ACD GRUPPE

14. September 2023 | Frank Römer, Sales

Android™ für den industriellen Einsatz - darauf sollten Sie achten!

Damals in der Windows CE-Welt…

1990	2000	2005
		

…und heute in der Android-Welt

- Intuitiv bedienbare, moderne Benutzerschnittstellen
- Basis ist Android
- Ist heute in allen Branchen zuhause, wie Logistik, Automotive, Gerätetechnik und Automatisierung

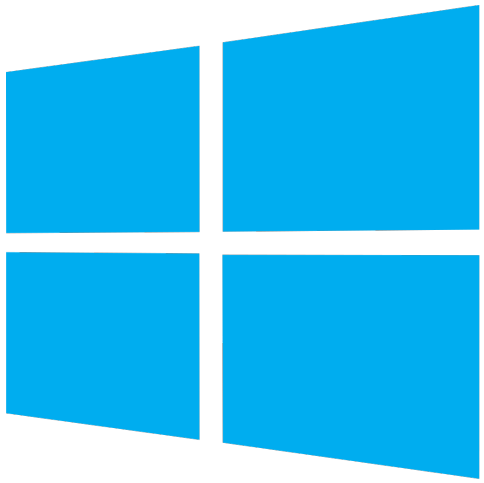
Smartphones und Android als Betriebssystem veränderten eine ganze Industrie

Für Sie als Nutzer stellt sich die Frage:

Was muss ich bei Auswahl und Kauf eines Android Gerätes beachten und warum?

Warum hat sich Android und nicht Linux durchgesetzt?

- ✓ Touchbedienung und Laufzeit
- ✓ Schnell programmierbare Standard-Apps statt native, proprietäre Programme (Java statt C)
- ✓ Wifi Anforderungen
- ✓ Industriestandard
- ✓ Schick & modern
- ✓ Mobile Anwendung



Was ist der Unterschied zwischen Windows und Android?

Windows oder Android?

1. Desktop-System
2. Embedded Betriebssystem

Mit Windows CE war die Embedded Welt noch einfach…

- Industrieprozessor
- Windows CE
- Einem Sensor, d. h. der eigentlichen Kundenanwendung

… und konnten Windows CE-Geräte aufgrund der CP/M, DOS und Windows Erfahrung (leicht) entwickelt werden

Durch den drastischen Technologiesprung ist die Android Geräte Entwicklung sehr aufwendig ….

Community (geführt von Google)

AOSP (Android Open Source Project)

↓ **AOSP**

Qualcomm, NXP, Broadcom, etc.

Spezifisches CPU BSP (Board Support Package)

↓ **BSP, AOSP**

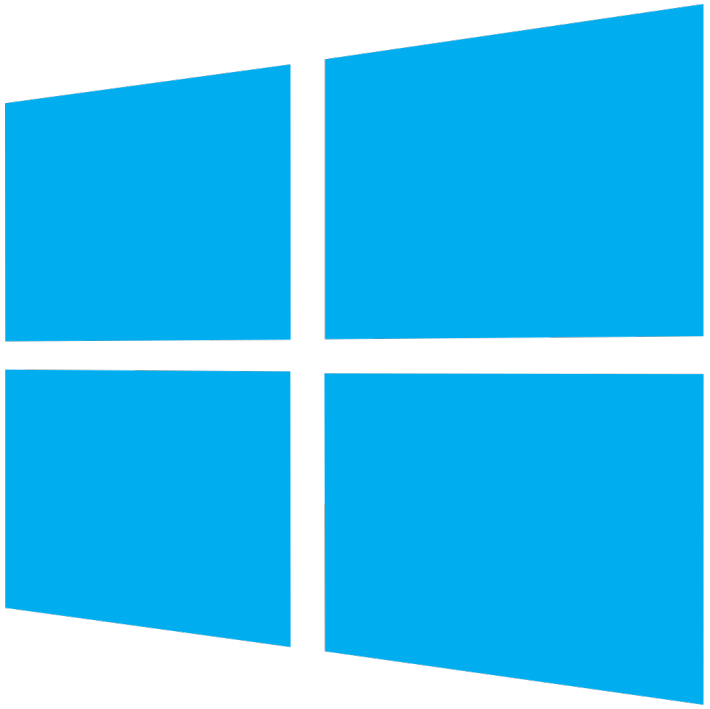
Hersteller von Mobilgeräten (ACD, asiatische ODMs, etc.)

