Mobile Geräte im Amateurfunk

Workshop bei OV Wedding, D10 am 30.10.2015

Thomas Osterried DL9SAU D23
dl9sau@darc.de

Download: http://dk0bln.de/wiki/doku.php?id=users:dl9sau:start

Themen

- Dies ist ein Workshop und kein Vortrag. Gegenseitige Tips. Fragen sofort stellen. Vorstellungsrunge; Eure Erwartungen.
- Für unsere Neueinsteiger beginnen wir mit der Vorstellung von Geräten: kleine und große „Smartphones“ und „Tablets“. Die Qual der Wahl der Systeme
- Datentarife; Begriffe GSM / UMTS / LTE; WLAN; weitere Schnittstellen wie Bluetooth
- Internetnutzung: Web, E-Mail, DARC E-Mail-Adresse
- Daten selbst publizieren / wiederveröffentlichen: Zwischen Urheberrecht, Abmahnwahn, Privatsphäre und Datenschutz.
- Wichtige Webseiten für unser Hobby (s. Linksammlung)
- APPs für den Amateurfunk; Tip Amateurfunkwebseiten

Smartphones und Tablets..

- Für jeden Anwendungsfall das richtige Gerät
- Smartphone vs. Tablet; Betriebssysteme; Größe
- Mit Tablets kann man nicht telefonieren.
- Tablets gibt es mit GSM+WLAN oder nur mit WLAN
- Größe: iPhone hatte mit 3,5“ angefangen, ist aber dem Trend der anderen Hersteller gefolgt und hat jetzt 4,7 oder 5,5“. Andere Hersteller bewegen sich auch auf 6" zu.
- Tablets: 8"-13". A4 lesen mit 8" geht nicht ohne Blättern. 13" ist schon sehr schwer und unhandlich. 10" scheint optimal.
- Auflösung: "Retina" (Apple: 217-401 ppi) -> man sieht keine Pixel mehr.

..Smartphones und Tablets

- Die großen Anbieter: Diverse Hardwarehersteller mit Betriebssystem Android (von google, teils mit ihren eigenen Erweiterungen); oder Apple mit IOS

- Tablet Grundsatzfrage (abhängig vom Einsatzort/-art): Tablet mit oder ohne GSM? GSM .. bis LTE? Oder arbeitet man unterwegs über Handy-Freigabe oder UMTS-Ei?
  Beachte iPad: nur die Mobilfunkversion hat einen GPS Chip. GPS will man haben.

- WLAN

  - WLAN sollte 2.4 und 5 GHz haben. 802.11ac ist aktuell.
    Mobile Geräte: idR. 150 MBit 802.11n, 433 Mbit 802.11ac.

  - WLAN: Sichere Einstellungen. Empfohlen: WPA2-PSK mit CCMP (kein TKIP)., kein WPA, kein WEP.
    802.11n (ohne 802.11b) für bessere Performance. Standards sind rückwärtskompatibel.

  - Tip Aktuell: Auf "WLAN Unterstützung für IOS" achten. Bedeutung: bei schlechtem WLAN wird einfach auf GSM umgeschwenkt. Das kann zu mehr Datenverbrauch führen.

- Bluetooth mit BT 4.0. BT macht etwa 2 MBit.

Rund um den Datentarif..

- Tablet TK-Anbieter: Zweitkarte zum bestehenden Handytarif ggf. preislich Attraktiv
  -> nach Angeboten schauen, oder
  anderer Anbieter (anderes Netz, bessere Chancen auf größere Abdeckung)

- TK-Anbieter Überblick z.B.
  http://www.teltarif.de/tarife/handy/prepaid-und-vertrag/internet/?dauermin=0&mb=500&sms=0&smssum=

- Gut sind manchmal Kombinationen: z.B. Familienvertrag, inkl. DSL,
  oder z.B. auf 2 Jahre befristete Sonderaktionen zum Schnäppchenpreis

- Immer drauf achten: Vertragslaufzeit, Kündigungsfrist (sonst Verlängerung um n Monate, oft n = 12), Preissteigerung innerhalb der Vertragslaufzeit, einmalige Setupgebühr.

