Handysicherheit

Für Endanwender

Christoph Weinandt
IT-Stammtisch Darmstadt
2013

Handysicherheit

Profil

Christoph Weinandt

IT-Stammtisch Darmstadt

·Skills:

- CCSA
- CNA

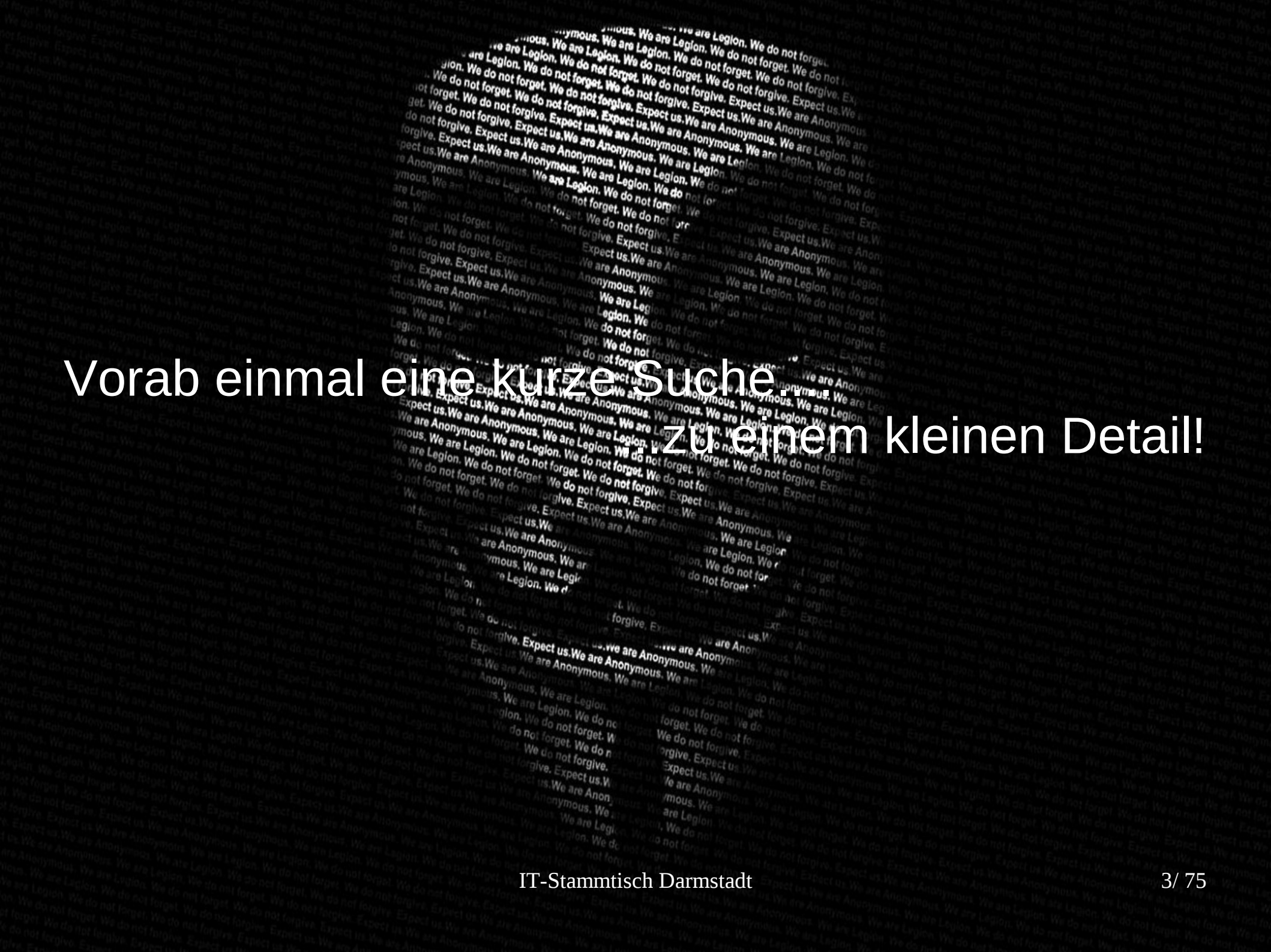
  IT-Sicherheit

  Forensic

  Penetration Testing

  Networking

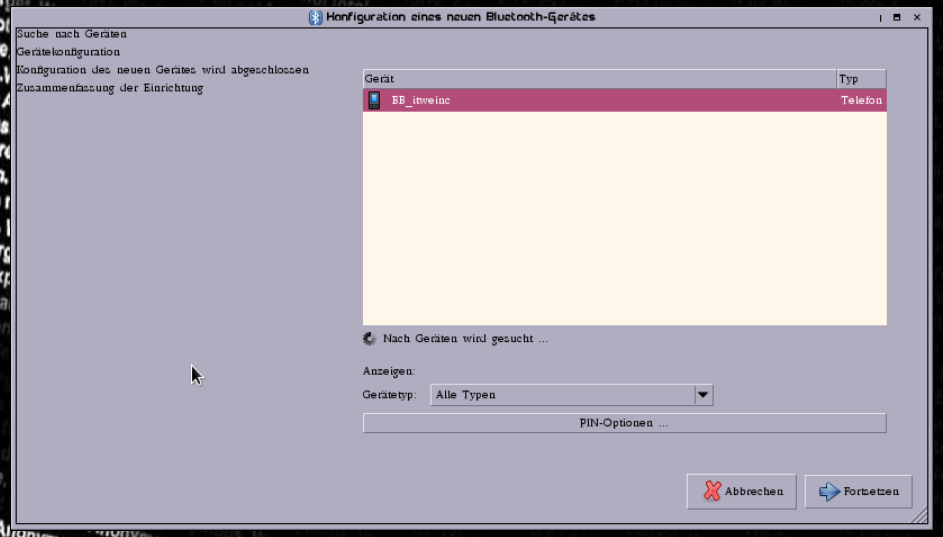
  ITILv3


Vorab einmal eine kurze Suche...
...zu einem kleinen Detail!


Nach Bluetooth Geräten...

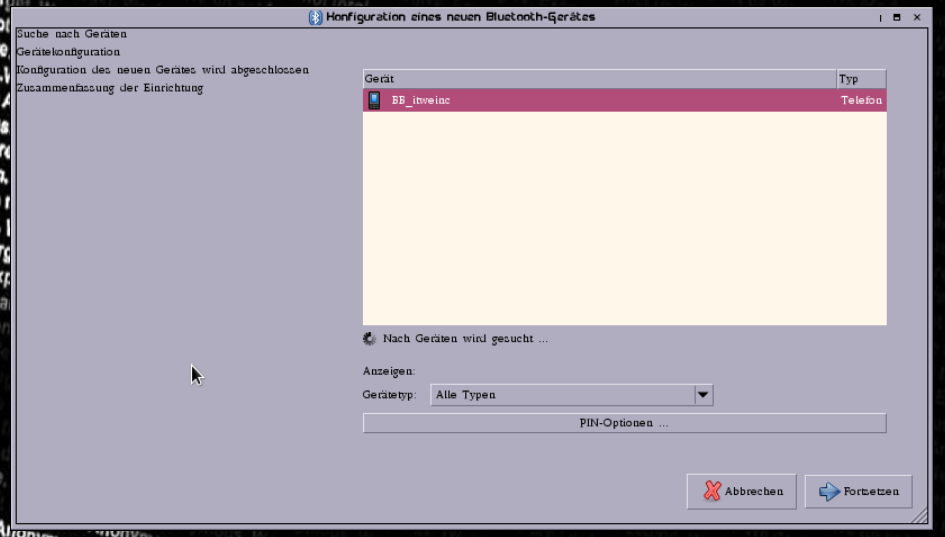
Was haben wir da...

- Gerätename
- MAC Adresse

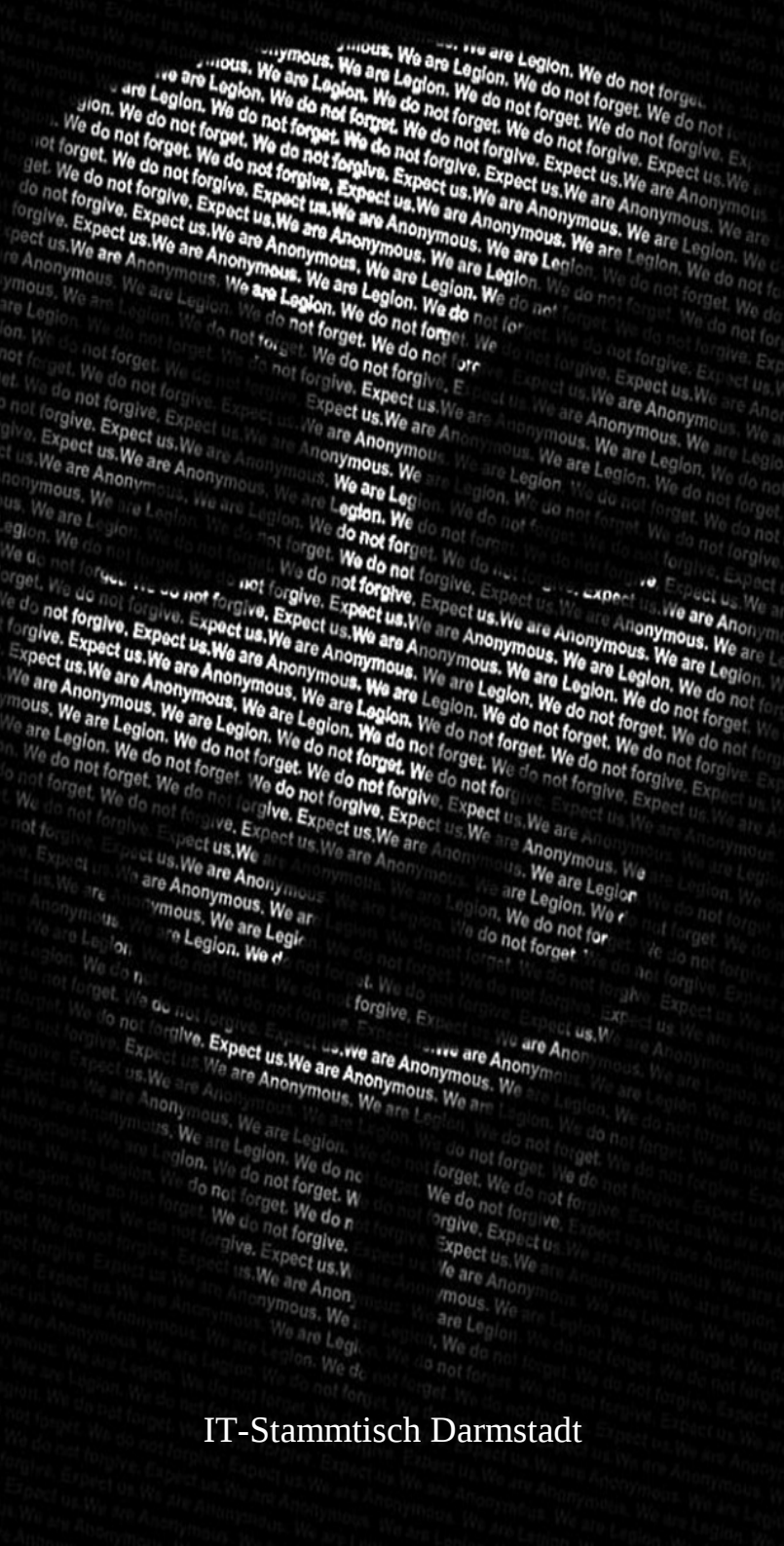


Was ich machen könnte...

- Mich bei Ihnen anmelden
  - BT Headset
- Ihre Daten runterladen
- Ihr Telefonat mithören
- Ihre Musik hören



Mehr davon??


We are Legion. We do not forget. We do not forgive. Expect us.We are Anonymous.

Agenda

- Verwendung von Smartphones im Alltag
- Gefährdungslage
- Anforderungen an die Handysicherheit
- Empfehlungen und Tools
- LiveDemos
- Inklusive Pause ;)

Agenda

Verwendung von Smartphones im Alltag

1994...

- Telefonieren

2013

- Email
- Chat
- Soziale Netzwerke
- Online Bezahlen
- Online Banking
- Internet Radio
- Internet TV
- SMS
- Adressen und Termine
- Cloud Computing
- Telefonieren

Agenda

Vorabinfo´s

Vorabinfo´s

- GSM Standard
  1992
- Verschlüsselung
  abschaltbar
- Kontrolle
  durch Basisstation (BTS)
- Priorität
  nach Signalstärke

Vorabinfos

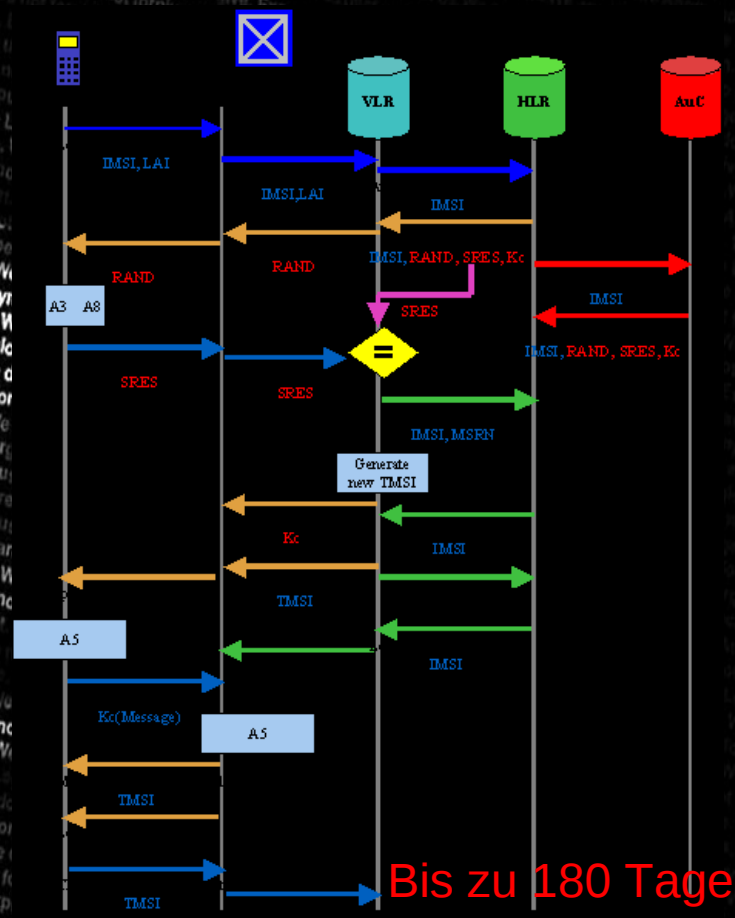
- GSM Anmeldung

  Einbuchung in Providernetz:

  - CID, LAC, IMSI
  - Location Registration VLR/HLR
  - Location Update
  - Ortung des Standorts ist unbedingt notwendig für Telefonfunktion

  Speicherung:

  - CID
  - Uhrzeit
  - IP Adresse
  - IMSI



Vorabinfo´s

- Was wird gespeichert
  - IMSI
  - MSISDN
  - MSRN

Vorabinfo´s

- GSM Sicherheit
  - RAND
  - SRES
  - Kc

Vorabinfo´s

- GSM Datenübertragung
  - GPRS
  - EDGE
  - HSCSD
- UMTS
  - HSDPA
  - HSPA+
- LTE

