dokumentieren**

Zugang des mobilen Endgerätes zum Firmennetz

- Firmen-WLAN als separate Sicherheitszone
- Auf Netzwerksegmentierung achten
- Nur registrierten Mobilgeräten Zugang erlauben
- GAST-WLAN für Kunden
- Zugriff auf Ressourcen im Unternehmensnetz vom WLAN über Firewall steuern

- Wichtig: **rein private Smartphones sollten nie Zugang zum Unternehmensnetz erhalten**
- Höchstens Gast-WLAN des Unternehmens für Internetanbindung (E-Mail u. Surfen)

Fernzugriff auf das Firmennetz über Internet

- Auf sicheren Fernzugriff auf Firmendaten achten
- Siehe Vortrag: „Lösungen für sicheren Fernzugriff auf die Unternehmensdaten“

Unterwegs im WLAN (öffentliche Hotspots)

- Keine öffentlichen HotSpots verwenden (wenn erforderlich über VPN)
- Im ICE niemals ohne VPN
- Offene WLANs ohne VPN – No Go!
- Auch in verschlüsselten WLAN-Netzen müssen Sie dem Betreiber des LANs dahinter bzw. dem Provider vertrauen – also auch dort besser VPN (allerdings Vertrauen zum VPN-Provider erforderlich)
- Guter Rat: WLAN immer dort ausschalten, wo es nicht gebraucht wird
- Auch in Mobilfunknetzen schadet VPN nicht!

Sensibilisierung der Benutzer

- **Mitarbeiter über den sicheren Umgang mit mobilen Geräten aufklären und für das Thema Informationssicherheit sensibilisieren.**
- Benutzer für Sinn und Zweck der Sicherheitsmaßnahmen sensibilisieren.
- Benutzer verpflichten, die Konfigurationseinstellungen nicht zu verändern.
- Es ist entscheidend, dass die Anwender die Smartphone-Richtlinien als „persönliches Schutzschild“ akzeptieren.

Auswahl und Beschaffung

- Unterschiedliche Grundvoraussetzungen in der iOS- und Android-Welt

- Die Technik der Smartphones ist sehr unterschiedlich, sodass eine Einigung auf möglichst einen Hersteller und nur wenige Gerätetypen vorteilhaft ist. Andernfalls ist der Betrieb der Geräte wirtschaftlich nicht tragbar.

- Smartphones, bei denen Hard- und Software von einem Hersteller kommen, bieten ein höheres Maß an Sicherheit als andere Geräte.

- Tipp: **Möglichst einheitliche Modelle eines Herstellers wählen**
  „Ihr Dienstfahrzeugpark ist auch meist homogen aufgestellt“

Vergleich mobiler Betriebssysteme

	iOS	Android	Windows Phone
Apps und Stores			
Name des Stores	Apple App Store	Google Play	Windows Phone Store
Bezahlung	Kreditkarte, Gutscheine, PayPal, Lastschrift (via ClickandBuy), "iTunes-Geschenk"	Kreditkarte, Geschenkkarten, Gutscheincodes, Telefonrechnung (T-Mobile, Vodafone, O2), PayPal	Kreditkarte, PayPal und Microsoft Points
Benutzerkonto	Apple ID	Google-Konto	Microsoft-Konto
Verfügbare Apps	2.000.000 (08/16)	2.357.497 (08/16)	669.000 (06/16)
Prüfung der Apps	Vor Veröffentlichung	Evtl. nach Veröffentlichung	Zertifizierung vor Veröffentlichung
Besonderheiten	Bindung an iTunes		Apps testen möglich
Weitere Stores?	Nein	Ja, z. B. Amazon App Store, F-Droid	Nein