..Rund um den Datentarif

- Datenvolumen: Richtgröße 500 MB .. 1 GB. Danach erfolgt Drosselung auf 9k6 (vgl. Packet-Radio ;)
  - Großer Einfluß auf Transfervolumen: Video, Voip, Bilder, komplexe Webseiten, Werbung.

Begriffswirrwar:	GSM 2G mit GPRS / Edge	UMTS (3G) mit HSPA+	LTE (4G)
Frequenzen (EU):	900 / 1800	950 / 1900 / 2100 800	1800, 2.6G / 700, 900, 1500
Bitraten	9.6kBit..171.2 / 59.2k..236kBit	384kBit bis 42Mbit	50-150MBit; adv.: 300MBit

- Das gewählte Netz erkennt man am Symbol (G, E, U / H / 3G, 4G)
- Lesetip: https://de.wikipedia.org/wiki/Universal_Mobile_Telecommunications_System

Grundbegriffe Internet

- IP: jeweils 4x8bit Sender -> Empfänger. Bei sog. NAT keine direkte Kommunikation möglich
- Auf IP liegen udp, tcp, icmp oder andere Protokolle.
- DNS: udp oder tcp -> Namensauflösung statt der „rohen“ IP-Adresse.
- ICMP signalisiert Probleme (MTU, ..). Wird für „ping“ und „traceroute“ (-> Diagnose bei Problemen) verwendet.
- TCP: die meisten höheren Protokollschichten verwenden tcp.
- Höhere Protokolle: http für Web, smtp/pop/imap für E-Mail, rtp für Audio/Video, ftp, chat, proprietäre (skype, apple facetime, ..) uvam.
- Mit TLS (vormals SSL) verschlüsselte Protokolle werden mit angehängtem „s“ gekennzeichnet (https, imaps, ..)

WWW - World Wide Web..

- WWW ist das wichtigste Protokoll im Internet geworden
- Mit einem sog. Webbrowser ,,surft" man Webseiten an. Damit man findet was man sucht, bedient man sich sog. Suchmaschinen (z.B. goolge) oder klickt sich von interessanten Artikeln (z.B. aus dem Online-Lexikon wikipedia) durch.
- Webseiten sind codiert in sog. *URL* (Uniform Resource Layer). Beispiel:

http://www.darc.de/d/
http das Protokoll
:// der Trenner
www.darc.de - der Domainname; löst auf die Adresse 85.13.131.248 des DARC-Servers auf
www ist ein Hinweis auf das Protokoll. Muß aber nicht.
Manche arbeiten ohne, manche verwenden auch www2, etc.
Auf ,,.de" endet die sog. TopLevelDomain, de für Deutschland.
,,darc.de": diese Domain hat der DARC bei der de-Registry gemietet.
/ ein Trenner
d/[..] die eigentliche Unterseite, die einen interessier (DARC Distrikt Berlin)

..WWW..

- Inhalte von Web: statische Webseite, Blog, Forum, Wiki, Webmail, „social Media“
- Tracking / Privacy / Werbung / Sicherheit (wie erkennen wir https? Signalisiert der Browser durch ein grünes Zeichen oder Schloß im URL Feld)
- Das Web ist „klickbasiert“ (Maus, Gesten / Touch auf dem mobilen Gerät).
  - Navigation über die Seite oder vor-/zurück-Knopf oder Wischgesten.
  - Links sind oft blau hinterlegt. In modernem design schwieriger zu finden (irgendwas anklickbar, hinter abstrakten Grafiken verbergen sich Navigationsmenus) Das ist nicht ganz einfach für Anfänger.
- Filme, Bilder, VOIP, aber auch Werbung erhöhen Datenvolumen
- Oft nicht erkennbar was Inhalt der Webseite oder Werbung ist. Ungeübte fangen also an in einem Forum zu suchen und landen über einen falschen Klick auf etwas (das eine Anzeige ist) dann ungewollt im Amazon-Shop.

..WWW

- Werbeblocker
  - IOS hat seit IOS 9 auch eine Schnittstelle für seinen Webbrowser Safari
  - Alternative Android Browser wie Firefox und Opera bieten „Plugin“ für Adblocker. Oder auch privacy Browser "ghostery".
- Beachte: ich habe mir diverse weitere Alternativbrowser angeschaut und warne vor Nutzung, weil sie Surfdaten erheben um Nutzerprofile zu erstellen um diese zu verkaufen.

