



KUKETZ
IT-SECURITY

Smartphones: Der Spion in meiner Tasche

Wo sind eigentlich meine Daten?
Habe ich eigentlich noch die Kontrolle?

[07.11.2013]



Was mache ich?

- ▶ IT-Sicherheitsberatung mit folgenden vier Schwerpunkten:
 - ▶ Netzwerksicherheit
 - ▶ Mobile Endgeräte
 - ▶ Penetrationstests
 - ▶ Systemabsicherung



Mike Kuketz

- ▶ **Kurz:** Den bösen Buben den Tag erschweren
- ▶ **Infos:** www.kuketz-security.de | www.kuketz-blog.de

Agenda

- ▶ Apps: Unsere täglichen Begleiter
- ▶ Berechtigungen von Apps am Beispiel von Android
- ▶ Schock! Und was kann ich jetzt tun!?



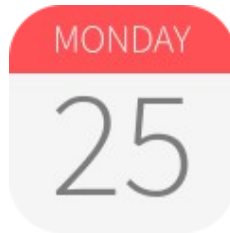
1. Apps: Unsere täglichen Begleiter

Was sind Apps?

- ▶ Apps sind Programme für Smartphones
- ▶ Erweitern den Funktionsumfang
- ▶ Bekannte Bezugsquellen:
 - ▶ GooglePlay Store (Android)
 - ▶ App Store (iOS)
- ▶ Es gibt kostenlose und kostenpflichtige Apps
 - ▶ 38% kaufen sich Apps
 - ▶ 45% nutzen lediglich kostenlose Apps
 - ▶ 17% laden keine zusätzlichen Apps
- ▶ **Allgemein gilt:** Smartphone Apps sind trendy, bunt und bieten oftmals einen Mehrwert

Kommunikation

► Standard-Apps



► AppStore



Navigation

► Standard-Apps



► AppStore



Spielkonsole

► AppStore



Soziale Netzwerke

► AppStore



Unzählige Beispiele ...

► **iOS:** > 1.000.000 Apps
Stand: Oktober 2013

► **Android:** > 1.200.000 Apps
Stand: Oktober 2013

Smartphones sind Taschenspione!

- ▶ Es gibt Apps für alle Lebenslagen!
- ▶ Smartphones erleichtern dadurch den Alltag
- ▶ Aber sie sind auch kleine **Taschenspione!**
- ▶ Es herrscht eine »Wild West Mentalität« – Apps greifen ungeniert auf sensible Informationen zu und leiten diese ungefragt weiter
- ▶ Selbst kostenpflichtige Apps sammeln Daten
- ▶ Smartphone Anwender haben längst die Kontrolle über ihre Daten verloren
- ▶ Niemand weiss wohin die Daten gehen und was damit passiert



2. Berechtigungen von Apps am Beispiel von Android

Das Popup vor jeder Installation...

- ▶ Fakten:
 - ▶ »Die hellste LED Taschenlampe«
 - ▶ Über 10 Millionen Downloads
 - ▶ 5 von 5 Bewertungssternen ★★★★★
 - ▶ Positives Kundenfeedback
 - ▶ Knapp 600.000 Rezensionen
- ▶ Und natürlich (extrem) wichtig:
 - ▶ **KOSTENLOS!**
 - ▶ Klasse – auf geht's!



App permissions

Super-Bright LED Flashlight needs access to:

Storage

Modify or delete the contents of your USB storage

Your location

Approximate location (network-based), precise location (GPS and network-based)

Camera

Take pictures and videos

Your applications information

Retrieve running apps

Phone calls

Read phone status and identity

Network communication

Full network access

Was sind Berechtigungen?



- ▶ »Das nervige Popup vor jeder Installation ...«
- ▶ ... ist **wichtig!**
- ▶ Es fasst zusammen: Was darf eine App und was nicht?
- ▶ **Idee:**
In ihrer Grundidee sollen Berechtigungen auf Android gewährleisten, dass Apps **ohne** explizite Rechte keinerlei Aktionen auf dem Gerät ausführen dürfen.
- ▶ **Realität:**
Überforderte Anwender, die sich weder mit den Berechtigungen herumschlagen wollen, noch den **Sinn** dahinter verstehen.