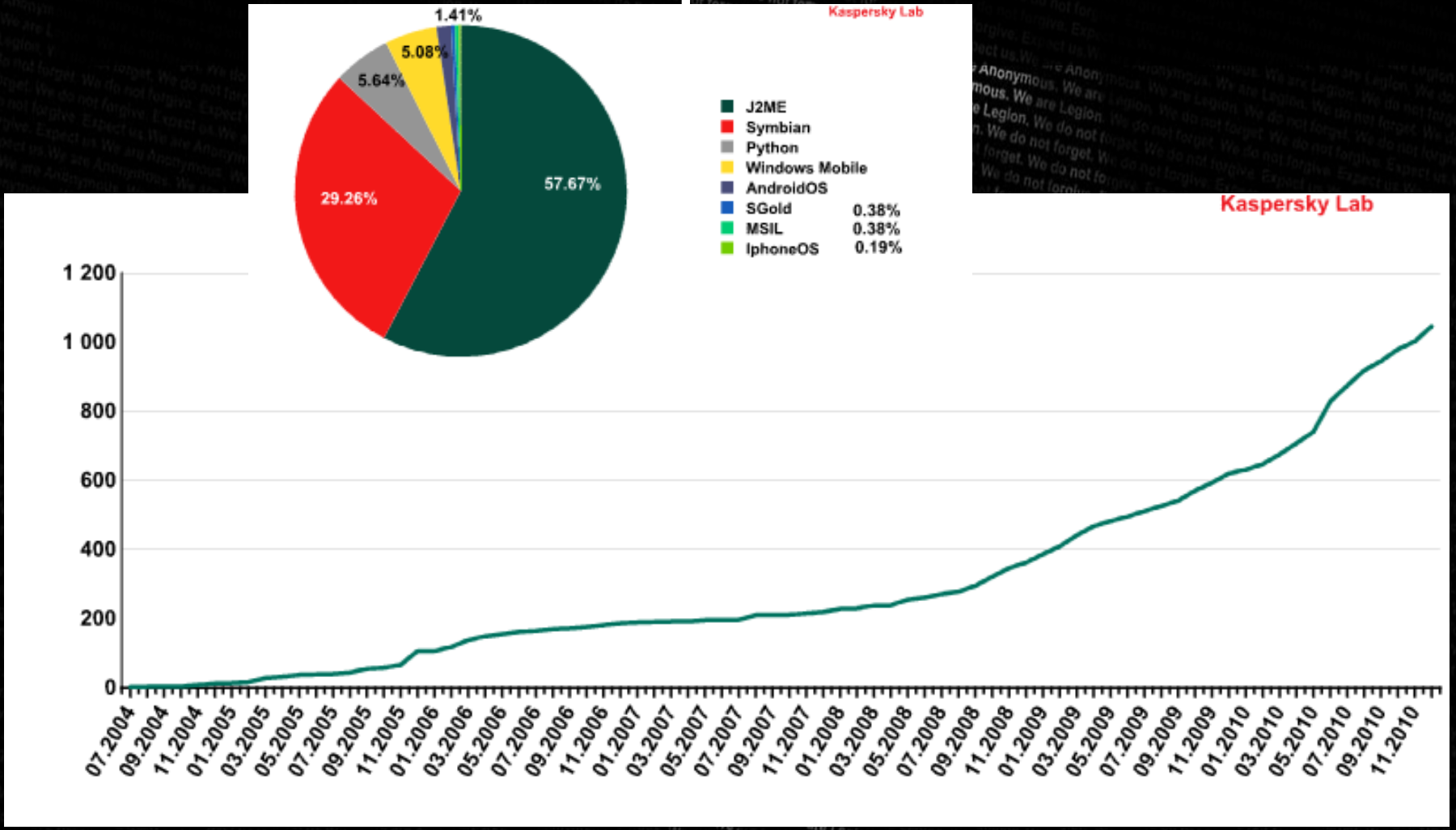
Entwicklung

- Vom Handy zum Smartphone
- Vom Telefonnetz zum Multimedianetz
- Vom Leben „offline“ zu „online“

Agenda

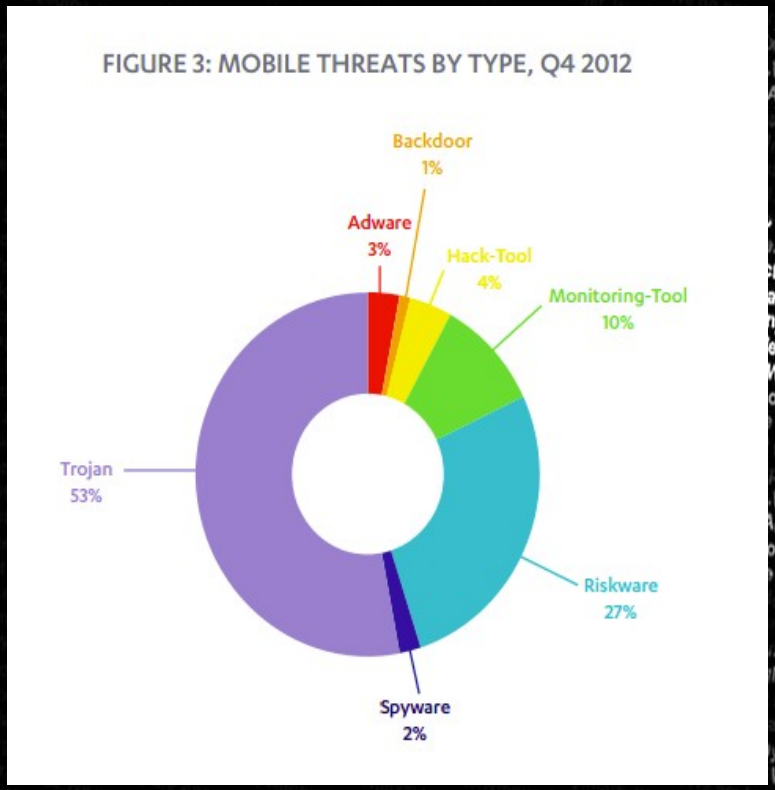
Gefährdungslage

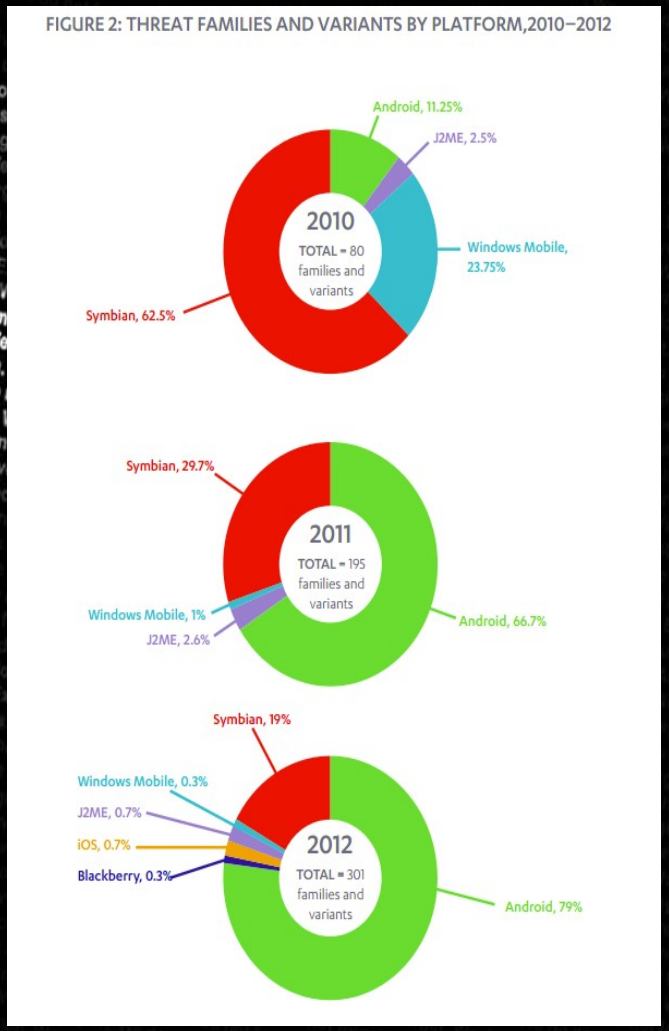
Mal ein paar Zahlen



http://www.securelist.com/en/analysis/204792168/Mobile_Malware_Evolution_An_Overview_Part_4#14

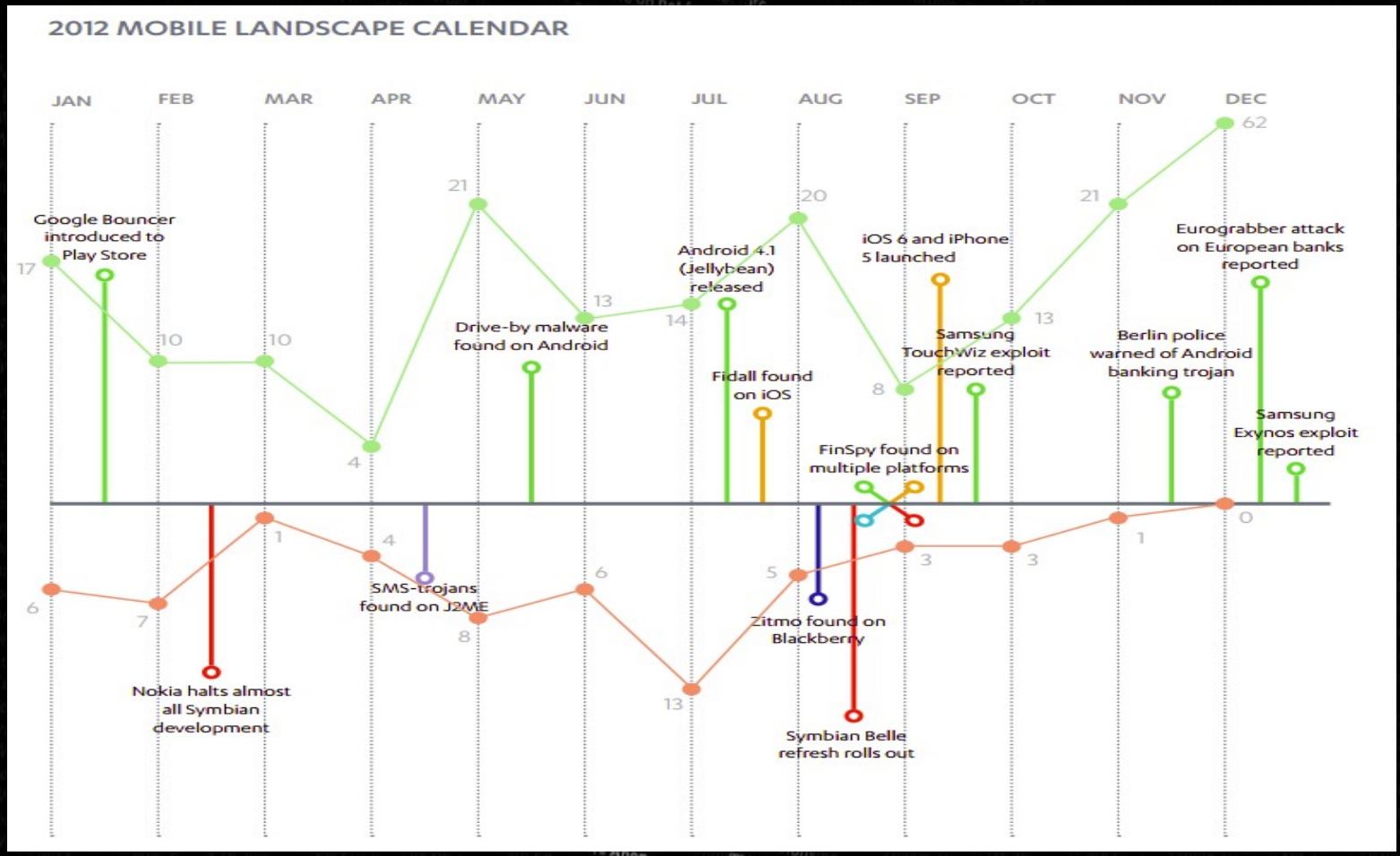
Mal ein paar Zahlen





http://www.heise.de/newsticker/meldung/Android-ist-das-Top-Ziel-fuer-mobile-Malware-1818986.html

Mal ein paar Zahlen



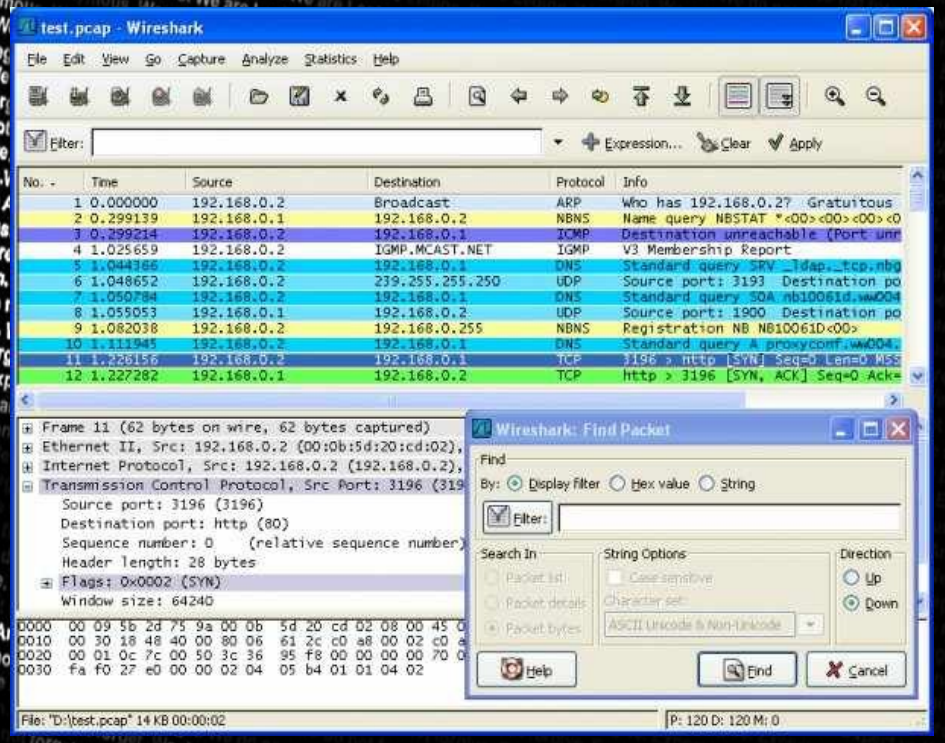
http://www.heise.de/newsticker/meldung/Android-ist-das-Top-Ziel-fuer-mobile-Malware-1818986.html

Gefährdungslage

- Verschlüsselung?
- Privatsphäre?
- Datensicherheit?
- Authentisierung?

GSM bietet nur „authentisierte Teilnehmer“

Abschaltbare Verschlüsselung



Gefährdungslage

- „Locationgate“
  Apple Iphone / Android
- Malware
- App-Berechtigungen
- Anwendungen von Drittanbietern
- Trojaner
  Zeus
- Firmware Bugs und Custom ROMs
- (Un-)Locked Bootloader
- Abofallen
- Vorratsdatenspeicherung:
  „Polizei erfasst Tausende Handydaten“
- GSM Sicherheit ist unzureichend

Gefährdungslage

- Diebstahl
  Stern Online

News am 10.03.2013 Startseite Schlagzeilen Themen Newsletter Mobil iPad Blogs Investigativ Hefte Login

Suche

stern.de Zur Homepage

sternTV Home | sternTV Archiv | sternTV Reportage Archiv | Über sternTV | produziert von i&u

RTL sternTV | Sendung vom 06.03.2013

Handy-Aufspürprogramm

7. März 2013, 10:13 Uhr

Smartphone-App überführt Langfinger

Die Zahl der gestohlenen Smartphones nimmt rasant zu. Die meisten davon bleiben verschwunden. *stern* TV hat den Test gemacht und sich beklauen lassen. Eine neue App half, den Dieb zu überführen.

Twittern 15 | Gefällt mir 465 | Senden | +1 21 | Drucken | Versenden

Der Spion auf dem Handy
Neuartige App spürt Smartphone auf

Karneval in Köln. In einer Diskothek liegt ein herrenloses Samsung Galaxy SIII auf der Theke. Es dauert nur Sekunden, bis es in der Tasche einer Feierlustigen verschwindet. So geschehen mit einem Test-Smartphone von *stern* TV. Und es passiert inzwischen täglich tausendfach. 3,5 Millionen Deutschen sind schon das Handy geklaut worden. Die wenigsten kommen zu ihren Eigentümern zurück. Besonders beliebt unter Langfingern: neuwertige, internetfähige Smartphones für mehrere Hundert Euro. Mal macht die Gelegenheit Diebe, mal sind es gezielte Streifzüge von Dieben durch Cafés, Clubs und Bars.

Zur Sendungs-Übersicht

MEHR ZUM ARTIKEL

Fahndung nach dem Handy-Dieb
So verwenden Sie die App

Überwachungssoftware spioniert Dieben nach
Laptop-Klau lohnt nicht

Tausende Notebooks werden pro Jahr in Deutschland gestohlen - und tauchen nicht wieder auf. Doch wer stiehlt Laptops? Und was passiert mit dem Diebesgut? *stern* TV macht den Test.

Gefährdungslage

- Firmware Bugs
  Heise Online

heise online > News > 2013 > KW 10 > Sperrbildschirm des Samsung Galaxy S3 lässt sich umgehen

07.03.2013 13:12

heise Security « Vorige | Nächste »

Sperrbildschirm des Samsung Galaxy S3 lässt sich umgehen UPDATE

vorlesen / MP3-Download

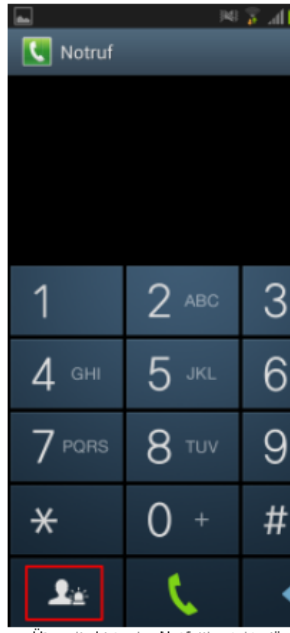
Der Sperrbildschirm des Galaxy S3 von Samsung schützt das Smartphone nicht vor ungewollten Zugriffen. Auch ohne Passwort oder PIN lässt sich das Gerät von einem Angreifer dauerhaft freischalten. Der Angriff basiert auf der seit kurzem bekannten Lücke beim Samsung Note 2, die jedoch nur einen kurz Einblick auf den Startbildschirm gewährt.