E-Mail..

- Protokolle smtp, pop3 und imap und ihre sichereren Varianten imap+starttls bzw. imaps. Webmail unterschiedlicher Ausprägungen. "ActiveSync" über https. Wir wollen Verschlüsselung, Grundsätzlich.

- Android
  - zwangsweise mit google mail (gmail) verheiratet.
    - Pro: sehr einfach, eine gut funktionierende E-Mail Adresse (@gmail.com) zu erhalten
    - Con: google finanziert sich aus Werbung und erhebt dazu Daten aus Nutzerverhalten und E-Mail-Inhalten
  - Android hat eigenes E-Mail Programm installiert. Alternativempfehlung: k9mail.

- IOS
  - E-Mail Adresse @icloud.com (früher me.com, mac.com).
  - Apple ist teurer, unterstreicht aber, daß sie es genau nicht mit Verkauf von Profilen für Werbung kompensieren.
  - IOS E-Mail Programm ist gut.

..E-Mail

- Problem Spam und Phishing Mail. Sicherheit. Verunsicherung. Niemals nie antworten.
- Internet macht keine anderen Kosten als die zum ISP. Verträge (z.B. Bestellungen im Web Onlineshop) kommen durch beidseitige Willenserklärung zustande die dann verbindlich sind; der Vorgang wird dann i.d.R. über E-Mail abgeschlossen.
  Absolute Vorsicht ist angeraten beim Verwenden einer Kreditkarte - oder komplett meiden.

Cloud und Standorte der Anbieter, Datenschutz, Sicherheit..

- Cloud: android wie apple schieben Daten in die Cloud. Private Daten verlassen also den Rechner (Bilder, Adreßbücher, E-Mail, Dokumente, URLs, Passworte WLAN und vieles mehr).
  Beispiel: s. Liste der Synchronisationsoptionen für google in Android.

- Google lebt von zielgerichteter Werbung und verknüpft das Profil; „dank“ dem Browsercookie der Anmeldung für google-Mail z.B. erkennt google den Surfer wieder. Jegliche Suchanfrage speichert google über viele Jahre. Google durchforstet das E-Mail Konto auch nach Begriffen für zielgerichtete Werbung.

..Cloud und Standorte der Anbieter, Datenschutz, Sicherheit

- Standorte der Anbieter ist USA mit dortigem Rechtsraum. Ganz neue Problematik vor dem Hintergrund der Spionage von NSA, GCHQ und vielen anderen Diensten. http://www.heise.de/newsticker/meldung/Safe-Harbor-Deutsche-Datenschutzbehoerden-wollen-transatlantisch

- => Verschlüsseln, verschlüsseln, verschlüsseln.,,

- Wir“ sind auch nicht besser: Sie BND-Skandal / NSA Untersuchungsausschuß, und das neue Gesetz zur Vorratsdatenspeicherung (-> Der Gesetzgeber suggeriert: Ihr alle seid mögliche Verbrecher, deshalb muß man Eure Verbindungsdaten sammeln, wann Ihr von welchem Standort wie lange mit wem telefoniert habt)

- Beachte auch: Verschlüsselung ist nur ein zeitlicher Schutz. Alle Algorithmen haben ihre Schwächen und wurden bisher in der Vergangenheit alle mit im Laufe der Jahre immer weniger Rechenaufwand „knackbar“ (leistungsfähigere Computer, neue mathematische Erkenntnisse, Erkennen von Designschwächen).

Sicherheit und Privacy der Betriebssysteme..

- Sicherheit Betriebssystem
  - Android: eine Katastrophe.
    google patcht seine eigenen Geräte zeitnah - andere Hersteller aber nicht.
    Samsung hat sich für ein Problem, das mehr als 80% aller Android-Geräte (alt wie aktuell) betrifft, inakzeptable 3 Monate Zeit gelassen.
    -> Eigene Sicherheitsmaßnahmen extrem anstrengend, z.B. fremde WLANs vermeiden.
    Die meisten Android-Geräte auf dem Markt bleiben ungepatcht, weil zu alt und vom Hersteller nicht mehr supported; wir kennen sogar Geräte größerer Hersteller, die frisch auf den Markt kommen, für die zu diesem Zeitbunkt bereits künftige Betriebssystem-Aktualisierungen abgekündigt sind.
  - IOS: vorbildlich.
    Allerdings nur so lange Geräte nicht abgekündigt sind

..Sicherheit und Privacy der Betriebssysteme..