Adaptation auf das spezifische Gerät, **jedes Android OS ist HW spezifisch**

- ✓ Vorgehen sehr aufwendig
- ✓ Hardware spezifisch
- ✓ Kostenfrei
- ✓ Kein Support und Wartung

Android ist Hardware spezifisch!

Dagegen ist Windows grundsätzlich anders aufgebaut



- Funktioniert auf allen x86 kompatiblen Chipsätzen
- Wird über Lizenzen verkauft
  Support durch Kauf der Lizenz, d. h. Updates und Sicherheitspatches
- Keine Open Source

Wie kann man mit einem Open Source (OS) Produkt Geld verdienen?

Die Rezertifizierung – GMS: Dienste für Daten

- GMS: Google Mobile Services
- Zusatzdienste (Playstore, Maps, etc.) nur mit Zustimmung zu den Lizenzbedingungen
- Enterprise Recommended für B2B

Was bedeutet Enterprise Recommended?

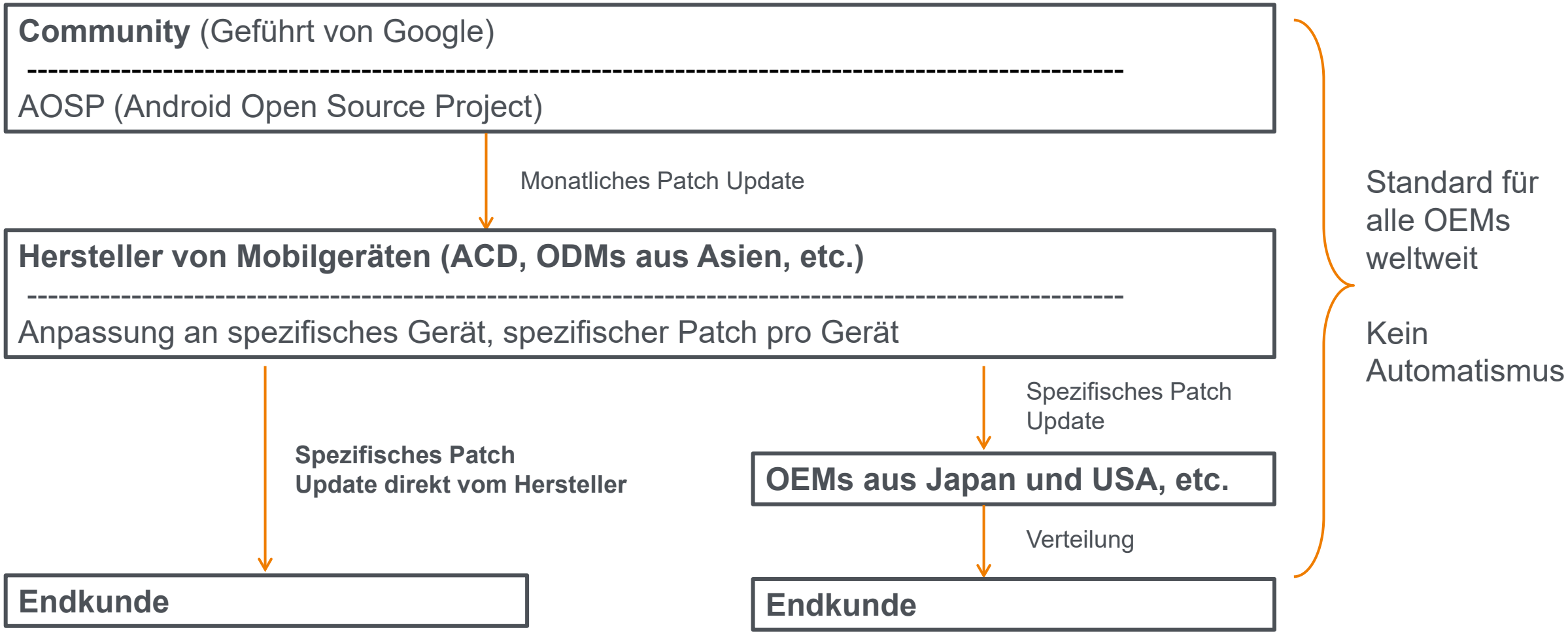
- Freiwillige Selbstverpflichtung, kein Label für besondere Robustheit
- Upgrades und Patches während der releasten Version, d. h. ca. drei Jahre – ändert sich immer mal wieder
- GMS ist Voraussetzung, also Dienste für Daten

Oder unsichere Systeme aus Asien

- Vorinstallierte Apps mit Malware-Funktionen
- Datenabwanderung durch vorinstallierte Apps
- Apps, die unerwünscht auf die Hardware wie z. B. Kamera zugreifen

Wie werden Updates und Upgrades bereit gestellt?