Wir konnten den deutlich gravierenderen Fehler auf einem aktuellen Galaxy S3 mit Android 4.1.2 problemlos nachvollziehen. Damit der Angriff funktioniert müssen einige Voraussetzungen erfüllt sein. So darf die Liste mit Notfallkontakten nicht leer sein und das Gerät muss im passenden Mobilfunknetz eingebucht sein. Ansonsten gibt das Gerät nur eine kurze Fehlermeldung aus. Auch ohne eingelegte und freigeschaltete SIM-Karte klappt es nicht. Sind die Voraussetzungen erfüllt, lässt sich wie schon beim iPhone mit dem richtigen Timing der Zugriffsschutz über die frei zugängliche Notruffunktion aushebeln.

Dort wählt man links unten die Liste mit den eigenen Notfallkontakten an. Wird diese mit dem Home-Button geschlossen und direkt danach der Einschaltknopf gedrückt, ist das Gerät beim nächsten Einschalten des Bildschirms unter Umständen nicht mehr gesperrt. Das klappte zwar nicht bei jedem Versuch, ließ sich aber mit dem richtigen Timing zuverlässig nachstellen. Den größten Erfolg hatten wir in unseren Versuchen, wenn der Bildschirm per PIN gesperrt war.

Danach hat man nicht nur vollständigen Zugriff aufs Gerät, es bleibt auch bis zum Neustart weiterhin völlig ungeschützt. Will man das Passwort ändern, wird man weiterhin danach gefragt. Ganz ohne weiteres lässt sich der rechtmäßige Besitzer also zumindest nicht aussperren. Unter Umständen lässt sich aber das Passwort auch über die Vorschläge der Tastatur herausfinden.

Update 7.3. um 13:33: Tatsächlich darf die Notfallliste auch leer sein. Solange sie sich aufrufen lässt, funktioniert der Angriff. In unseren Versuchen passierte dies zunächst nicht, warum ist noch unklar. (asp)

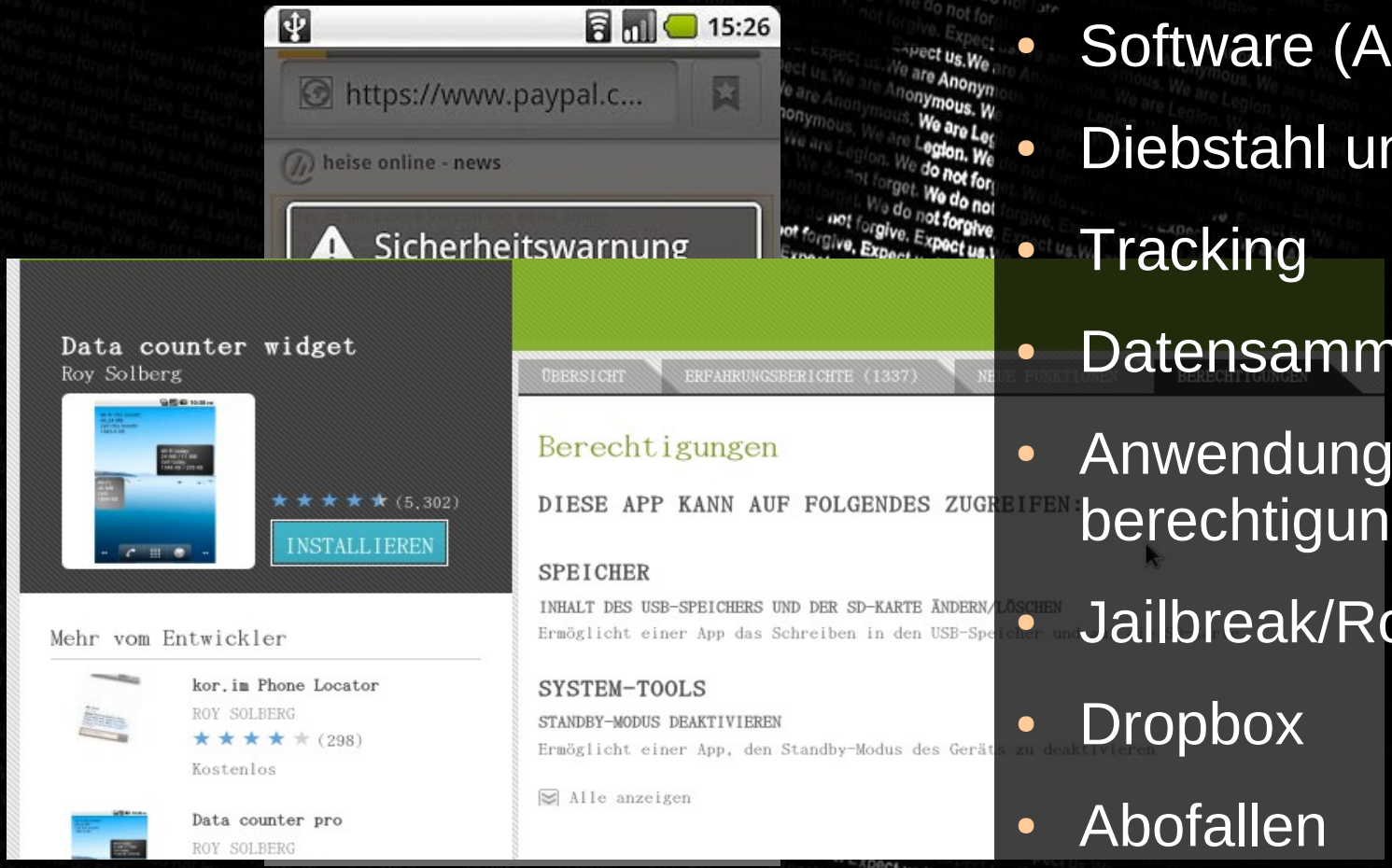


Über die Liste der Notfallkontakte lässt sich der Sperrbildschirm beim S3 mühelos umgehen.

Gefährdungslage

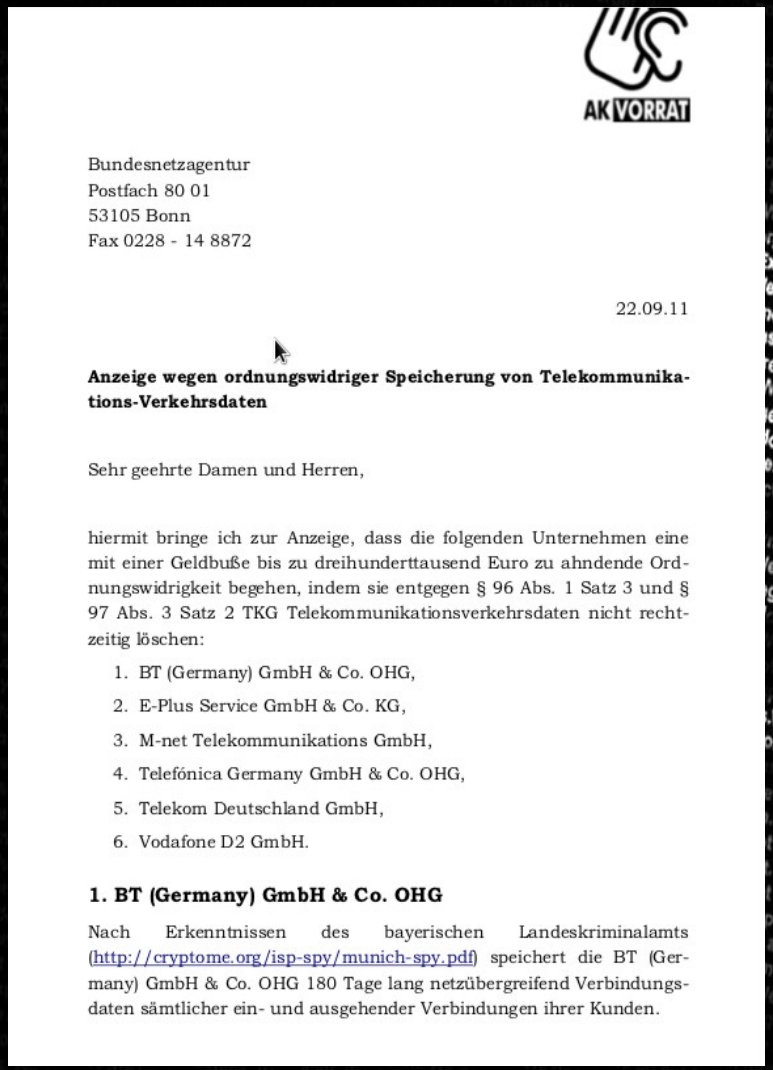
- Ziele:
  - mTAN/Banking
  - Kostenlos Surfen und Telefonieren
  - Ihre Daten
  - Nutzerverhalten
  - Standort
- Ein lukrativer Markt:
  - Botnetze
  - Profiling
  - Tracking
  - Werbung

Achtung – Wichtig!



- Software (Apps)
- Diebstahl und Verlust
- Tracking
- Datensammelwut
- Anwendungs-berechtigungen
- Jailbreak/Rooting
- Dropbox
- Abofallen
  - MobileSpy
  - jamba

Ihre (Verkehrs-)Daten



AK VORRAT

Bundesnetzagentur
Postfach 80 01
53105 Bonn
Fax 0228 - 14 8872

22.09.11

Anzeige wegen ordnungswidriger Speicherung von Telekommunikations-Verkehrsdaten

Sehr geehrte Damen und Herren,

hiermit bringe ich zur Anzeige, dass die folgenden Unternehmen eine mit einer Geldbuße bis zu dreihunderttausend Euro zu ahndende Ordnungswidrigkeit begehen, indem sie entgegen § 96 Abs. 1 Satz 3 und § 97 Abs. 3 Satz 2 TKG Telekommunikationsverkehrsdaten nicht rechtzeitig löschen:

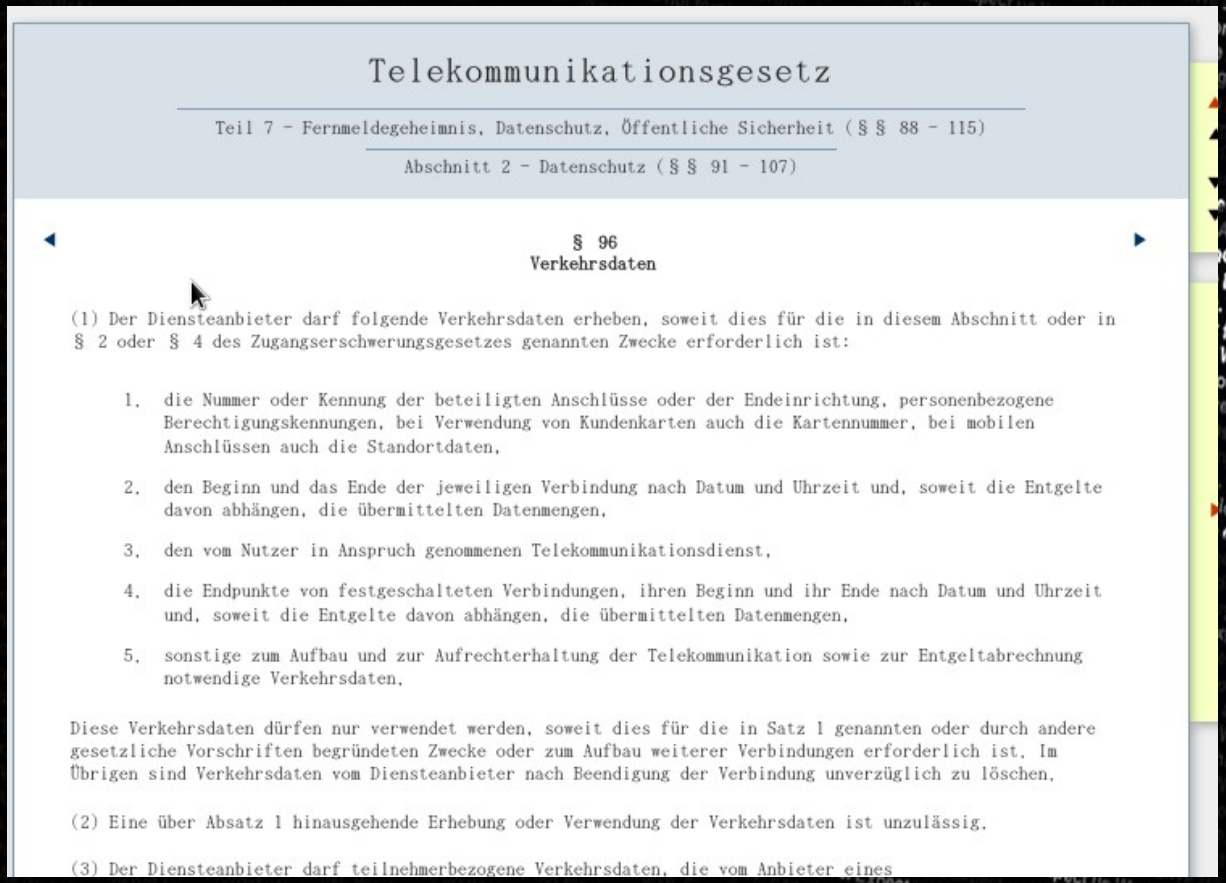
1. BT (Germany) GmbH & Co. OHG,
2. E-Plus Service GmbH & Co. KG,
3. M-net Telekommunikations GmbH,
4. Telefónica Germany GmbH & Co. OHG,
5. Telekom Deutschland GmbH,
6. Vodafone D2 GmbH.

1. BT (Germany) GmbH & Co. OHG

Nach Erkenntnissen des bayerischen Landeskriminalamts (http://cryptome.org/isp-spy/munich-spy.pdf) speichert die BT (Germany) GmbH & Co. OHG 180 Tage lang netzübergreifend Verbindungsdaten sämtlicher ein- und ausgehender Verbindungen ihrer Kunden.

- Werden genutzt für Werbung
- Werden genutzt für Statistiken und Auswertungen Ihres Verhalten
- Werden genutzt für Bewegungsprofile
- Werden 90 – 180 Tage lang gespeichert (obwohl dies rechtswidrig ist, TKG)
- Werden „mitgelesen“
- Stehen Staatsanwaltschaft und Urheberrechteinhabern zur Verfügung
- Sind in der Regel unverschlüsselt und Dritten zugänglich

Verkehrsdaten



Telekommunikationsgesetz

Teil 7 - Fernmeldegeheimnis, Datenschutz, Öffentliche Sicherheit (§§ 88 - 115)

Abschnitt 2 - Datenschutz (§§ 91 - 107)

§ 96
Verkehrsdaten

(1) Der Diensteanbieter darf folgende Verkehrsdaten erheben, soweit dies für die in diesem Abschnitt oder in § 2 oder § 4 des Zugangserschwerungsgesetzes genannten Zwecke erforderlich ist:

1. die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen auch die Standortdaten,
2. den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,
3. den vom Nutzer in Anspruch genommenen Telekommunikationsdienst,
4. die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,
5. sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten.

Diese Verkehrsdaten dürfen nur verwendet werden, soweit dies für die in Satz 1 genannten oder durch andere gesetzliche Vorschriften begründeten Zwecke oder zum Aufbau weiterer Verbindungen erforderlich ist. Im Übrigen sind Verkehrsdaten vom Diensteanbieter nach Beendigung der Verbindung unverzüglich zu löschen.

(2) Eine über Absatz 1 hinausgehende Erhebung oder Verwendung der Verkehrsdaten ist unzulässig.