Berechtigungen Taschenlampen-App (1)

- ▶ (1) Bilder und Videos aufnehmen
 - ▶ **Gutartig:** Ohne diese Berechtigung kann die App die interne LED nicht aktivieren. Wird also benötigt, ansonsten leuchtet nichts.
 - ▶ **Bösartig:** Bilder und Videos aus **allen** Lebenslagen. Noch dazu benötigt die App keine Bestätigung durch den Nutzer.

- ▶ (2) USB-Speicherinhalte ändern und löschen
 - ▶ **Beschreibung:** Alle Inhalte im **USB-Speicher** oder auf der SD-Karte werden dauerhaft gelöscht und der USB-Speicher oder die Karte wird für die Verwendung mit Ihrem Telefon vorbereitet.
 - ▶ Für welchen **Zweck** benötigt eine Taschenlampe den Zugriff auf die SD-Karte oder USB-Speicher?

Berechtigungen Taschenlampen-App (2)

- ▶ (3) Voller Netzwerkzugriff
 - ▶ **Gutartig:** Die App ist kostenlos und finanziert sich durch die Darstellung von Werbung. Dazu wird Internetzugriff benötigt.
 - ▶ **Bösartig:** Im Hintergrund sammelt die App fleißig persönliche Daten. Dazu gehört bei dieser App die eindeutige **IMEI** oder Daten vom **USB-Speicher**, um die Bilder und Videos verschicken zu können ...

- ▶ (4) Telefonstatus und Identität abrufen
 - ▶ **Gutartig:** Bei einem Anruf beendet sich die App selbst bzw. unterbricht ihre Arbeit und merkt sich den aktuellen Zustand.
 - ▶ **Bösartig:** Ermöglicht der App die **Erfassung** von Telefonnummer, der IMEI oder IMSI.

Berechtigungen Taschenlampen-App (3)

- ▶ (5) Genauer (GPS-)Standort, ungefährender Netzwerkstandort
 - ▶ **Beschreibung:** Ermöglicht die Ortung über das GPS-Modul, Mobilfunkantennen oder WLAN-Accesspoints
 - ▶ Auch hier gilt: Wozu benötigt eine Taschenlampen-App meinen **genauen** Standort?

Alternative:



Search Light
zu finden im PlayStore

Analyse des Internetverkehrs

- ▶ Nach dem Start werden folgende Verbindungen aufgebaut:
 - ▶ *.doubleclick.net
 - ▶ *.flurry.com
 - ▶ *.mydas.mobi
- ▶ **DoubleClick:** Wurde von Google gekauft und wird oft mit Spyware in Verbindung gebracht. Ermöglicht eine Aufzeichnung der angezeigten Werbung und welche angeklickt wurde.
- ▶ **Flurry:** Sammelt und wertet Daten aus.
- ▶ **MyDas:** Gehört zu Millennial Media und ist vergleichbar mit Doubleclick. Blendet auf Basis gesammelter Nutzerdaten personalisierte Werbung ein.

Wozu die Datensammelwut?

- ▶ Staat / Geheimdienste:
 - ▶ Jagd auf Billionen politischer, wirtschaftlicher, gesellschaftlicher und militärischer Informationen
 - ▶ Im Zentrum: Politik- und Wirtschaftsspionage
- ▶ Unternehmen / Konzerne:
 - ▶ Aufbau von **detaillierten** Benutzerprofilen
 - ▶ Personalisierte Werbung und Marktprognosen
- ▶ Kriminelle:
 - ▶ Abgreifen von **Bankgeheimnissen** (TAN, Kreditkarten)
 - ▶ Zugriff auf sensible Daten für Erpressung



3. Schock! Und was kann ich jetzt tun!?

(1) Informieren.

(2) Aufklären.

(3) Alternativen aufzeigen.

Allgemeine Tipps für Android

- ▶ Zunächst einmal – Smartphone entrümpeln!
 - ▶ Auf welche Apps kann ich **verzichten**?
 - ▶ Welchen Apps **vertraue** ich / welchen nicht?
 - ▶ Welche Apps **verletzen** nicht nur meinen Datenschutz, sondern auch den meiner gespeicherten Kontakte?