Wie programmiert man einen Patch oder ein Upgrade – immer Hardware spezifisch?



Patche sind Vertrauens-sache!

Prüfe, wer sich länger bindet: Strategien zur Android Auswahl

Frage 1

Wie sicher sind meine Daten bzw. ist Daten-sicherheit für mich wichtig?

Grundsätzlich gibt es folgende fünf Möglichkeiten

1. Ich nutze ein Smartphone und akzeptiere das

2. Ich nutze ein GMS/Recommended Gerät und akzeptiere das

3. Ich schotte mein Netz so ab, dass das Gerät nie Außenkontakt bekommt

4. Ich nutze ein industrielles Android Betriebssystem, das keine Google Dienste enthält

5. Ich nutze eine GMS/Recommended Gerät und nutzen einen GMS Blocker, erzeuge also nachträglich ein Gerät wie in Punkt 4.
   Etwas paradox, wird aber von den großen Brands oft so gemacht

Sichere Geräte sollten keine GMS Zertifizierung haben

1. **Datensicherheit ist nicht so wichtig**

→ GMS Gerät oder Smartphone
Mobile Geräte sind oft schon ab Werk mit Apps versehen, die Schad-Software enthalten

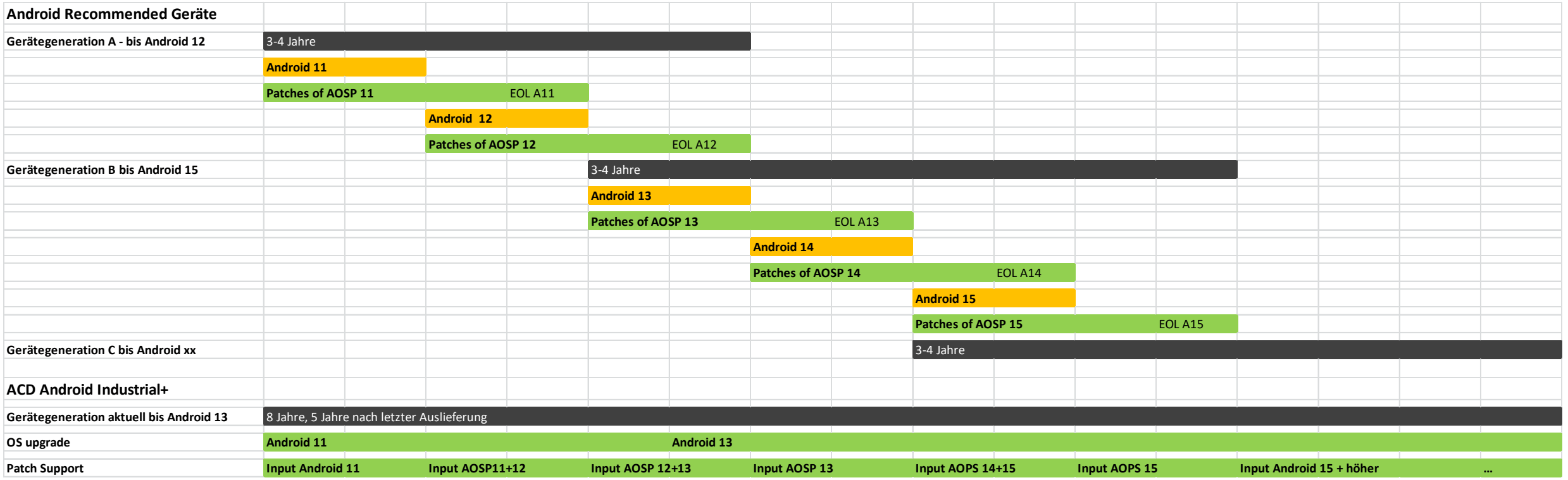
2. **Datensicherheit ist wichtig**

→ Gerät ohne GMS notwendig
Frei von Diensten Dritter und Langzeitverfügbarkeit

Frage 2

Wie lange bietet mein Anbieter Updates und Upgrades bzw. wie lange möchte ich mein Gerät nutzen?