Vergleich mobiler Betriebssysteme

Gerätevielfalt

Sicherheitsproblem

Geräte			
Auswahl	Kleine Geräteauswahl: Nur iPhones	Viele Geräte von unterschiedlichen Herstellern in allen Preisklassen	Viele Geräte von unterschiedlichen Herstellern
Erweiterungen	Kein Speicherkartenslot, eingeschränkte Bluetooth-Funktionen	Je nach Gerät viele Schnittstellen	Speicherkarten erst ab Version 8 unterstützt
Betriebssysteme			
Bedienung	Sehr einfach und intuitiv	Einfach, aber von Gerät zu Gerät leicht unterschiedlich	Sehr einfach, intuitiv, performant
Updates	Häufig, neue Funktionen auch für ältere Modelle	Teils lange Wartezeiten, bis Hersteller angepasst haben oder gar keine Updates mehr	Einheitliche Systemupdates
Hinweise	Kein Flash, wenige Anpassungen	Individuelle Anpassungen der Oberfläche	Kein Flash, keine Offline-Synchronisation

Benutzergruppen für mobile Endgeräte

Benutzergruppe 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.

Benutzergruppe 2:

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

Nutzungsszenarien

Benutzergruppe 3:

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

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

Lösungen …

- **Mobile Device Management** (MDM) → Gerätemanagement ist die Basis
  (erforderlich ab Benutzergruppe 2)

- **Mobile Application Management** (MAM) → Anwendungsmanagement

- **Mobile Content Management** (MCM) → Datenmanagement

- Spezielle Apple MDM-Lösung: „**Apple Configurator**“ für kleinere Unternehmen (kostenlos)

Mindeststandard für MDM vom BSI

BSI veröffentlicht Mindeststandard für Mobile Device Management

17.05.2017 07:46 Uhr – Volker Weber vorlesen

Der Mindeststandard definiert in 40 technischen und organisatorischen Regeln die Anforderungen an MDM-Systeme des Bundes sowie deren Betrieb. Er definiert, welche Richtlinien ein System umsetzen können muss, lässt aber Spielraum bei deren Ausgestaltung.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) nimmt sich des Einsatzes von mobilen Geräten bei Bundesbehörden an: Das vom BSI formulierte Regelwerk betrachtet das Management von Smartphones, Phablets und Tablets mit Android, iOS oder BlackBerry-Betriebssystem, nicht aber solche mit Windows.

Der Mindeststandard benennt lediglich Regeln für das Gerätemanagement, spart aber die eigentlichen Applikationen aus. Überraschenderweise regelt er nicht die Trennung privater und dienstlicher Daten.

Quelle: heisec.de

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

3. Das Sicherheitskonzept - Strategische Gedanken und Organisatorisches

1. Organisation, Planung und Konzeption
2. **Berufliches und Privates auf einem Gerät sicher voneinander trennen**
3. Bring Your Own Device (BYOD)

Einsatzszenarien für Smartphones im Unternehmen

- **Vermischung von geschäftlicher und privater Benutzung**
  - Gemeinsamer Gebrauch der im Betriebssystem integrierten Apps (Kontakte, Kalender, E-Mail-Client, Webbrowser) und/oder vergleichbaren Apps von Drittanbieter
  - Kein brauchbare Ansatz!
- **“Secure Container“**
  - Sämtliche geschäftliche Belange werden in einer abgeschlossenen, gesicherten Einheit bearbeitet. Es handelt sich um Drittanbieter-Apps.
  - Das Smartphone kann außerhalb dieses Containers normal, das heißt ohne spezielle, restriktive Konfiguration verwendet werden.
  - Beispiel: Android for Work, (für private Zwecke) Samsung MyKnox
- **Unterschiedliche virtuelle Maschinen für private und geschäftliche Bereiche**
  - Trennung nicht auf Anwendungsebene sondern auf Betriebssystemebene.