Anschließend bei der Installation neuer Apps auf die **Berechtigungen** achten

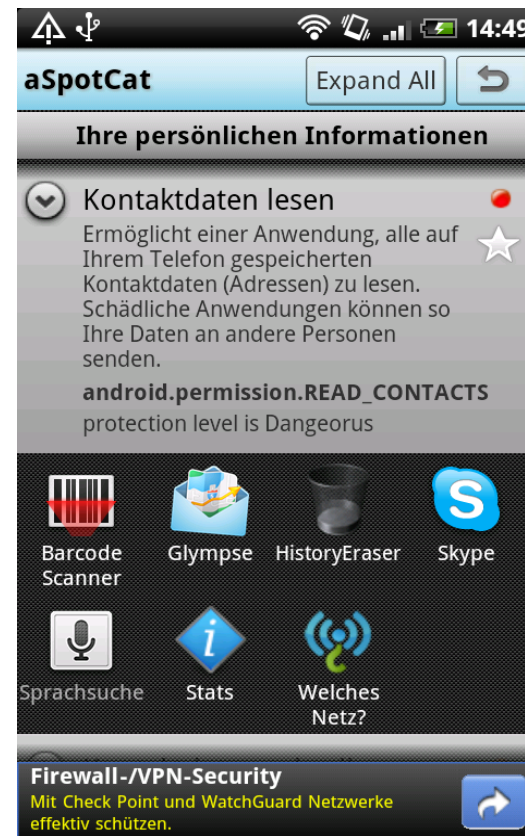
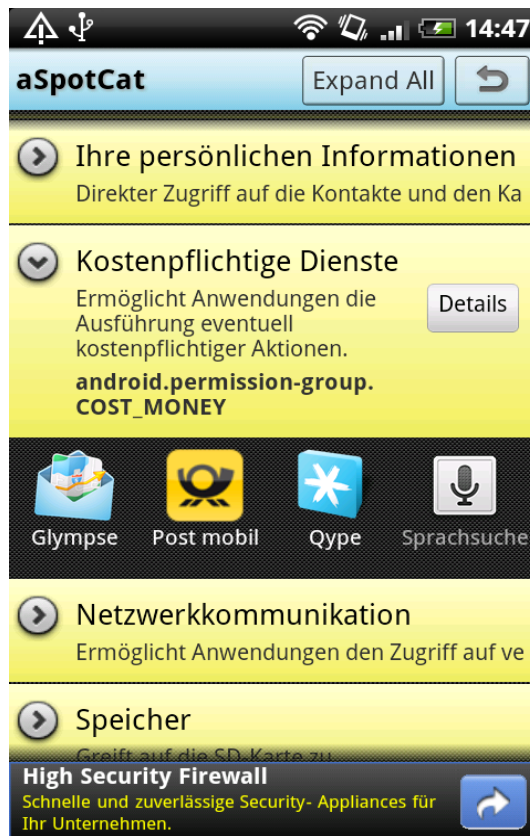
- ▶ Ich bin vollkommen planlos – Hilfe!