Drei Jahre sind im Industrieumfeld zu wenig – Verfügbarkeit von Prozessor und Android ist entscheidend



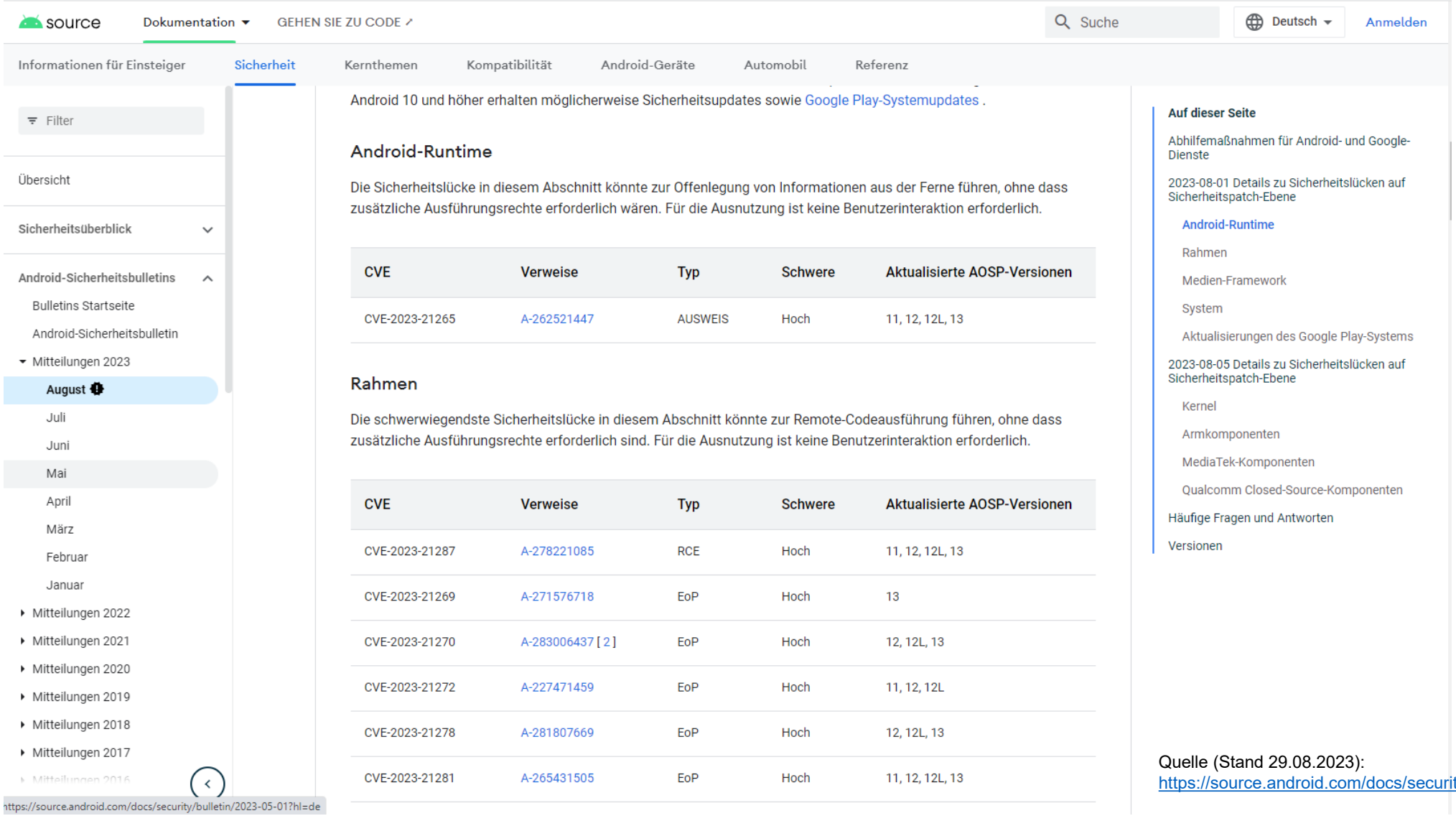
Sicherheitspatches – Allgemeines Vorgehen

Sicherheitspatches werden monatlich über Android.com über das AOSP (Android Open Source Project) zur Verfügung gestellt.