Tipps für gewerbliche Datennutzung auf Smartphones

- **Das Bundesdatenschutzgesetz (BDSG) schreibt eine strikte Trennung von geschäftlichen und privaten Daten auf einem Endgerät vor.**
- Datenverschlüsselung auf Smartphone erforderlich, betrifft auch Zusatzspeicherkarten.
- So wenig wie möglich dienstliche Daten auf dem Smartphone (Prinzip der Datensparsamkeit)
- Möglichst keine vertraulichen (sensible) Informationen speichern
- **Speicherort**
  - Gespeichert auf Server in Firma
  - Notfalls Server in Deutschland (allenfalls EU)
  - Nicht lokal auf dem Smartphone
- **Anbindung an Server**
  - Sichere Anbindung an das Unternehmen
  - Nur über Virtual Private Network (VPN)

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

3. Das Sicherheitskonzept - Strategische Gedanken und Organisatorisches

1. Organisation, Planung und Konzeption
2. Berufliches und Privates auf einem Gerät sicher voneinander trennen
3. **Bring Your Own Device (BYOD)**

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
  - Geräte sind Eigentum des Unternehmens
  - **Personalisierte Endgeräte, Corporate owned – business only (COBO)** bzw. **Corporate owned – personally enabled (COPE)** oder als
  - **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 Endgeräteanwender 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.
  - Achtung! Das Bundesdatenschutzgesetz (BDSG) schreibt eine strikte Trennung von geschäftlichen und privaten Daten auf einem Endgerät vor!

BYOD (1)

- **Vorab**:
  BYOD-Geräten sollte der Zugang zum Unternehmensnetzwerk und dessen Ressourcen verweigert werden, solange sie nicht mit MDM-Funktionen ausgestattet wurden.

- **Berücksichtigung des rechtlichen Aspektes der Geräteverwaltung**
  Diese Geräte sind nicht Eigentum des Unternehmens und damit die Administratoren nicht automatisch zu deren Verwaltung berechtigt.

- **Empfehlung: Endbenutzer-Lizenzvertrag (EULA) für BYOD**
  In EULA die Maßnahmen erläutern, welche das Unternehmen auf dem Gerät durchführen können muss. Der Endanwender kann den Vertrag annehmen oder ablehnen. Bei Ablehnung wird kein Zugriff auf die Unternehmensressourcen gewährt.

BYOD (2)

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?

BYOD (3) – 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!

Bewertung BYOD

- Das Bundesdatenschutzgesetz (BDSG) schreibt eine strikte Trennung von geschäftlichen und privaten Daten auf einem Endgerät vor
- Die neue EU-Datenschutzverordnung erschwert noch mehr die doppelte Nutzung (privat und geschäftlich)
- Neben dem BDSG gibt es eine Fülle anderer deutscher Gesetze, die im Umgang mit BYOD eine Rolle spielen
- Die rechtliche Situation ist bei BYOD so komplex, dass eine ausführliche Rechtsberatung notwendig ist.
- Dieser Aufwand lohnt sich nicht!

NoGo für BYOD im Handwerksbetrieb!

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

6. Vorläufiges Fazit

Auch bei YouTube

Smartphones im Geschäftsalltag nutzen? Aber sicher!

Erstes 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.

Spezielle KDH-Workshops in 2018

1. **Maßnahmen und Checklisten für ein sicheres IT-Netz im Handwerksbetrieb**
   - IT-Sicherheitsmanagement im Handwerksbetrieb
   - Ermittlung der „Kronjuwelen“
   - Organisatorische Maßnahmen
   - Technische Maßnahmen
     - Hardware und Software
     - Kommunikation
     - Systempflege
   - Personelle Maßnahmen
   - Infrastrukturelle Maßnahmen
   - Notfall-Maßnahmen
   - Einsatz von Checklisten

Weitere KDH-Workshops in 2018

2. **Absicherung eines Arbeitsplatzrechners für den Einsatz im Handwerksbetrieb**
   - Härtung Betriebssystem in Theorie und Praxis
   - Sicheres Surfen
   - Systemschutz und –Pflege mit Checklisten
   - Werkzeuge und Tools zur Unterstützung

3. **Absicherung eines Android-Endgerätes**
   - Konkrete Maßnahmen und Konfigurationseinstellungen
   - Einsatz eines MDM in der Praxis

4. **Absicherung eines iOS-Endgerätes für den Einsatz im Handwerk**
   - Maßnahmen und Konfigurationseinstellungen
   - Einsatz eines MDM in der Praxis

Im Webinar: Schutzmaßnahmen nach Lebens-zyklus

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

Vielen Dank für Ihre Aufmerksamkeit