(3) Der Diensteanbieter darf teilnehmerbezogene Verkehrsdaten, die vom Anbieter eines

- Rechtsgrundlage

  TKG, TDDSG, TDSV, BDSG

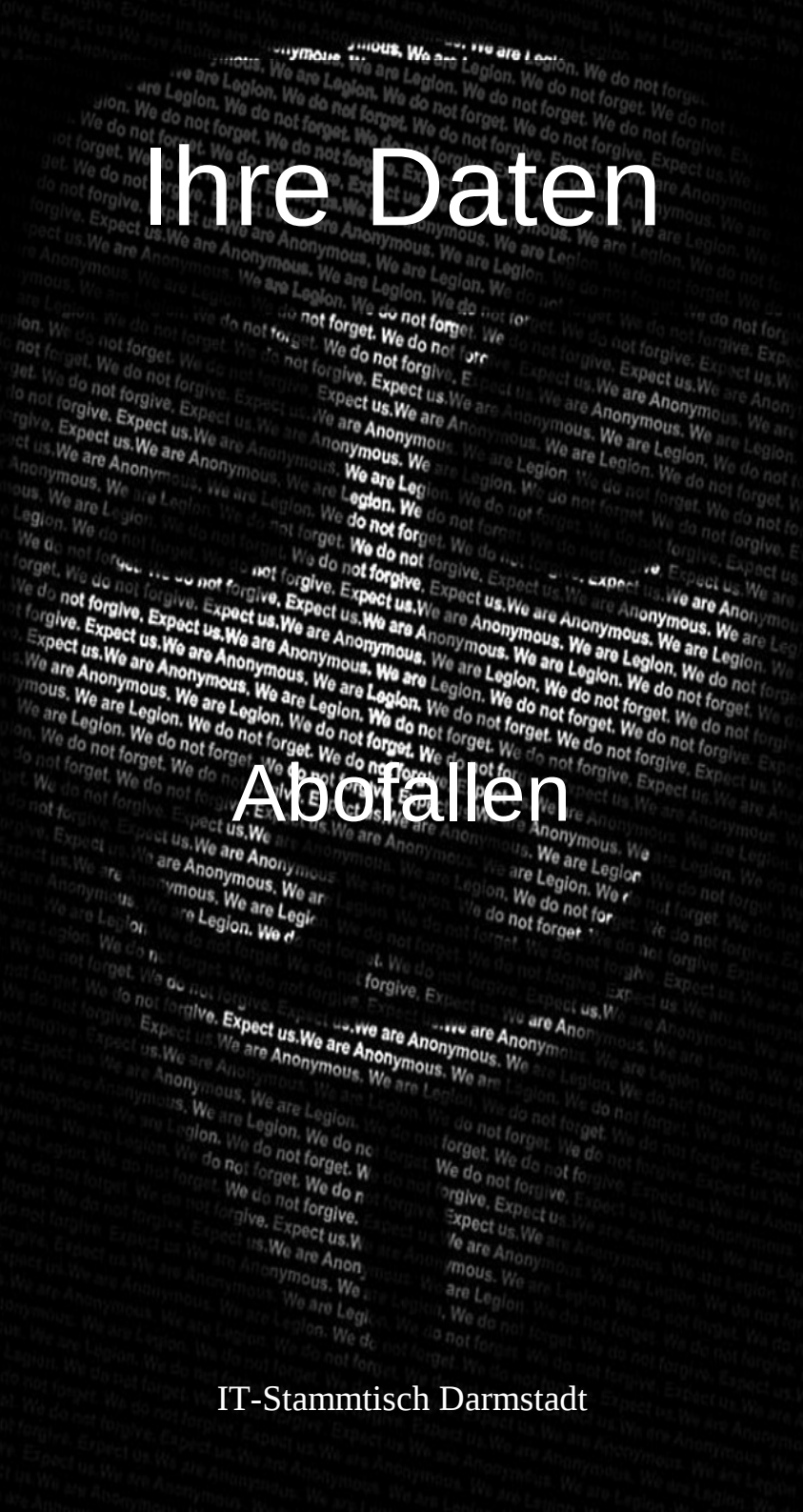
- TKG

  § 96 und 97 regelt die Speicherung der sog. „Verkehrsdaten“ zu Abrechnungszwecken

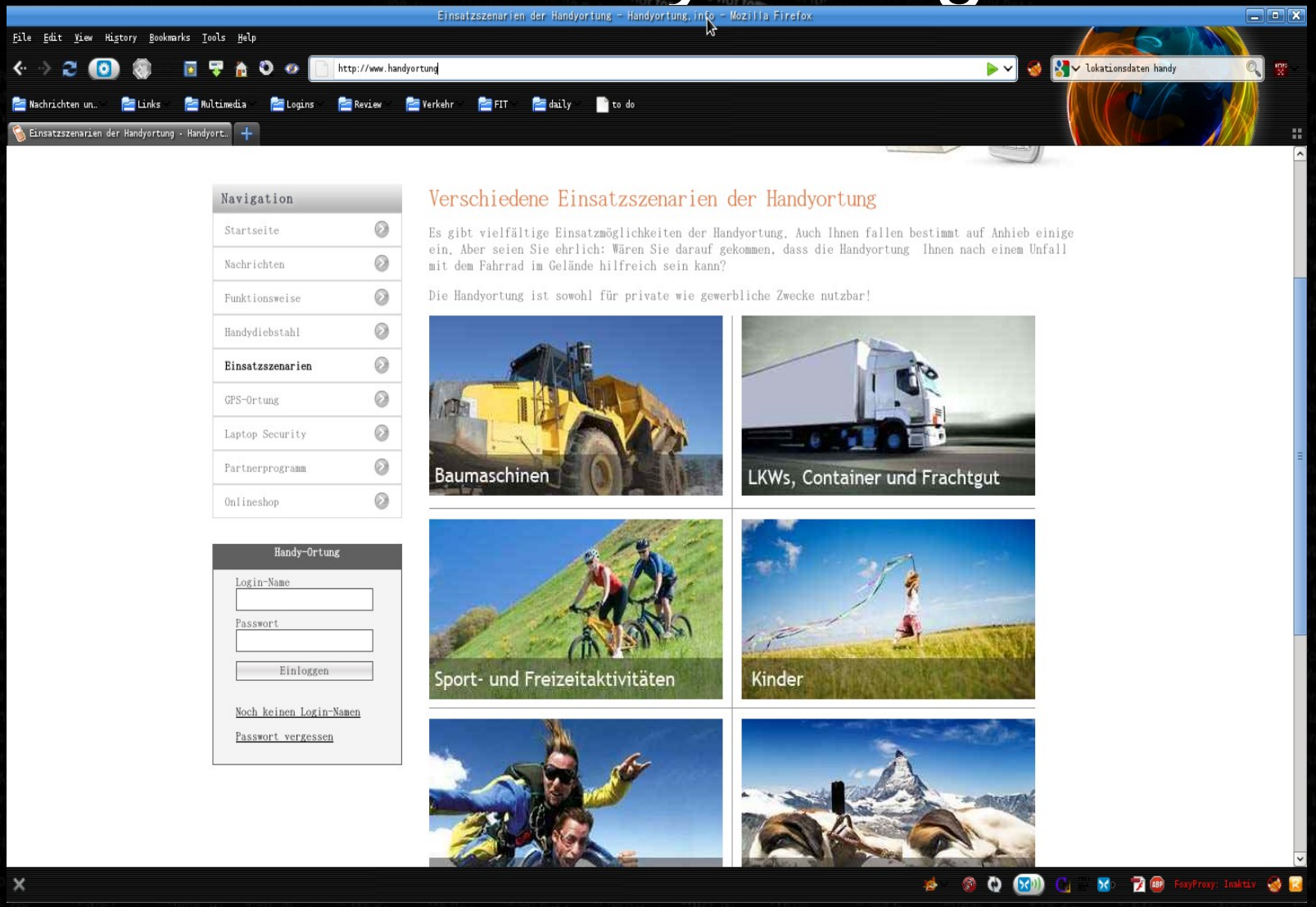
- Verstoss = Ordnungswidrigkeit
- Max. € 50.000,-

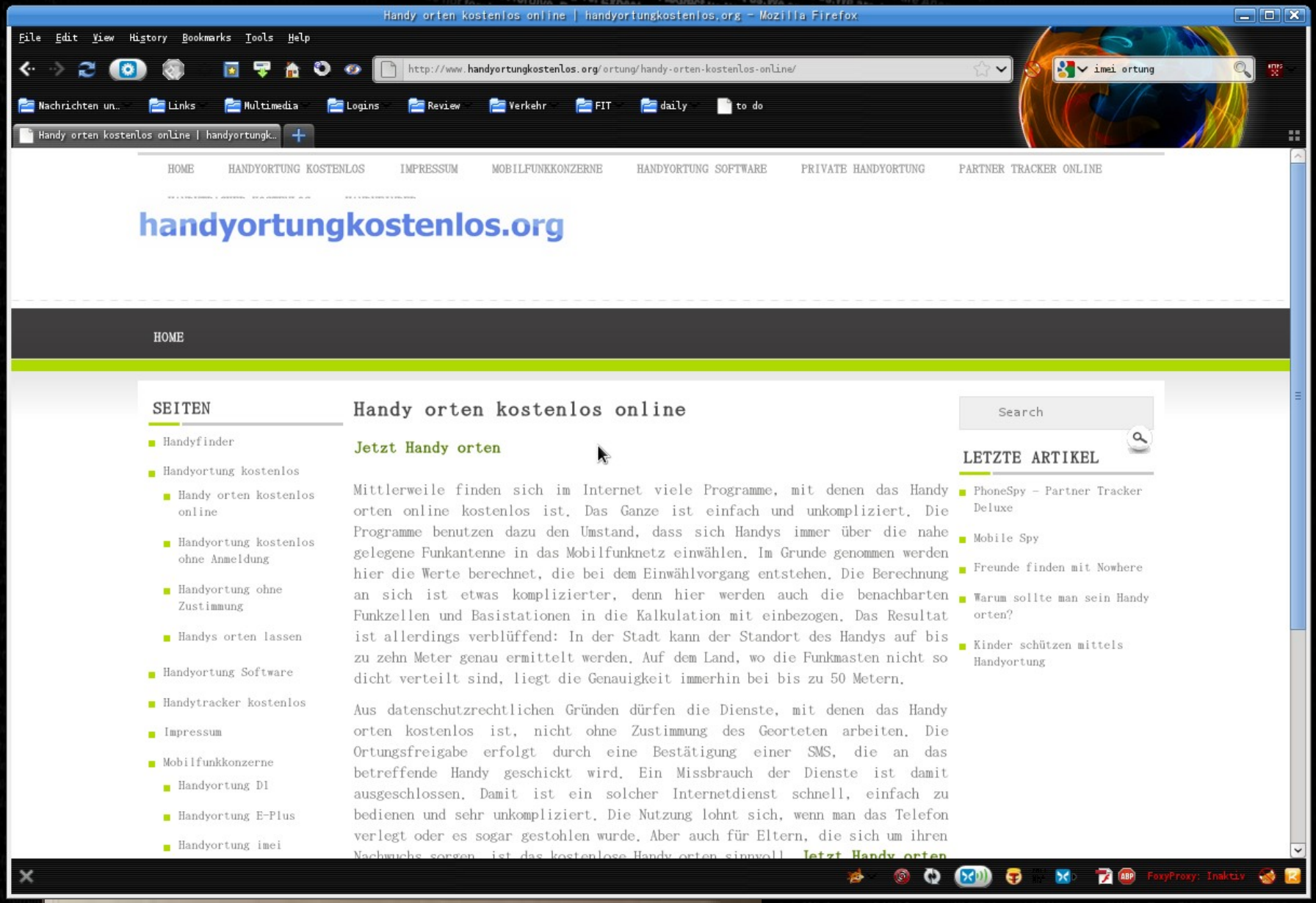
http://www.itrechtler.de

Ihre Daten



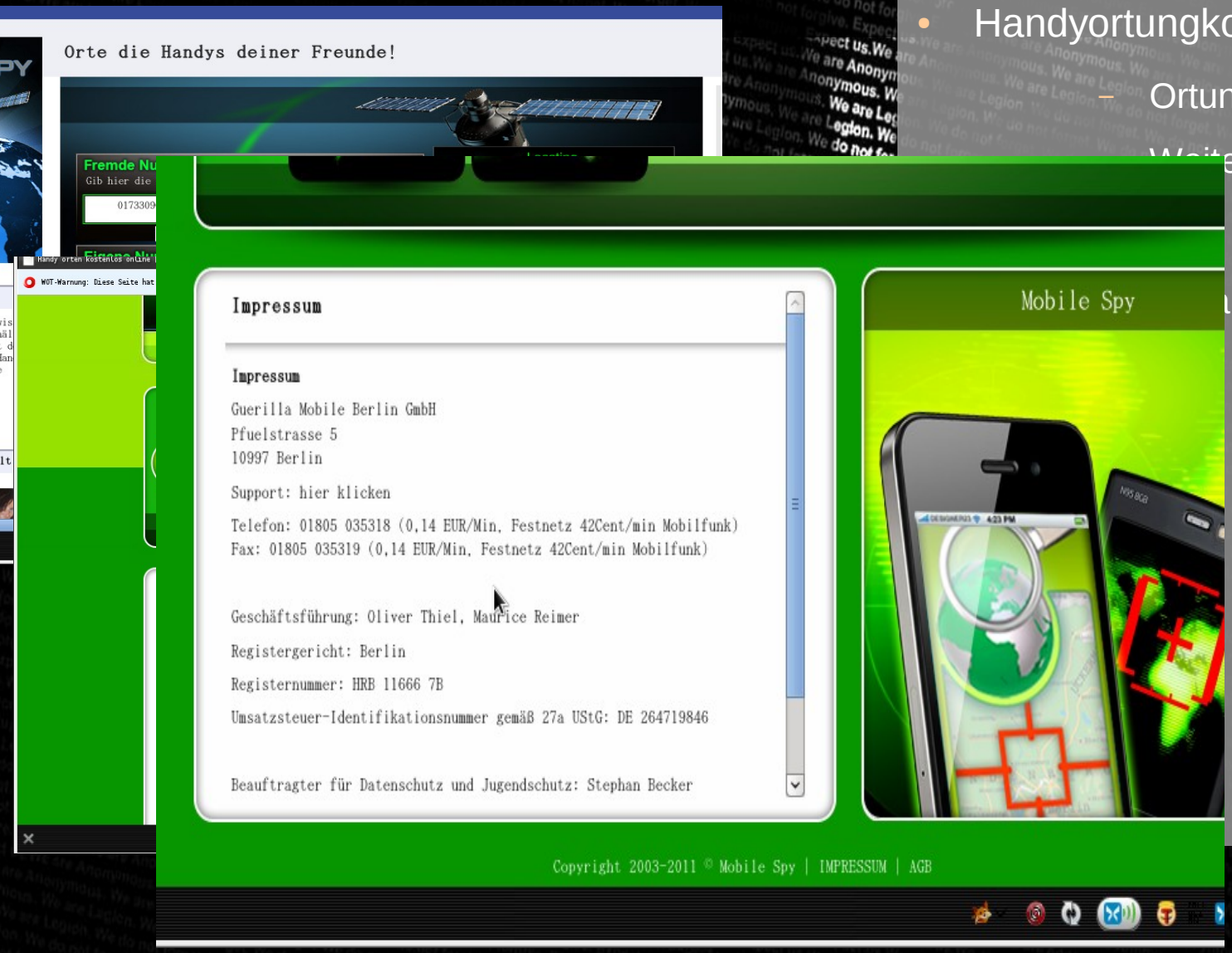
Handyortung




Handy orten kostenlos online | handyortungkostenlos.org - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.handyortungkostenlos.org/ortung/handy-orten-kostenlos-online/
imei ortung
Nachrichten un... Links Multimedia Logins Review Verkehr FIT daily to do
Handy orten kostenlos online | handyortungk...
HOME HANDYORTUNG KOSTENLOS IMPRESSUM MOBILFUNKKONZERNE HANDYORTUNG SOFTWARE PRIVATE HANDYORTUNG PARTNER TRACKER ONLINE
handyortungkostenlos.org
HOME
SEITEN
Handyfinder
Handyortung kostenlos
Handy orten kostenlos online
Handyortung kostenlos ohne Anmeldung
Handyortung ohne Zustimmung
Handys orten lassen
Handyortung Software
Handytracker kostenlos
Impressum
Mobilfunkkonzerne
Handyortung D1
Handyortung E-Plus
Handyortung imei
Handy orten kostenlos online
Jetzt Handy orten
Mittlerweile finden sich im Internet viele Programme, mit denen das Handy orten online kostenlos ist. Das Ganze ist einfach und unkompliziert. Die Programme benutzen dazu den Umstand, dass sich Handys immer über die nahe gelegene Funkantenne in das Mobilfunknetz einwählen. Im Grunde genommen werden hier die Werte berechnet, die bei dem Einwählvorgang entstehen. Die Berechnung an sich ist etwas komplizierter, denn hier werden auch die benachbarten Funkzellen und Basistationen in die Kalkulation mit einbezogen. Das Resultat ist allerdings verblüffend: In der Stadt kann der Standort des Handys auf bis zu zehn Meter genau ermittelt werden. Auf dem Land, wo die Funkmasten nicht so dicht verteilt sind, liegt die Genauigkeit immerhin bei bis zu 50 Metern.
Aus datenschutzrechtlichen Gründen dürfen die Dienste, mit denen das Handy orten kostenlos ist, nicht ohne Zustimmung des Georteten arbeiten. Die Ortungsfreigabe erfolgt durch eine Bestätigung einer SMS, die an das betreffende Handy geschickt wird. Ein Missbrauch der Dienste ist damit ausgeschlossen. Damit ist ein solcher Internetdienst schnell, einfach zu bedienen und sehr unkompliziert. Die Nutzung lohnt sich, wenn man das Telefon verlegt oder es sogar gestohlen wurde. Aber auch für Eltern, die sich um ihren Nachwuchs sorgen, ist das kostenlose Handy orten sinnvoll. Jetzt Handy orten
Search
LETZTE ARTIKEL
PhoneSpy – Partner Tracker Deluxe
Mobile Spy
Freunde finden mit Nowhere
Warum sollte man sein Handy orten?
Kinder schützen mittels Handyortung
FoxyProxy: Inaktiv

Handyortung

- Handyortungkostenlos.org
  - Ortung gibts **keine**!
  - Weiterleitung auf:
  - annte Abofalle!