Diese werden in mehrere Kategorien eingeteilt:

- Moderate
- High
- Critical

Android-Sicherheitsbulletin



Quelle (Stand 29.08.2023):
https://source.android.com/docs/security/bulletin/2023-08-01?hl=de

ACD als Beispiel

- Innovatives mittelständisches Unternehmen
- Inhabergeführte Unternehmensgruppe
- **Seit 45 Jahren Spezialist für mobile und stationäre Geräte mit Benutzerschnittstellen …**
- **…und wir haben Android Expertise**

Sicherheitspatches – Vorgehen von ACD

1. Monatliches Treffen des Android-Sicherheits-Team
2. Prüfung, Qualifizierung und Priorisierung der Sicherheitspatches
3. ACD stellt eigene Sicherheitspatches zur Verfügung
4. Relevante Sicherheitspatches werden zwei Mal pro Jahr bereitgestellt
5. Auslieferung per OTA (Over the Air)
6. Roll-Out beim Kunden

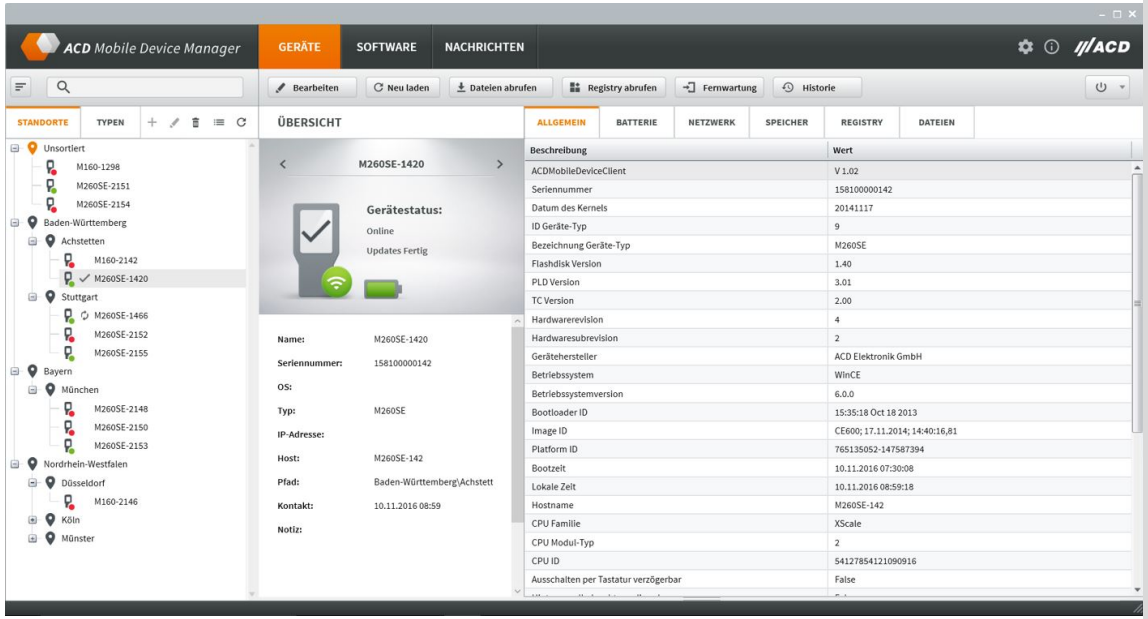
Sicherheitspatches – Vorgehen von ACD

- Android Industrial+ Sicherheitspatche unabhängig von der zugrunde liegenden AOSP Version
- Längere Supportphasen möglich
- Upgrades auf höhere Android-Versionen, jedoch nicht im schnellen Rhythmus von Consumer Geräten
- Relevante Sicherheitspatche werden über fünf Jahre nach Auslieferung oder länger mit Sondervereinbarung zur Verfügung gestellt

Frage 3

Wie möchte ich meine Geräte verwalten?