Android FirstAid Kit

In 5 Schritten zu mehr Sicherheit
und Datenschutz

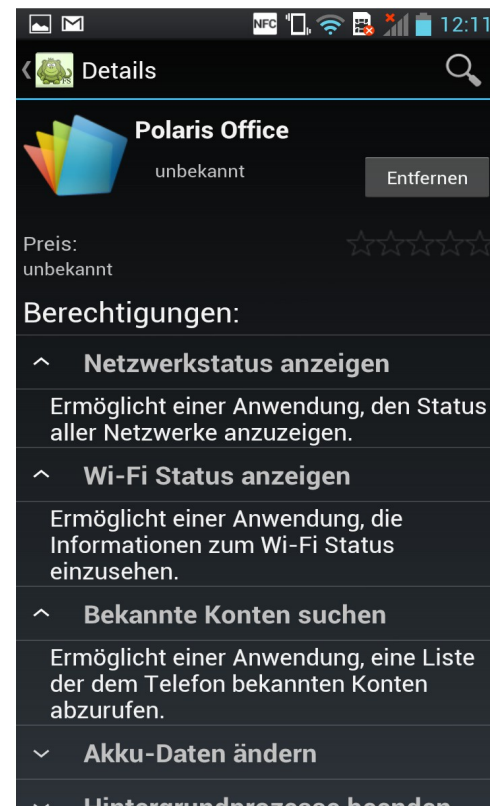
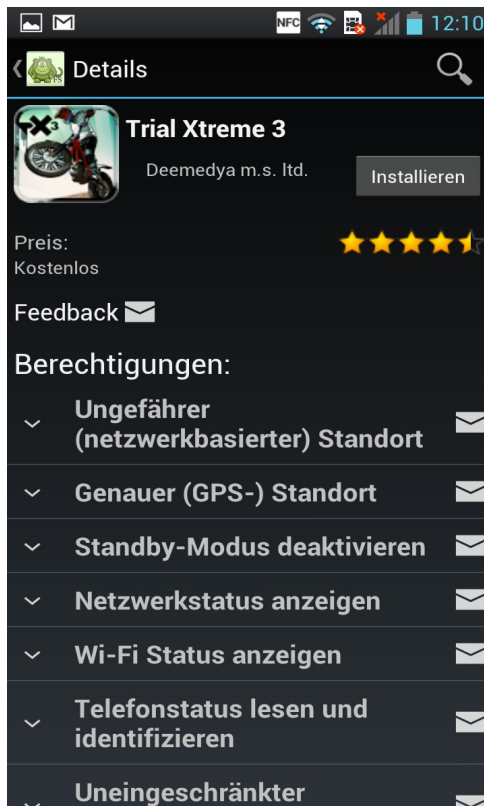
FirstAid – aSpotCat (1)

- Apps nicht installieren, die zu viele Berechtigungen einfordern. **aSpotCat** hilft beim Verständnis



FirstAid – APEFS (2)

- Gezielt nach Apps suchen, bei denen Sie selbst festlegen welche Berechtigungen »okay« sind. **APEFS** unterstützt diese Möglichkeit (Universität Siegen)



FirstAid – Entwickler Infos (3)

► Entwickler bieten teilweise Informationen aus welchem Grund Ihre App Berechtigung XY benötigt

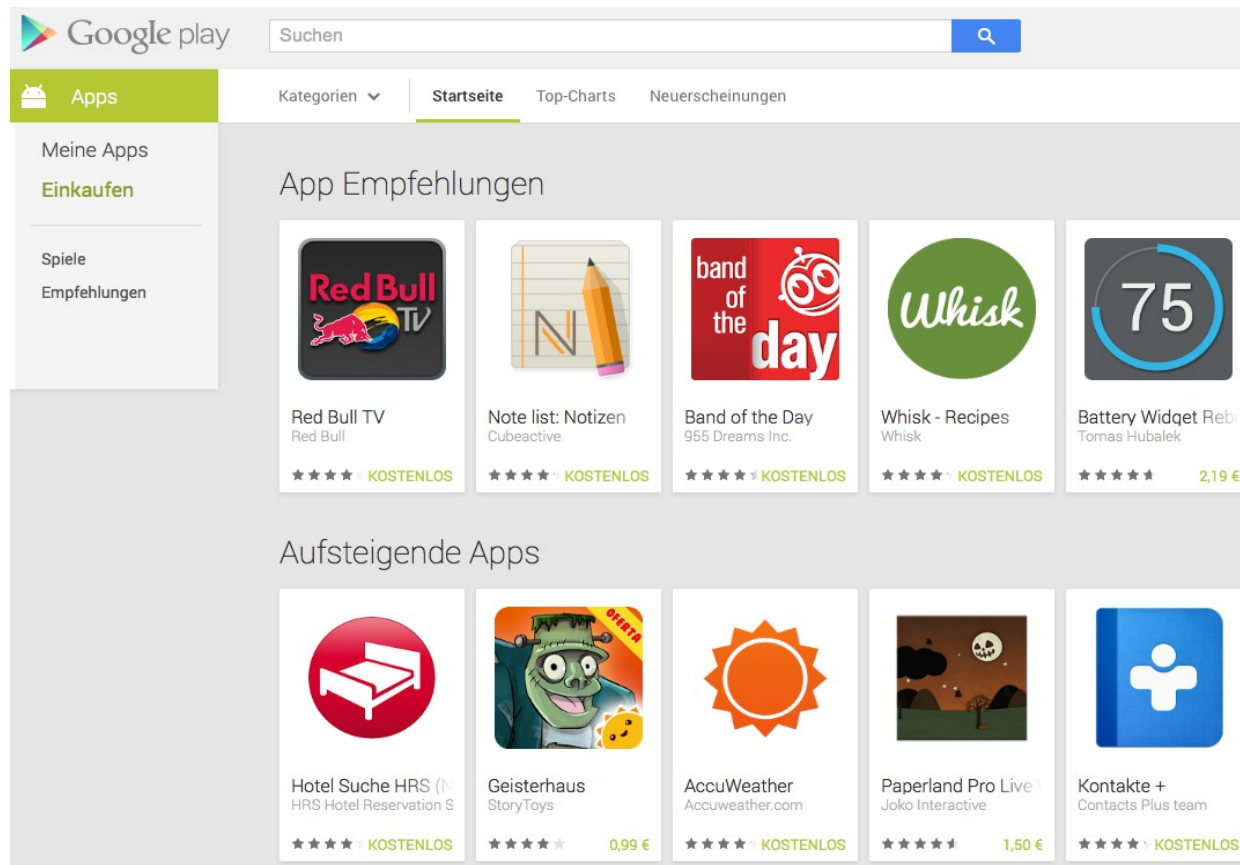
Firefox für Android verwendet zur Zeit folgende Berechtigungen:

- **Ihr Standort – genauer (GPS-)Standort.** Der GPS-Standort wird nur übertragen, wenn Sie sich entschließen, Ihren Standort einer Webseite mitzuteilen. Firefox nutzt Ihre Standortdaten niemals für sich selbst oder teilt die Daten niemals ohne Ihre Zustimmung einer Webseite mit. [Erfahren Sie mehr über standortbezogenes Surfen mit Firefox.](#)
- **Speicher – SD-Karten-Inhalt ändern/löschen.** Firefox nutzt diese Berechtigung, um heruntergeladene Dateien auf einer SD-Karte zu speichern. Firefox speichert ebenfalls seine eigenen Einstellungen und die Chronik auf einer SD-Karte, falls Sie Firefox über die Android-Einstellungen auf die SD-Karte verschoben haben.
- **Hardware-Steuerelemente – Bilder und Videos aufnehmen.** Wenn eine Webseite eine Bilddatei zum Hinaufladen anfordert, bietet Ihnen Firefox die Möglichkeit, mit der im Gerät eingebauten Kamera ein Foto zu erstellen. Firefox nimmt aber niemals ohne Ihre Zustimmung ein Foto oder Video auf. Für weitere Informationen lesen Sie bitte den Artikel [What's new for web developers in Firefox 9](#) („Was gibt's Neues für Webentwickler in Firefox 9“).
- **Netzwerkkommunikation – Uneingeschränkter Internetzugriff, Netzwerkstatus anzeigen.** Firefox nutzt diese Berechtigungen, um Webseiten, Erweiterungen oder andere Inhalte aus dem Internet herunterzuladen.
- **System Tools – Install shortcuts.** Diese Berechtigung wird von Firefox verwendet, um Ihnen zu ermöglichen, dass Sie Lesezeichen oder Web-Anwendungen auf dem Startbildschirm Ihres Gerätes ablegen.
- **System-Tools – Standby-Modus deaktivieren.** Das Adobe Flash-Plugin nutzt diese Berechtigung in den Versionen von Firefox, die Flash-Unterstützung bieten.
- **System-Tools – Allgemeine Systemeinstellungen ändern.** Firefox nutzt diese Berechtigung, um Ihr Firefox-Sync-Benutzerkonto zu aktivieren oder zu deaktivieren, wenn Sie Ihre Sync-Einstellungen ändern.
- **Ihre Konten – Als Kontoauthentifizierer fungieren, Authentifizierungsinformationen eines Kontos verwenden, Kontoliste verwalten.** Wenn Sie Firefox-Sync einrichten, benötigt Firefox diese Berechtigungen, um das Sync-Benutzerkonto zu ihren Android-Synchronisierungseinstellungen hinzuzufügen.