- Sicherheitsupdates von Betriebssystem und Apps
  Die Frage kommt immer wieder: soll man updaten? Ich sage sowohl für Betriebssystem als auch für Apps: ja unbedingt, denn sie schließen mit dem Update ggf. auch wichtige Sicherheitslücken.

- Privacy
  - IOS lässt granularer konfigurieren als Android welche Rechte eine App hat (z.B. ob mein APRS Programm meinen Kalender auslesen darf).

  - Bei Android sieht man bei der Installation was die Rechte sind die der Programmierer sich einräumte. Entweder man akzeptiert (und lebt damit, und vergißt es sogar..) oder man installiert die App erst gar nicht und sucht sympathischere Alternativen.

..Sicherheit und Privacy der Betriebssysteme..

- Apps im Allgemeinen:
  - Werbefinanzierte Apps sind leider bei Android wie IOS anzutreffen. M.E. locken bei Android die Anbieter die Nutzer mehr mit ihren Apps sensible Informationen abfischen zu können.
  - Auf Rechte achten: Android: nur vor Installation einsehbar. IOS: jederzeit nachbesserbar.
  - Unterschiede Software: Bezahl-Apps, Kostenlose Apps, Freie Apps (Source-code einsehbar), Werbefinanzierte Apps.

..Sicherheit und Privacy der Betriebssysteme

- kritische Distanz:
  - Werbung (teils aufdringlich)
  - In-App-Käufe (an der Sicherheit des App-Stores vorbei; Abo-Fallen möglich))
  - Herkunftsland
  - Attraktives Ziel (Beispiel Taschenlampen-App, Spezialthema (Satelliten..)).
- Wir erinnern uns auch an WhatsApp (war sehr gehypted, mittlerweile von Facebook aufgekauft). Sendete ungefragt komplettes Adreßbuch des Telefons an die Firma.
- Werbung und die Folgen
  - Bei Lücken im Betriebssystem: da viele Apps Werbebanner einblenden, kann darüber auch das Betriebssystem angegriffen werden.

Sicherheit OS / Apps

- Android
  - OS Updates nur bei google-Geräten schnell, oder wenn man sein Gerät mit dem Android-Derivat cyanogenmod geflasht hat
  - läßt auch zu, selbst Programme zu installieren (gut für „freie“ Programme).
    Vorsicht: dazu zu verleiten ist ein Angriffsverktor, von z.B. banking trojaner.
  - Alternativer App-Store: f-droid
  - "root" auf seinem System ist man nur mit Alternativ-Android cyanogenmod.
  - Telefonhersteller bringen viele fragwürdige Apps mit, die nicht entfernbar sind, ggf. Sicherheitslücken haben und Dinge im Netz tun obwohl man sie nie gestartet hat(!)
  - Manche Telefonanbieter "Branden" ihr Gerät mit eigner teils schlechter Software
  - Geräteverschlüsselung möglich, aber von Hause aus aus.
  - Backup der Geräte: sehr schlecht. Datenverlust vorprogrammiert!

- IOS
  - IOS wird regelmäßig und recht zeitnah aktualisiert-
  - IOS läßt nur den Apple Appstore zu und behält sich vor Apps aus dem Store zu schmeissen (Unterwerfen der USA Moralvorstellungen (Wlan Scanner, Brüste selbst in Gesundheits-Apps).
    => Bevormundung. Weniger kostenlose Apps für den Amateurfunk verfügbar
  - Kein "root" auf seinem eigenen Gerät.
  - Ein Softwareprojekt muß Jahresbeitrag bezahlen um im Appstore veröffentlichen zu dürfen.
  - Keine Brandings.
  - Geräteverschlüsselung von Hause aus an.
  - Backup der Geräte: sehr gut, sogar re-Installation von alt- zu Neugerät.