Für eine Geräteverwaltung gibt es vier Möglichkeiten



1. Händische Verwaltung
2. Drittanbieter wie SOTI, etc.
3. Herstellereigene Tools, z. B. ACD MDM
4. Mischung aus Drittanbieter und Google Diensten – Datensicherheit beachten

…und das sind die Möglichkeiten der ACD

Geräte-verwaltung	Geräte-einrichtung	Geräte-konfiguration	Geräteinformation und -updates	Kiosk-Betrieb	Geräte-kommunikation
ACD Mobile Device Manager Geräteverwaltung und zentraler Versand von Updates und Nachrichten	**ACD EasyToConfig** Einfache Konfiguration und Klonen von Geräten	**ACD ScanConfig** Konfiguration des integrierten Scanners	**ACD SystemApp** Informationen vom Mobilen Handheld Computer sowie Updatemöglichkeit	**ACD KioskMode** KioskMode zur Einschränkung für den Nutzer	**ACD WebAppService** Zur Kommunikation zwischen einer browserbasierten Webapplikation und der ACD-Hardware
ACD Remote File Commander Einfache Fernsteuerung von ACD Android™ Geräten via FTP	**ACD EasyToStart** Einfache Erst-einrichtung von Geräten und automatische Installation einer kundenspezifischen App	**ACD Network Manager** Übersichtliche Informationen und einfache Konfiguration von Netzwerken		**ACD KioskBrowser** KioskBrowser um eine einzige URL zuzulassen	
		ACD KeyConfig Einfache Konfiguration aller Tasten (Scannertasten, etc.)			

Android ist Hardware spezifisch!

Patche sind Vertrauenssache!

ACD kann Android!

Wenn Sie wissen möchten, wie eine individuelle Lösung
für Ihr Unternehmen aussehen könnte ...

Wir zeigen es Ihnen gerne persönlich!

ACD Elektronik GmbH | Engelberg 2 | 88480 Achstetten | Tel. +49 7392 708-499 | Email vertrieb@acd-elektronik.de | Web www.acd-gruppe.de

Beispiel 1 für Datenunsicherheit

Play Store

Spionage und unerlaubte Werbung: Diese Android-Apps sollten Sie deinstallieren

Teilen Pocket

Wer Android-Apps nicht beim Googles Play Store, sondern von einem anderen Anbieter herunterlädt, muss die Installation über die Sicherheitseinstellungen erlauben. dpa/Andrea Warnecke

Diese Sicherheits-Apps für Android sollten Nutzer löschen:

- Security Manager
- Virus Cleaner '20
- Super (Phone) Cleaner
- Clean Master

Zwar geben die Apps wie in diesem Fall vor, einen legitimen Zweck zu erfüllen, doch im Hintergrund installieren die Apps oft Malware.

Außerdem sollten folgende Android-Apps deinstalliert werden:

- Magic Filter Photo Editor
- Selfie Camera Pro
- Prizma Photo Effect
- Photo Editor
- Art Filter (Photo) App
- Smart Gallery
- Water Drink Reminder (Wasser Trinken Erinnerung)
- DU Recorder (Bildschirm Recorder)
- Ringtone Maker
- Hiketop+
- MP4 Video Downloader
- Tank Classic

Wer eine der oben genannten Apps auf dem Smartphone installiert hat, sollte diese deinstallieren, um kein Sicherheitsrisiko einzugehen.

Quelle (Stand 29.08.2023): https://www.focus.de/digital/handy/schaedliche-android-apps-welche-sie-nun-loeschen-sollten-wie-sie-sich-schuetzen_id_12177875.html

Beispiel 2 für Datenunsicherheit

Startseite

Aktuelle Betrugswarnungen

27. Mai 2022 um 17:48 Uhr
Alexander Kant, Maurice Ballein und Gerrit Gerbig

Das Internet steckt voller Gefahren, wie Betrugsmaschen und Viren. Damit ihr diese erkennt und vor ihnen gefeit seid, sammeln wir auf dieser Übersichtsseite aktuelle Betrugswarnungen.

Nur zu gerne nutzen Kriminelle die Möglichkeiten des Internets für ihre Zwecke aus. Täglich droht eine neue Gefahr aus dem Netz. Deshalb ist es wichtig, auf der Hut zu sein. Wir helfen euch dabei.

Diese Gefahren lauern im Netz

1. Phishing
2. Malware
3. Ransomware
4. Identitätsdiebstahl
5. Love-Scamming
6. Fake-Gewinnspiel
7. Abofallen
8. Anrufe

Quelle (Stand 29.08.2023): https://www.netzwelt.de/betrugswarnungen/index.html#google_vignette