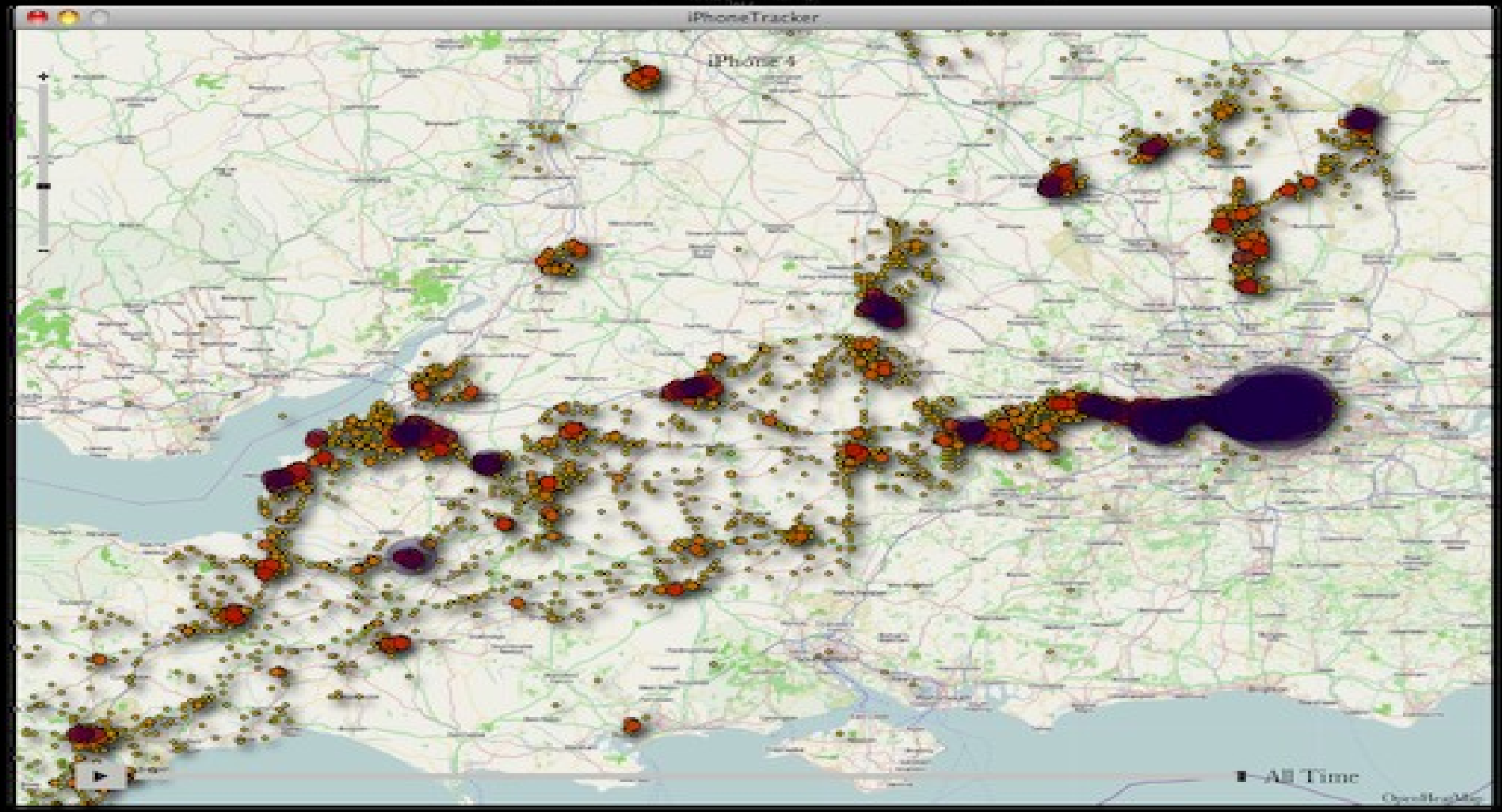


Handyortung

- Handyortungkostenlos.org
  - Ortung gibts keine!
  - Abofalle!
- Mobilesoy.de
  - Bekannte Abofalle!

So schnell geht das!

Handyortung



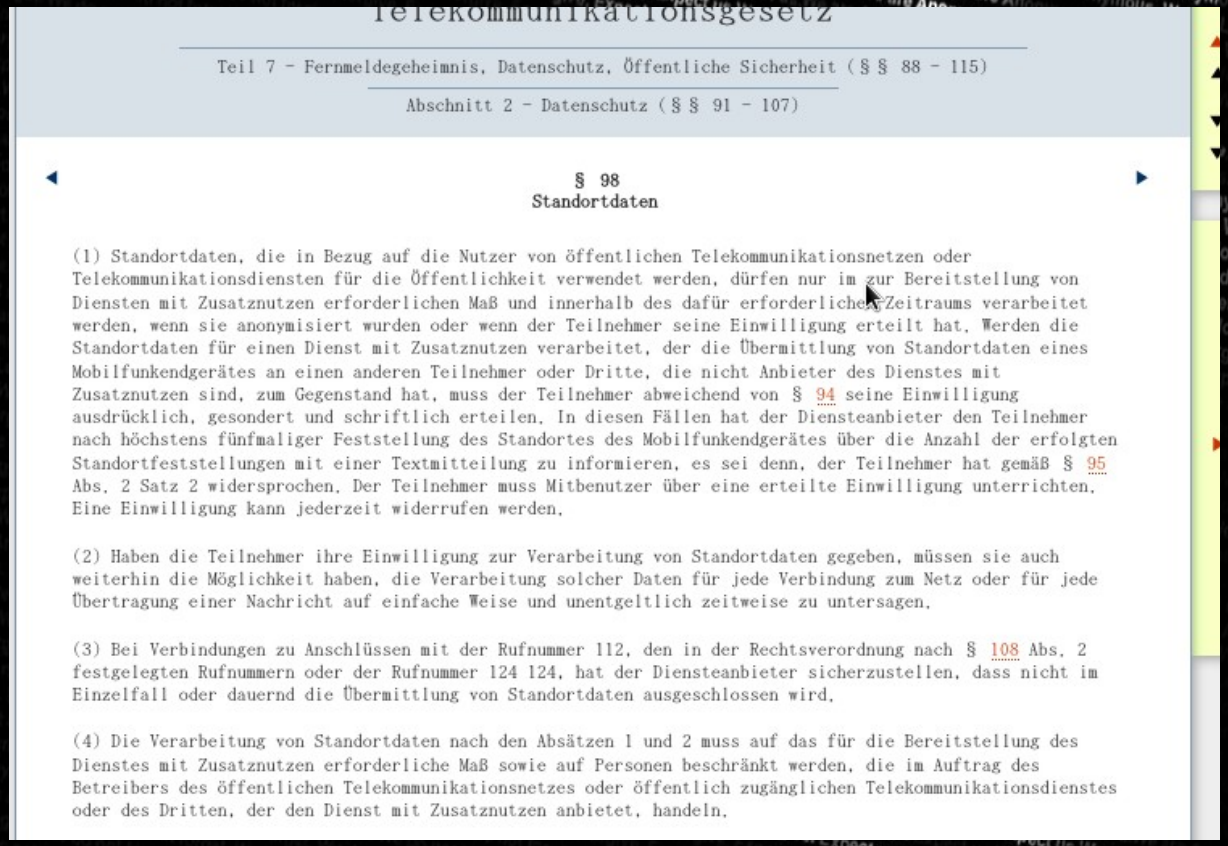
Handyortung

- Ortung

  auch mit deaktivertem GPS und Mobilfunknetz:

  - CID
  - LAC
  - Ortung jederzeit möglich -> 3 GSM Funkzellen (Triangulation)
  - http://www.umtslink.at

Handyortung



Telekommunikationsgesetz

Teil 7 - Fernmeldegeheimnis, Datenschutz, Öffentliche Sicherheit (§§ 88 - 115)

Abschnitt 2 - Datenschutz (§§ 91 - 107)

§ 98
Standortdaten

(1) Standortdaten, die in Bezug auf die Nutzer von öffentlichen Telekommunikationsnetzen oder Telekommunikationsdiensten für die Öffentlichkeit verwendet werden, dürfen nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Teilnehmer seine Einwilligung erteilt hat. Werden die Standortdaten für einen Dienst mit Zusatznutzen verarbeitet, der die Übermittlung von Standortdaten eines Mobilfunkendgerätes an einen anderen Teilnehmer oder Dritte, die nicht Anbieter des Dienstes mit Zusatznutzen sind, zum Gegenstand hat, muss der Teilnehmer abweichend von § 94 seine Einwilligung ausdrücklich, gesondert und schriftlich erteilen. In diesen Fällen hat der Diensteanbieter den Teilnehmer nach höchstens fünfmaliger Feststellung des Standortes des Mobilfunkendgerätes über die Anzahl der erfolgten Standortfeststellungen mit einer Textmitteilung zu informieren, es sei denn, der Teilnehmer hat gemäß § 95 Abs. 2 Satz 2 widersprochen. Der Teilnehmer muss Mitbenutzer über eine erteilte Einwilligung unterrichten. Eine Einwilligung kann jederzeit widerrufen werden.

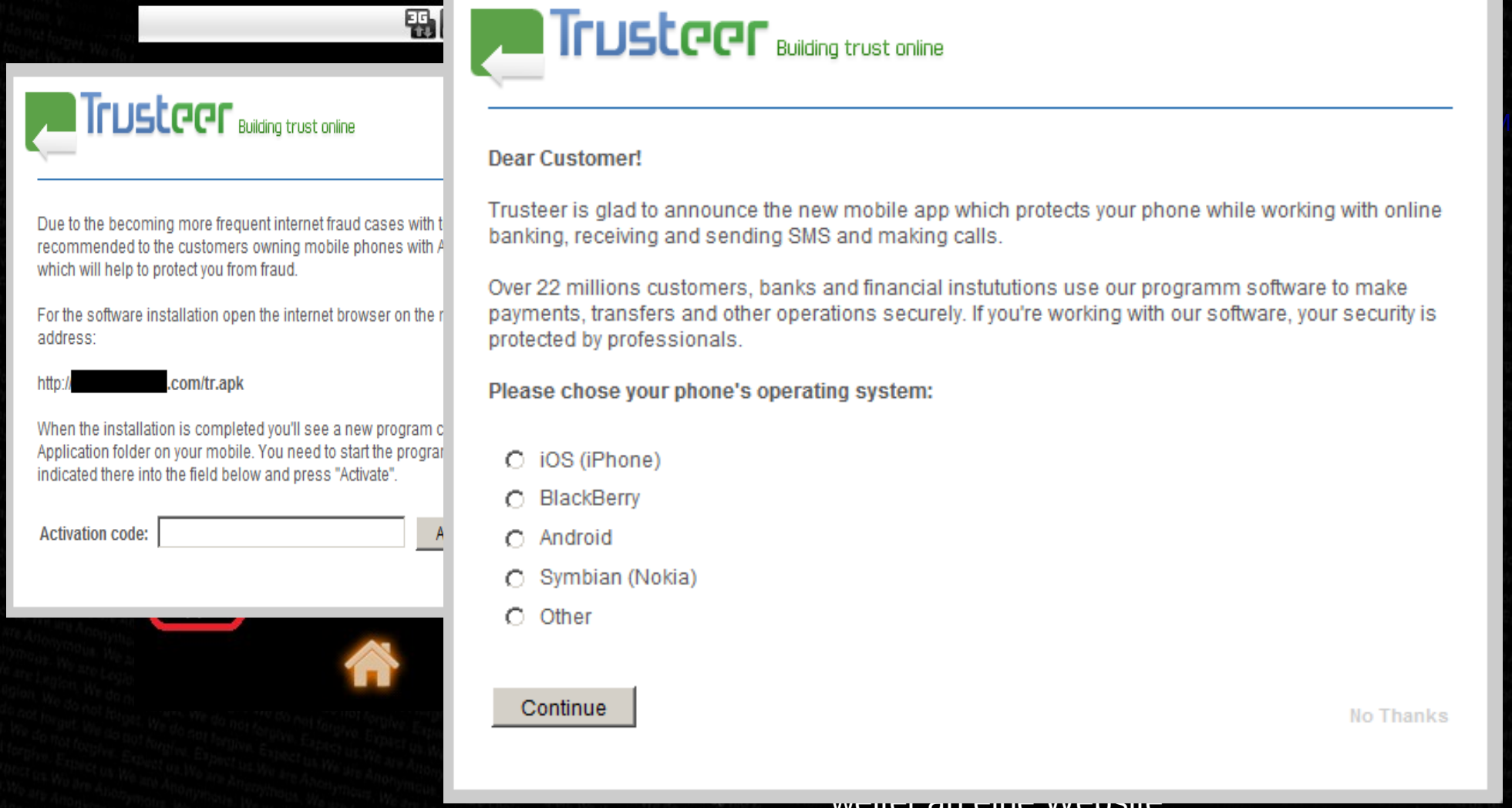
(2) Haben die Teilnehmer ihre Einwilligung zur Verarbeitung von Standortdaten gegeben, müssen sie auch weiterhin die Möglichkeit haben, die Verarbeitung solcher Daten für jede Verbindung zum Netz oder für jede Übertragung einer Nachricht auf einfache Weise und unentgeltlich zeitweise zu untersagen.

(3) Bei Verbindungen zu Anschlüssen mit der Rufnummer 112, den in der Rechtsverordnung nach § 108 Abs. 2 festgelegten Rufnummern oder der Rufnummer 124 124, hat der Diensteanbieter sicherzustellen, dass nicht im Einzelfall oder dauernd die Übermittlung von Standortdaten ausgeschlossen wird.

(4) Die Verarbeitung von Standortdaten nach den Absätzen 1 und 2 muss auf das für die Bereitstellung des Dienstes mit Zusatznutzen erforderliche Maß sowie auf Personen beschränkt werden, die im Auftrag des Betreibers des öffentlichen Telekommunikationsnetzes oder öffentlich zugänglichen Telekommunikationsdienstes oder des Dritten, der den Dienst mit Zusatznutzen anbietet, handeln.