Schnittstellen

- Je mehr desto besser? Nein, je freier desto gut.

- Apple machte bluetooth zunächst ganz dicht, fügte später wieder weitere Protokolle des Standards hinzu
  Das serielle Profil SPP gibt es aber bis heute nicht (vgl. Android-Demo APRS).
  Ebenso bei NFC: Android sehr offen; Apple stellt nur eine API für mobiles Bezahlen bereit.

- Geschichte tethering - Einfluß der TK-Anbieter auf die Gerätehersteller.
  - Anfang 2000 war es kein Problem, sein Handy mit dem "DUN" oder "PAN" Profil an sein Notebook freizugeben. Toll für die Industrie, endlich nutzt mal jemand mehr Daten als über WAP.
  - Dann kamen die smartphones. Plötzlich gab es viele Nutzer des überteuerten Mobilfunknetzes. Die Anbieter verkauften gesponserte Smartphones mit 2-Jahresverträgen um die Kunden zu binden. Traffic sollten die Leute mit dem Smartphone machen, um die Netze zu schonen - man untersagte schlicht die Anbindung eines Computers und nahm Einfluß auf die Hersteller, dafür Sorge zu tragen, daß die SIM Karte bestimmt ob der TK-Anbieter beim aktuellen Tarif die Kopplung erlaubt. Das nannte man dann hübsch wie neu "tethering", und ist ein Synonym für kastriertes PAN, und verkaufte es als Mehrwertfeature.

- tetherning Varianten: über Bluetooth (max. 2 MBit) oder WLAN (hotspot). Ich bevorzuge BT.

Urheberrecht, Abmahnwahn, Privatsphäre und Datenschutz..

- Unser Rechtssystem ist so komplex, daß das eine Privatperson kaum durchschaut.
- Während Gesetzgebungsprozessen wirken Lobbyverbände massiv ein um Geld vom Kuchen abzubekommen bzw. ihre Pfründe zu sichern.
- Mit einer typisch deutschen Erfindung „Leistungsschutzrecht“ („Lex Google“) sollen Suchmaschinenbetreiber für das Liefern von Suchergebnissen von Webseiten von Verlagen diesen Geld erstatten - hingegen wird die Leistung von der Suchmaschine als umsonst angesehen. Verkehrte Welt. Wehrt sich der Suchmaschinenbetreiber dagegen indem er deren Inhalte ausblendet, wird wegen Wettbewerbsverzerrung gewettert. Dreister geht’s kaum.
- Jeder Text und jedes Bild hat einen Urheber. In DL ist dieses Recht nicht abtretbar sondern fest mit der Person verbunden. Allenfalls Verwertungsrechte können abgetreten werden. Deshalb ist es wichtig, das eigene Werk (z.B. auch dieses hier) unter eine Lizenz zu stellen.
  Siehe auch: DARC CQ-DL Artikel zum Thema Urheberrecht.

..Urheberrecht, Abmahnwahn, Privatsphäre und Datenschutz

- Eine wahre Abmahnindustrie ist entstanden, die Jagd auf Urheberrechtsverstöße macht.
  Vorsicht: Verwertungsrechte können sich ändern. Unter alten Rechten ins Netz gestellt, gilt es trotzdem als Wiederveröffentlichung unter aktuellen Konditionen. -> Abmahnindustrie.

- Datenschutz / Recht am eigenen Bild
  -> vor Veröffentlichung um Erlaubnis fragen

- nicht bei Personen des öffentlichen Interesses oder bei Großveranstaltungen (Messen, Demonstrationen o.ä.)

- Vereinsmitgliedschaft ist ein datenschutzrechtlich schützenswertes Datum
  -> Keine Mitgliederlisten auf Webseiten stellen.

- Beispiel: OM hat sich krank gemeldet und geht auf den Fieldday, wird fotografiert; Chef findet das Bild im Netz und entläßt den OM.

Empfehlungen Amateurfunk-APPs und -Webseiten

- Amateurfunk-Apps und Links zu Webseiten rund um den Amateurfunk habe ich hier zusammengetragen: http://dk0bln.de/wiki/lib/exe/fetch.php?media=users:dl9sau:2015-10-30--mobile-geraete-im-amateurfunk--lis