FirstAid – PlayStore (4)

- Vertrauenswürdige Quellen zum Download von Apps nutzen



FirstAid – Bewertungen (5)

- ▶ Vergessen Sie das Bewertungssystem und Kommentare in den App Stores – Selbst urteilen und nicht der Masse folgen!



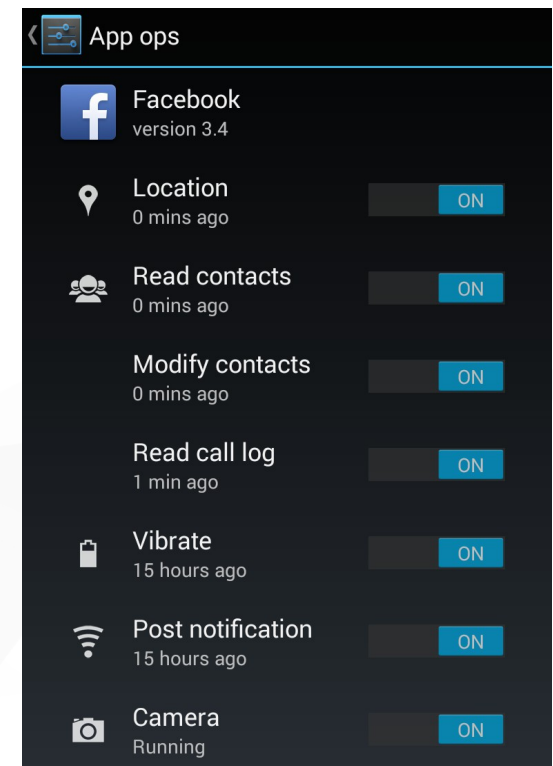
- ▶ Negativbeispiel: Mobiwol
- ▶ Keinerlei Funktion
- ▶ VPN-Tunnel nach Israel – was passiert mit meinen Daten?
- ▶ Trotz Kontaktaufnahme entfernt Google die App nicht
- ▶ Mehr Infos auf dem Blog: [Mobiwol Android Firewall Mogelpackung](#)

Bin ich jetzt sicher!?

- ▶ »Ja und Nein« → »Jein«
- ▶ Die Tipps helfen gegen die **größten** Datenschleudern
- ▶ Auf manche Apps wollen / können Sie aber **nicht** verzichten ...
- ▶ Wiederum andere Apps **beurteilen** Sie vielleicht falsch und nutzen Sie mit gutem Gewissen
- ▶ Daten verlassen noch immer **ungefragt** Ihr Smartphone
- ▶ Kann ich es **überhaupt** verhindern!?

Optional (1): Android 4.3

- ▶ Neue Funktion ab Android 4.3
- ▶ Rechteverwaltung »App Ops«
- ▶ **Problem:**
 - ▶ Ältere Geräte erhalten kein Update auf 4.3
 - ▶ Einige Berechtigungen lassen sich nicht verwalten
 - ▶ Funktioniert erst zuverlässig nach Löschen der App-Daten unter:
Einstellungen | Apps | App | Daten löschen



Optional (2): Gerät entsperren

- ▶ Smartphone »entsperren«:
 - ▶ Nennt sich bei iOS »**Jailbreak**«
 - ▶ Wird bei Android »**rooten**« genannt
- ▶ Ermöglicht die Veränderung des Systems und die Installation weiterer Apps (XPrivacy, OpenPDroid, AFWall+ ...)
- ▶ **Problem:**
 - ▶ Schwer für den normalen Verbraucher umzusetzen
 - ▶ Graubereich bei Gewährleistungs- und Garantiefällen
- ▶ **Fazit:** Ein sicheres oder gar datenschutzkonformes Smartphone existiert nicht. Wer sich und seine Daten schützen möchte muss dies in **eigene** Hände nehmen – und andere aufklären!

Vielen Dank ...

- ▶ ... für Ihre Aufmerksamkeit!
- ▶ ... für die Einladung zum Event!



Mike Kuketz
Dipl.-Inform. (FH)

Tel: +49 721 – 467 162 17
Mail: info@kuketz-security.de
Web: www.kuketz-security.de
Blog: www.kuketz-blog.de