- TKG
  - § 98 regelt die Speicherung von Standortdaten
  - Nur nach Einwilligung
  - Nur Anonymisiert
  - Zustimmungspflichtig im Einzelfall (> 5 Ortungen)
  - Widerspruchsmöglichkeit
  - Verpflichtung zur Ortung bei Notrufnummern

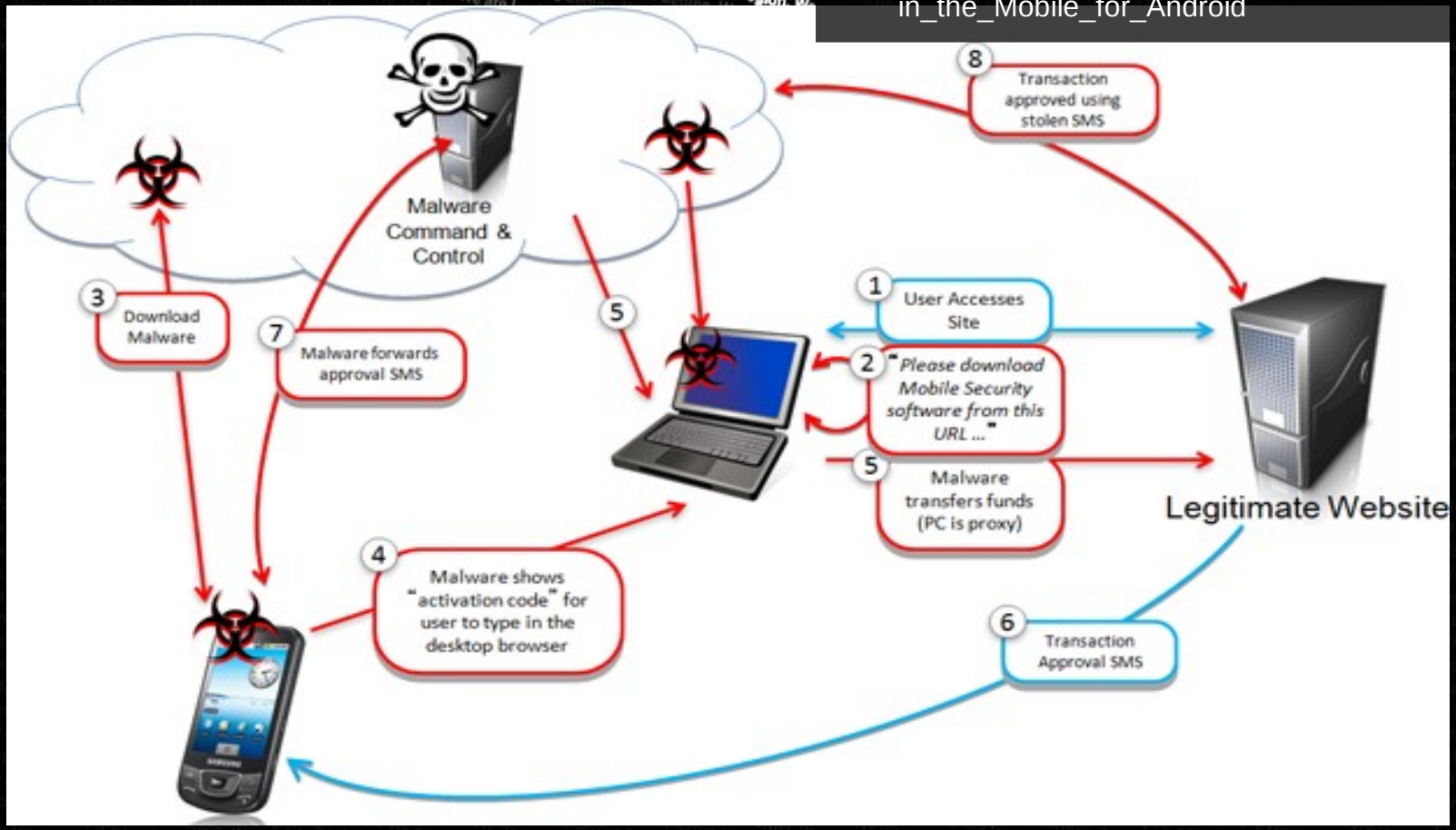
Malware


Trusteer
Building trust online
Due to the becoming more frequent internet fraud cases with t
recommended to the customers owning mobile phones with A
which will help to protect you from fraud.
For the software installation open the internet browser on the r
address:
http://[redacted].com/tr.apk
When the installation is completed you'll see a new program c
Application folder on your mobile. You need to start the progra
indicated there into the field below and press "Activate".
Activation code:
Trusteer
Building trust online
Dear Customer!
Trusteer is glad to announce the new mobile app which protects your phone while working with online banking, receiving and sending SMS and making calls.
Over 22 millions customers, banks and financial instututions use our programm software to make payments, transfers and other operations securely. If you're working with our software, your security is protected by professionals.
Please chose your phone's operating system:
iOS (iPhone)
BlackBerry
Android
Symbian (Nokia)
Other
Continue
No Thanks

Malware

- Beispiel:

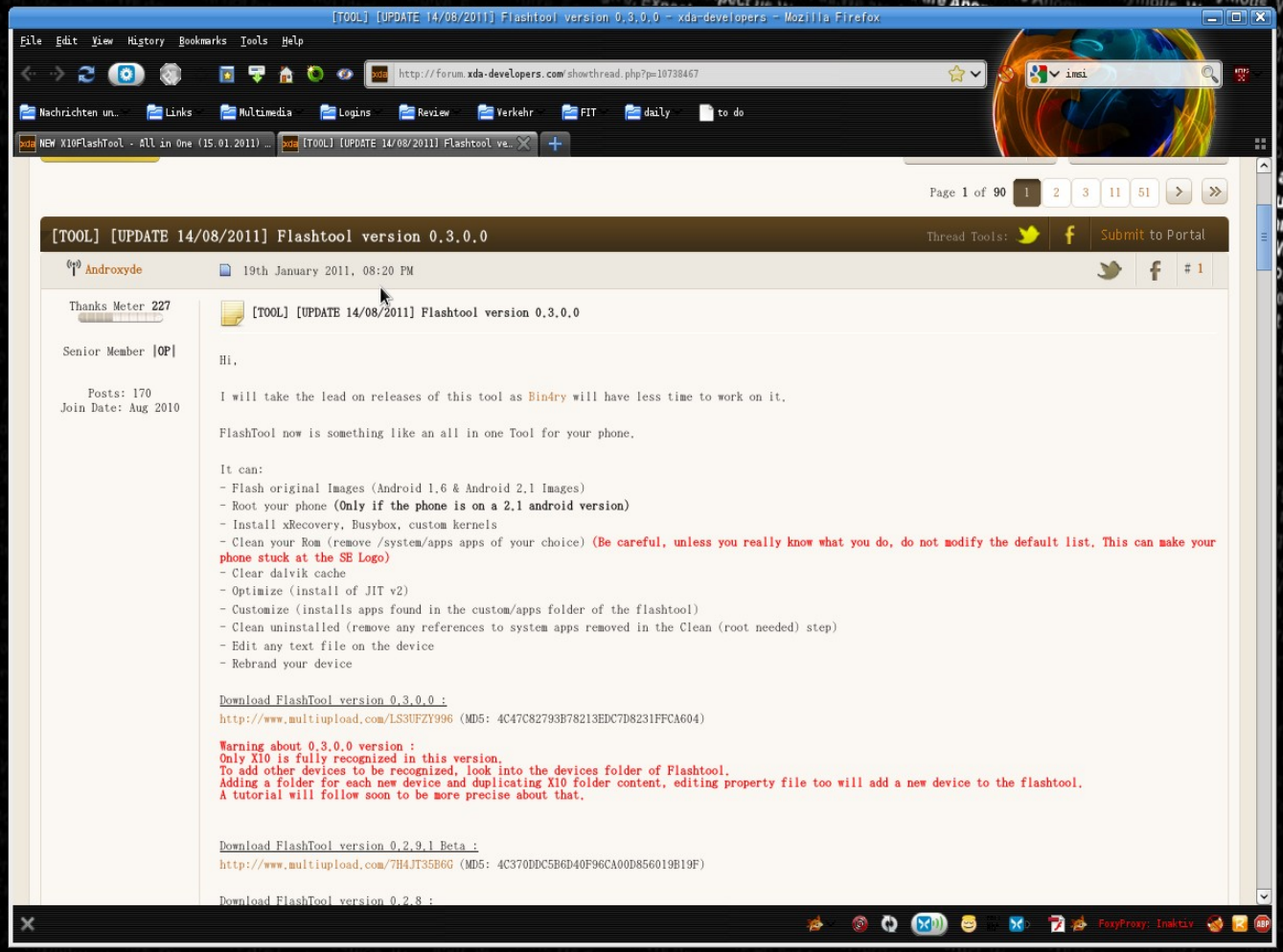
http://www.securelist.com/en/blog/208193029/ZeuS_in_the_Mobile_for_Android



„Ich bin root, ich darf das...!“

- Root Exploit
- Custom Firmware
- Tethering
- Unlock Bootloader
- Custom Software
  - Terminal
  - SSH
  - WebKey
  - APG
  - File Manager
- Configs

„Ich bin root, ich darf das...!“



- Root Exploit
- Custom Firmware
- Unlock Bootloader
- Custom Software
- Configs

xda-developers.com

Innenansichten

- Nutzungsstatistiken
  - Zeit
  - Startzähler
  - Anwendung

  10080 anonymous usage statistics
- Wifi
  - Status
  - Configs

Innenansichten

- GSM Netzmerkmale
  - IMSI
  - IMEI
  - LCID
  - SIM
  - LAC
  - Standort

Schlussfolgerung

- Vollständige Kontrolle nur durch Rooting/Jailbreaking
  - Garantieverlust
  - Eigenes Risiko
  - Kein Support

Have a break....!?


We are Legion. We do not forget. We do not forgive. Expect us.We are Anonymous.

Agenda

Anforderungen an die Handysicherheit

Antworten

- Distribution von
  - Firmware
  - Applikationen
- Berechtigungskonzept
  - „weniger ist mehr“
- Locked Bootloader
- User Rights Management
- DRM
- Digitale Signaturen
- Verschlüsselung
- Datenschutz

Antworten

Benutzer Akzeptanz ????

Marktanteile

Kosten

Umsatz

- Distribution von
  - Firmware
  - Applikationen
- Berechtigungskonzept
  - „weniger ist mehr“
- Locked Bootloader
- User Rights Management
- DRM
- Digitale Signaturen

Shareholder Value

- Verschlüsselung
- Datenschutz


Antworten
Tun Sie selbst etwas!
Behalten Sie die Kontrolle!

Agenda

Was können Sie tun?
Empfehlungen und Tools

Empfehlungen

- Ihr Prov
  - PIN
    dea

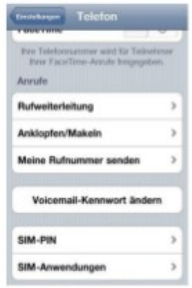
Anleitung zur Deaktivierung der PIN-Abfrage der Micro-SIM

Als provisorische Lösung der Probleme mit dem neuen iPhone 4S schlagen wir vor, die PIN-Abfrage der Micro-SIM vor dem Einsetzen in das neue iPhone 4S auszuschalten. Diese Lösung schafft in den meisten Fällen Abhilfe.

Benutzen Sie ein anderes Micro-SIM fähiges Gerät, z.B. ein iPhone 4, und führen Sie die folgenden Schritte aus:

1. Wählen Sie vom Startbildschirm „Einstellungen“ und dann „Telefon“

2. Wählen Sie im Menü „SIM-PIN“



3. Stellen Sie den Schieberegler auf aus (0)

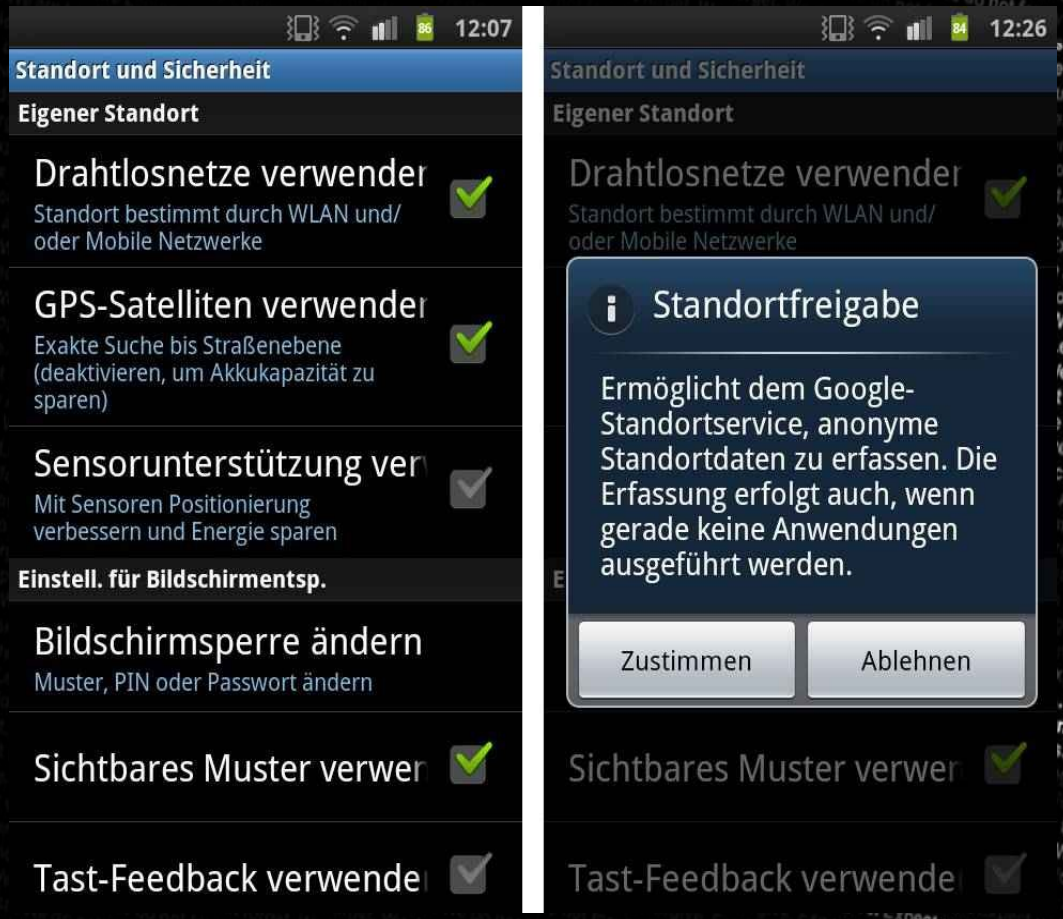
Empfehlungen

- Einstellungen ändern:
  - PIN Abfrage einschalten
  - Passwörter unsichtbar
  - Display-Sperre einschalten
  - SIM Sperre einschalten
  - Anmeldeinformations-speicher mit Passwort schützen
  - Standortdaten und GPS deaktivieren
  - Bluetooth und WLAN deaktivieren

Empfehlungen

- Einstellungen ändern:
  - Drahtlos & Netzwerke

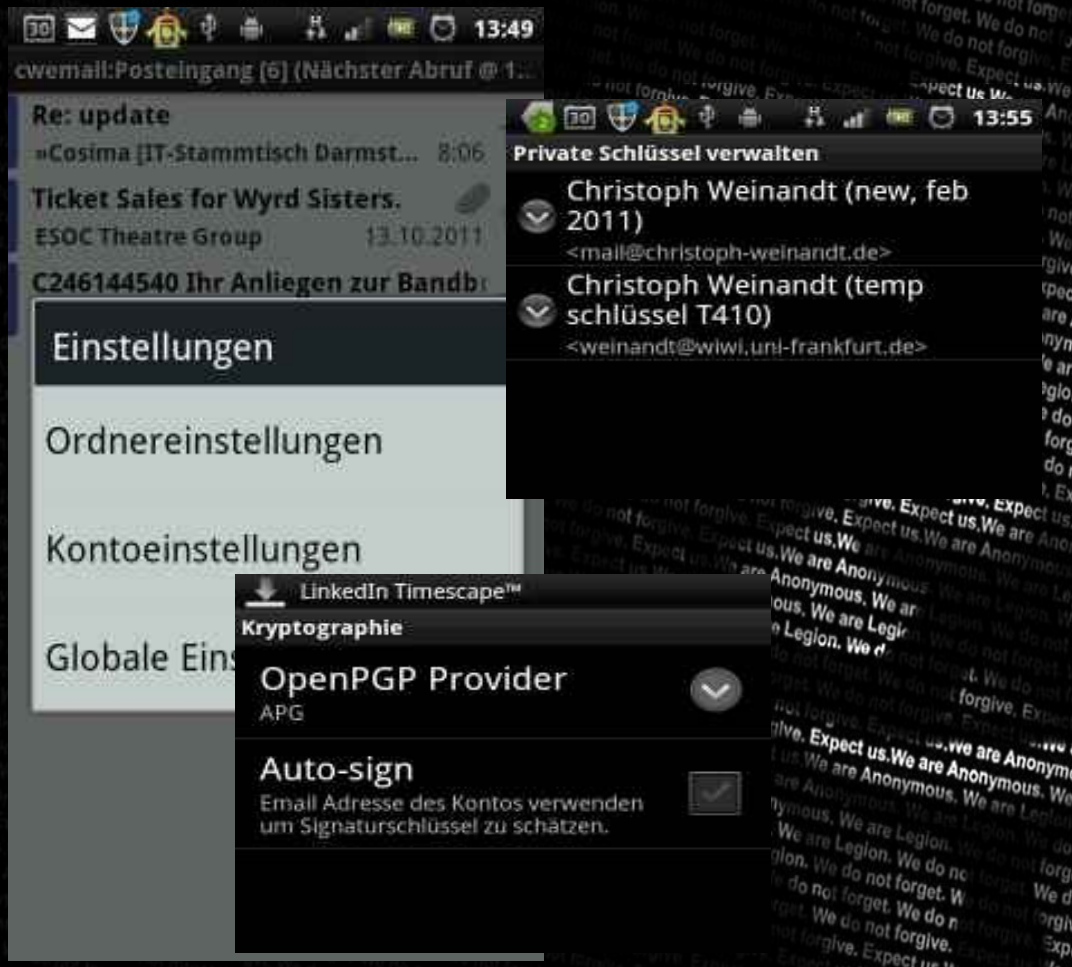
Einstellungen



- Dienste abschalten
  - GPS
  - Bluetooth
  - Data
  - Funkzellenortung
  - UMTS/GPRS

  und nur einschalten, wenn man sie nutzt!
- Vorteil
  - Schont den Akku
  - Erhöht die Sicherheit

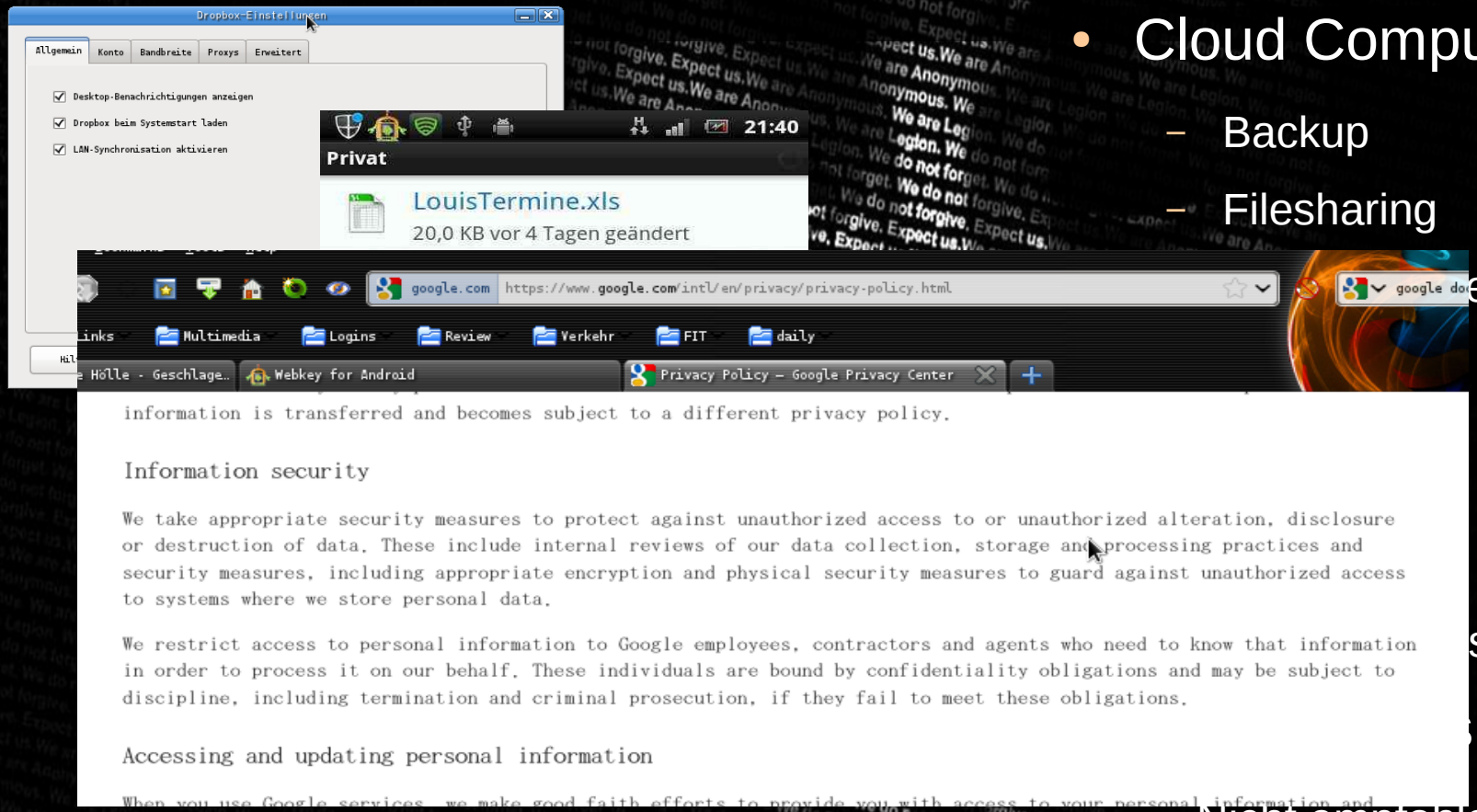
Einstellungen



- Email
  - TLS
  - SSL
  - IMAP
  - PGP

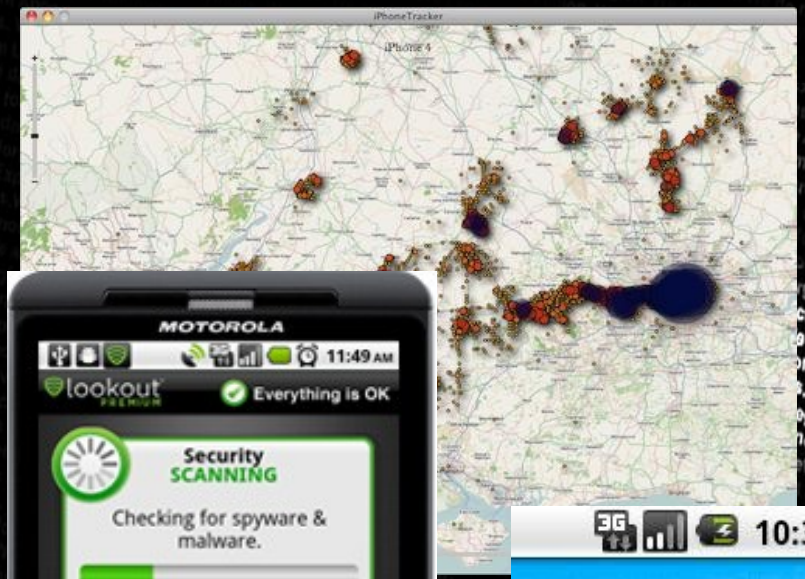
  Aktivieren!
- Vorteil
  - Verschlüsselung der Emails
- Tool
  - APG, K9 Mail

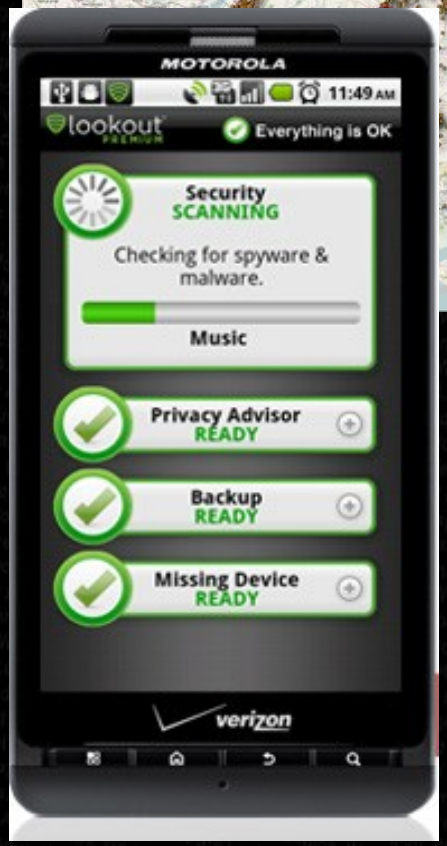
Einstellungen



- Cloud Computing
  - Backup
  - Filesharing
  - eiablage
  - sselt nutzen
  - Nicht empfohlen:
    - Nutzungsbedingungen
    - Keine Verschlüsselungsmöglichkeit

Tools





- Berechtigungs management
  - LBE
- SSH
- VPN
- Schutz vor Verlust
  - Iphone Tracker
  - Lookout
- Überwachung der Datennutzung
  - Android 4/LBE

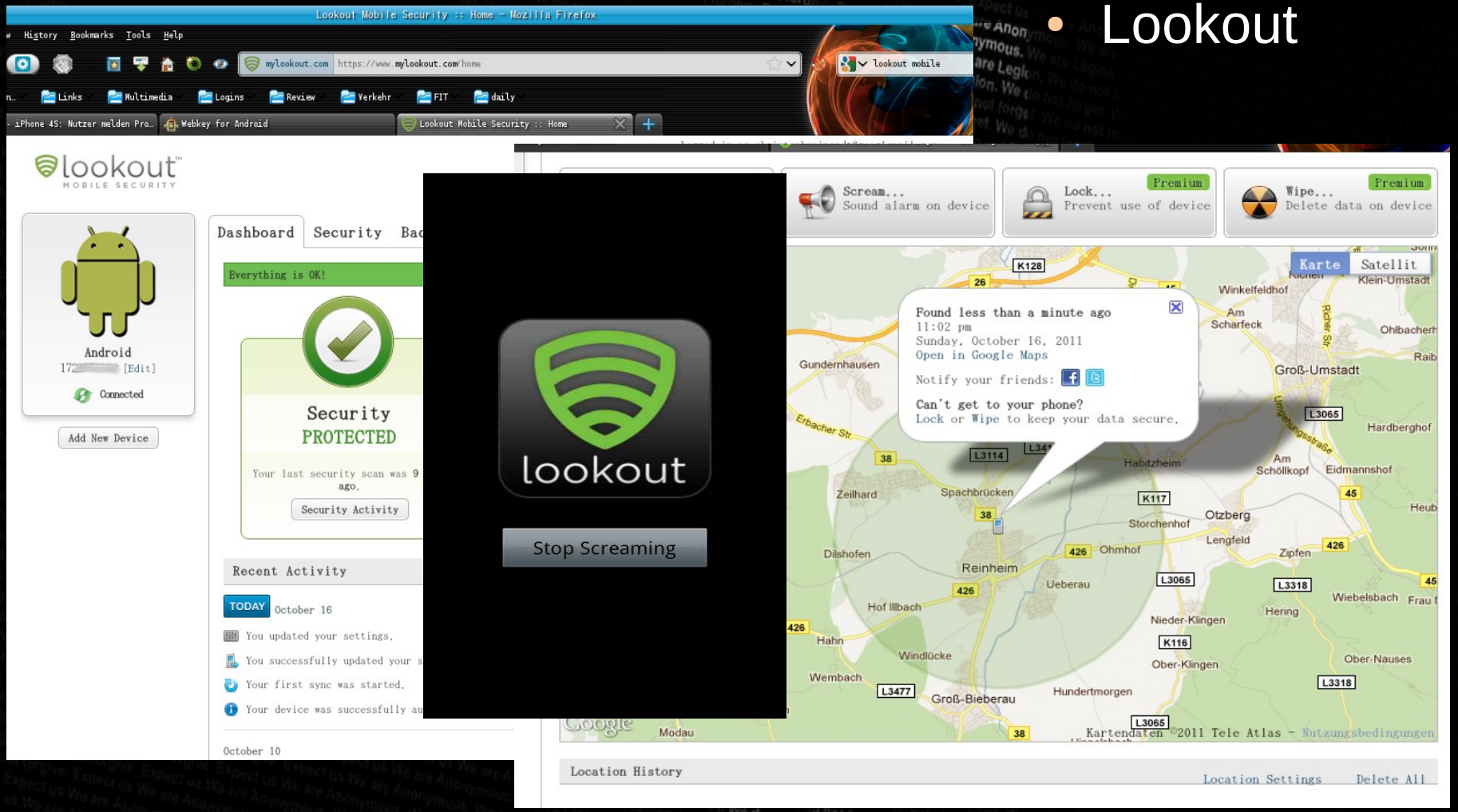
Tools

- Lookout „standard“
  - Malware Scanner gegen Trojaner
  - Backup zur automatisierten Datensicherung
  - Missing Device zum wiederfinden eines verlorenen oder gestohlenen Handys
- Lookout „premium“
  - Privacy advisor zum Schutz der eigenen Daten
  - Safe Browsing zum Schutz vor Malwareseiten beim Surfen
  - Remote Lock zum Sperren und Löschen eines verlorenen Handys

$ 2,99/monat oder $ 29,99/jahr

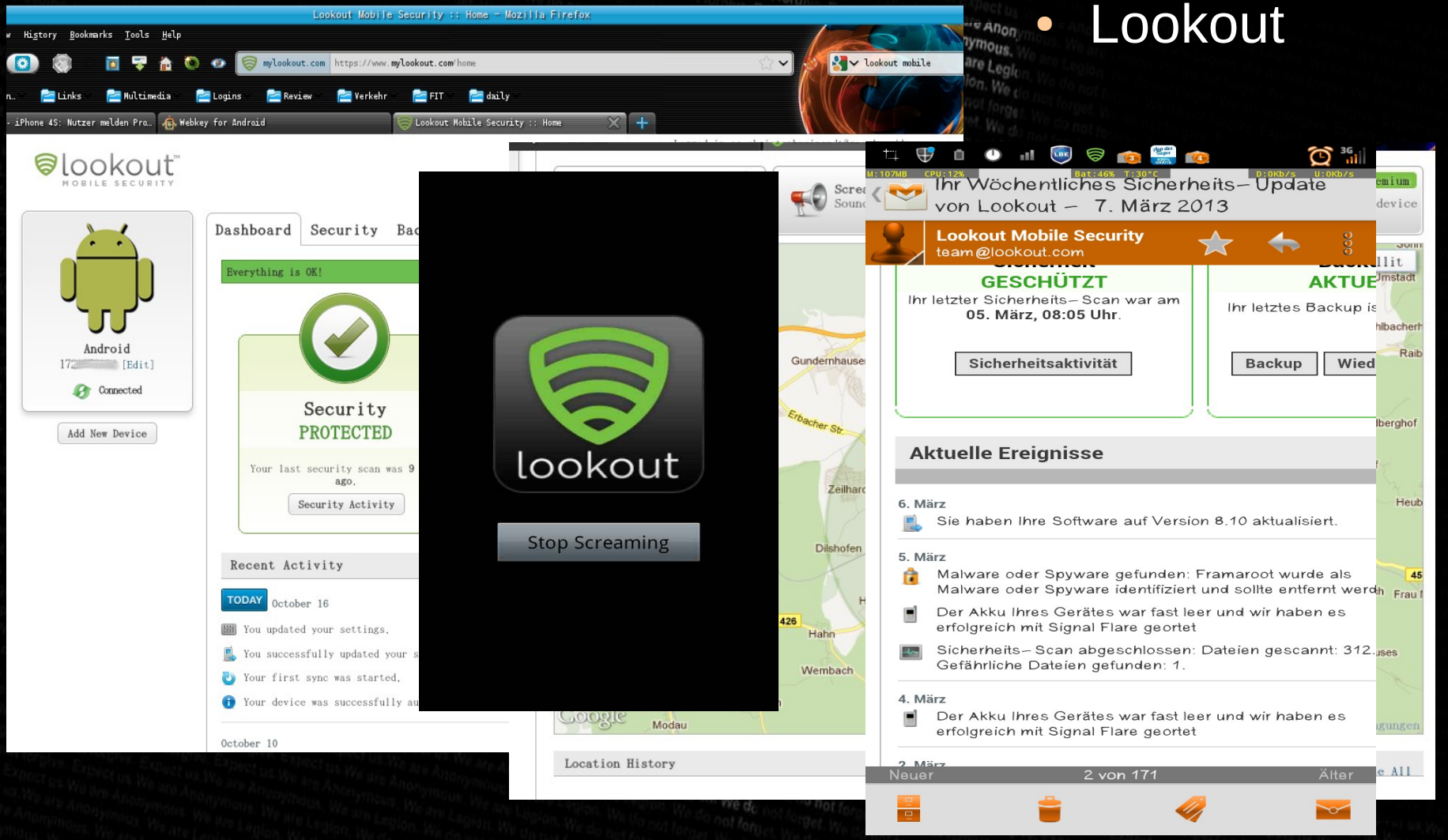
Tools

- Lookout



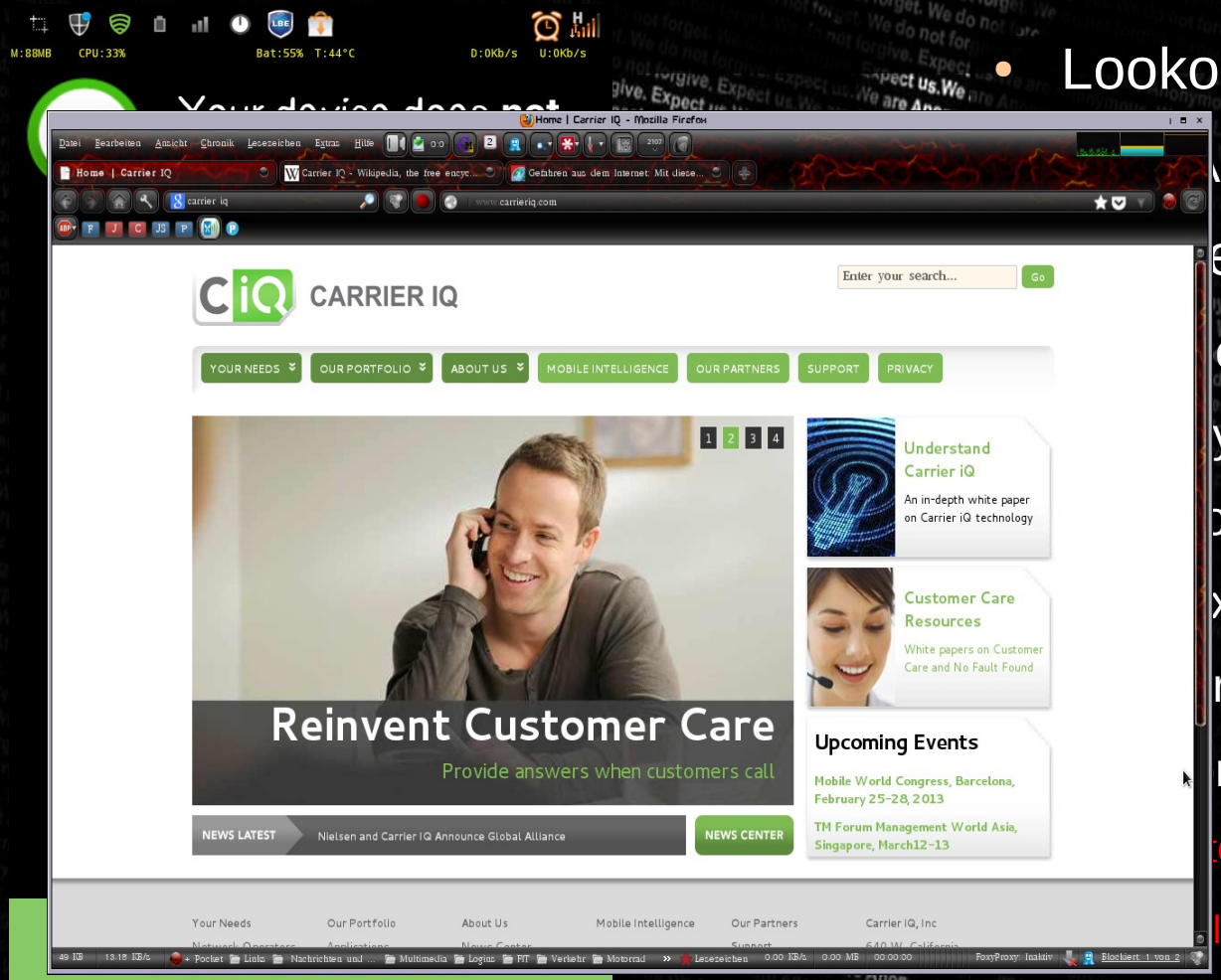
Tools

- Lookout



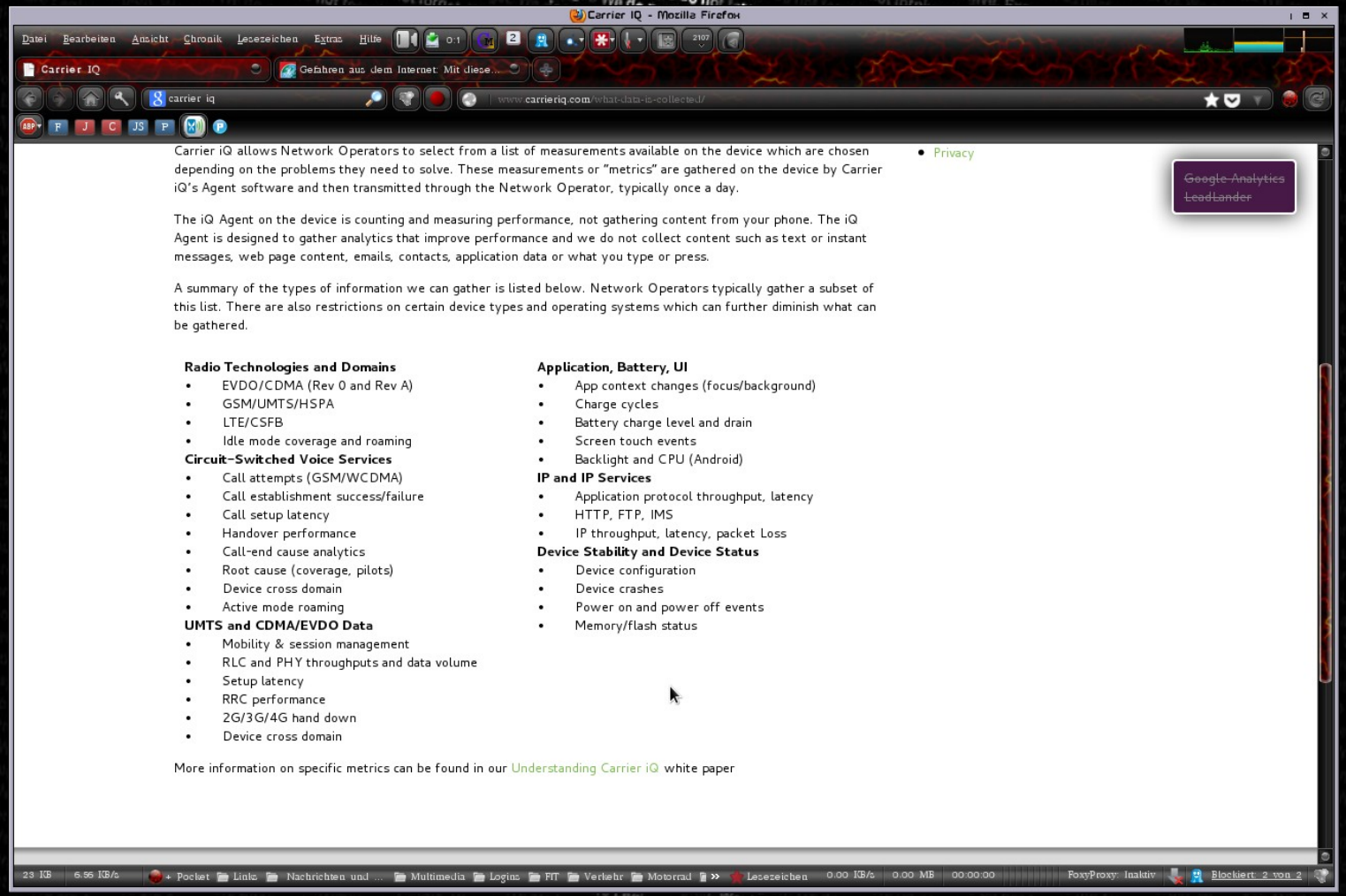
Tools

- Lookout „CarrierIQ“
- RRIER IQ Scanner
- erIQ“
- otkit
- ylogger
- owser Data Log
- xt Message Log
- rformance Data Log
- nsumer experience
- ernehmen
- le, Sprint, AT&T
- Samsung, Apple, HTC



LOOKOUT MOBILE SECURITY

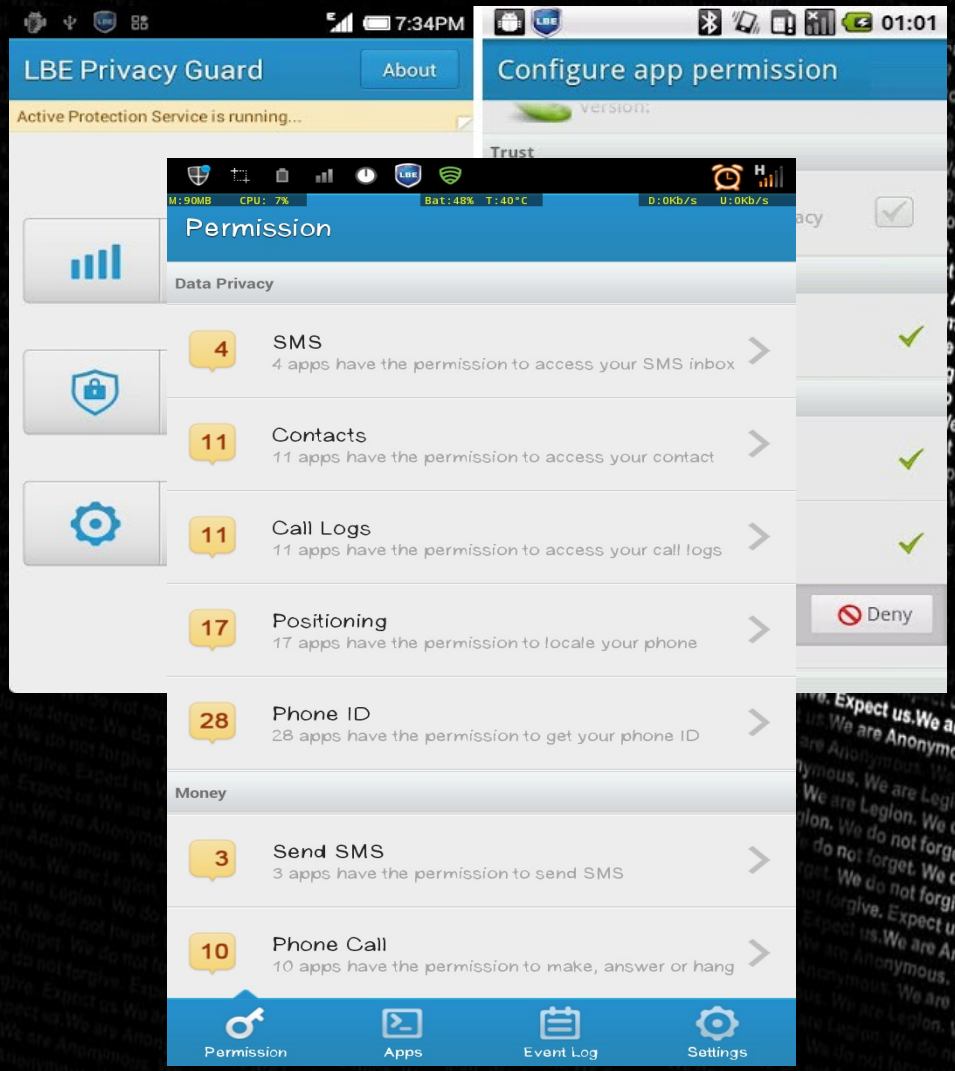
Tools: Carrier IQ



Tools

- Android Firewall
  - Zeigt versteckte Prozesse
  - Blockieren oder Erlauben eines Prozesses
  - Iptables Syntax
  - Iptables kommt von Linux wie Android auch

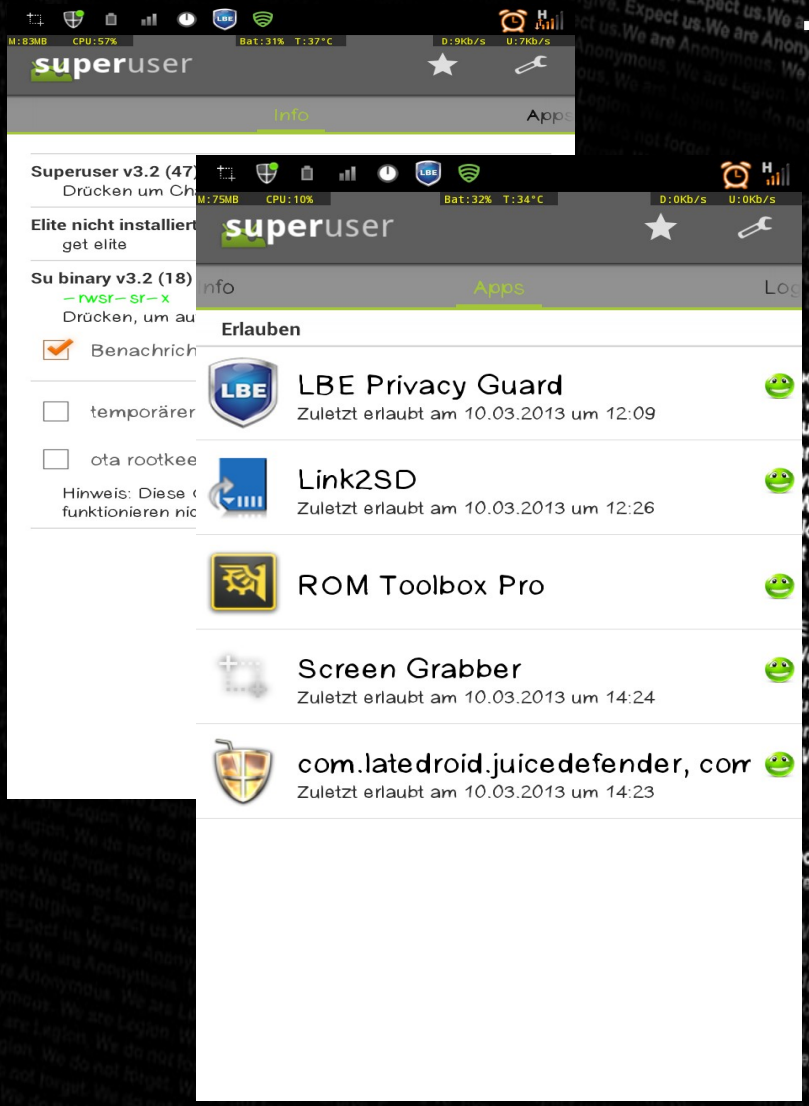
Tools



- LBE Privacy Guard
  - Rechte Management
  - Blockieren oder Erlauben eines Zugriffes
  - Überwachung der Datentransfers
  - Selbsterklärend
  - Nur mit ROOT Rechten wirksam

Tools

- SuperUser
  - Root Berechtigung

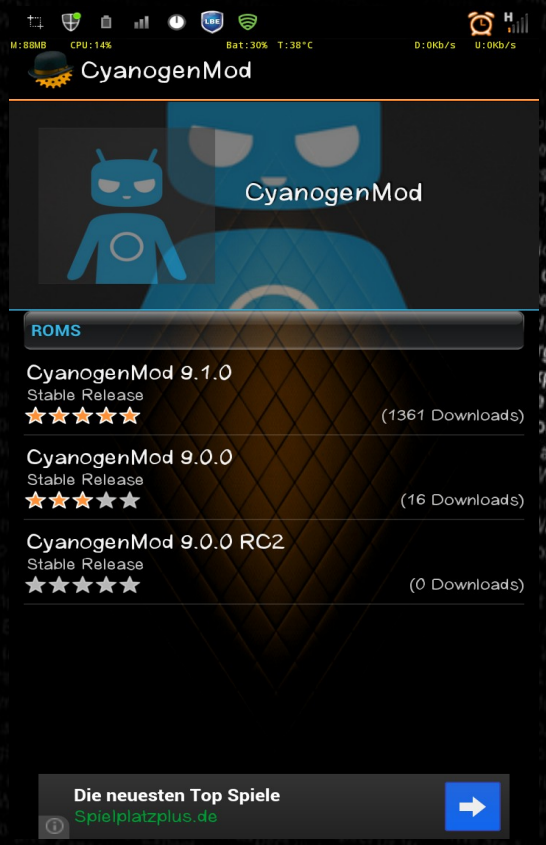


Tools

- Backup & Recovery
  - Rom Manager
  - Clockworkmod Recovery

Tools

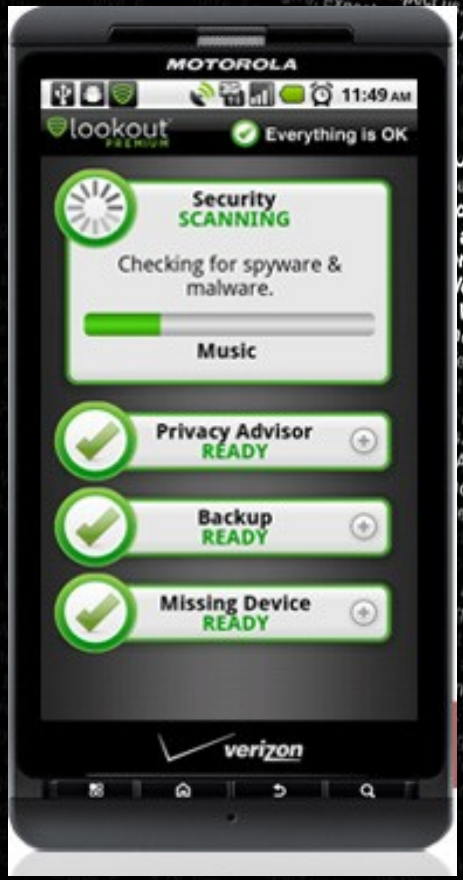
- Custom Rom
  - Cyanogen Mod 9.1



Agenda

LiveDemos

LiveDemo „Lookout“



- Features
  - Malware scanner
  - Privacy advisor
  - Online Backup
  - Missing Device

LiveDemo „LBE“

- Features
  - Rechtemanagement
  - Datenvolumen kontrolle
  - Paketfilter

LiveDemo
„Clockwork ModRecovery“

- Features
  - Backup und Restore
  - Firmware update
  - Cache Reset

Fazit

Einige wenige Apps und Verhaltensweisen geben Ihnen die Hoheit über Ihre Daten zurück und schützen Sie vor Missbrauch und Verlust!

Agenda

Vielen Dank für Ihre Aufmerksamkeit !

Vortragsfolien in Kürze unter
www.it-stammtisch-darmstadt.de