

Wie wir bewerten – Methodik & Begründung

Transparenz über unser Bewertungssystem

Jede Bewertung auf checkmeinhandy.de folgt einer festen, nachvollziehbaren Methodik. Dieses Dokument legt offen, welche Kriterien wir bewerten, wie wir gewichten und warum. Wer mag, kann jeden Score selbst nachrechnen.

Wir haben uns für diesen Ansatz entschieden, weil Transparenz das ist, was wir einfordern — und was wir deshalb selbst vorleben sollten.

Das Grundprinzip

Bewertet wird ausschließlich, was fest im Gerät verbaut ist — das Betriebssystem und die Hardware. Apps, Browser oder Cloud-Dienste bleiben außen vor: die kannst du wechseln, den Chip nicht.

Jedes Gerät wird in **13 Kriterien** bewertet — 3 zur Software, 10 zur Hardware. Jedes Kriterium erhält **0 bis 5 Punkte**. Diese Punkte werden mit der jeweiligen Gewichtung des Kriteriums multipliziert.

$$\text{Score-Beitrag} = (\text{Punkte} \div 5) \times \text{Gewichtung des Kriteriums}$$

Die Summe aller Score-Beiträge ergibt den **Gesamtscore (max. 100%)**. Bislang hat kein verfügbares Consumer-Gerät 100% erreicht — weil manche Komponenten heute noch nicht offen oder kontrollierbar sind.

Warum Hardware stärker gewichtet? Das Betriebssystem (30%) lässt sich mit dem richtigen Gerät ersetzen. Was in den Chips steckt, lässt sich nicht

umprogrammieren. Deshalb trägt die Hardware (70%) mehr zum Score bei.

 **51–100%** — mehr Kontrolle und Transparenz

 **26–50%** — eingeschränkte Transparenz

 **0–25%** — wenig Kontrolle, viel Unbekanntes

Alle 13 Kriterien im Überblick

#	KRITERIUM	KATEGORIE	GEWICHTUNG
1	OS-Quelloffenheit	Software	12%
2	Eingebaute Telemetrie	Software	10%
3	Bootloader entsperrbar	Software	8%
4	Baseband / Modem	Hardware	22%
5	Hardware Kill-Switches	Hardware	12%
6	Firmware Blobs / Treiber	Hardware	8%
7	WLAN & Bluetooth Chip	Hardware	7%
8	TEE / Secure Enclave	Hardware	6%
9	NFC-Chip	Hardware	5%
10	Power Management IC	Hardware	4%
11	Hardware-ID IMEI	Hardware	3%
12	Hardware-ID MAC / Bluetooth	Hardware	2%
13	IMU / Bewegungssensoren	Hardware	1%

Software gesamt: 30% · Hardware gesamt: 70%

Kriterien im Detail

1. OS-Quelloffenheit

12%

Ist der Programmcode des Betriebssystems öffentlich einsehbar? Nur was offen liegt, kann von unabhängigen Experten auf Hintertüren oder Fehler geprüft werden. Geschlossene Systeme müssen blind vertraut werden.

PUNKTE	BEDEUTUNG
5	Vollständig offen, unabhängig auditierbar — kein versteckter Code (z.B. GrapheneOS, PureOS)
4	Überwiegend offen, kleine geschlossene Anpassungen ohne Datenfunktion (z.B. LineageOS + microG)
3	Offene Basis, aber Hersteller-Dienste laufen im Hintergrund mit eingeschränkter Prüfbarkeit
2	Offene Basis mit deutlichen proprietären Schichten (z.B. Samsung One UI, OxygenOS)
1	Stark veränderte Basis, umfangreicher geschlossener Code, kein vollständiger Audit möglich
0	Vollständig geschlossenes System, kein öffentlicher Quellcode (z.B. iOS, HarmonyOS)

2. Eingebaute Telemetrie

10%

Sendet das Betriebssystem automatisch Nutzungsdaten an den Hersteller oder Dritte? Bewertet wird nur das vorinstallierte System — nicht nachträglich installierte Apps. Android sendet im Standardzustand alle paar Minuten Daten an Google, auch bei gesperrtem Display.

PUNKTE	BEDEUTUNG
5	Nachweislich keine Datenübertragung — durch unabhängige Netzwerkanalysen belegt (z.B. GrapheneOS)
4	Minimale, vollständig abschaltbare Telemetrie — Standard: opt-in (z.B. LineageOS ohne Google-Dienste)
3	Telemetrie standardmäßig aktiv, aber vollständig deaktivierbar, keine verbleibenden Verbindungen
2	Abschaltbar, aber Restverbindungen bleiben aktiv (z.B. Google Framework bleibt im Hintergrund)
1	Ausgedehnte Datenerfassung, nur teilweise deaktivierbar (z.B. Standard-Android mit Google-Diensten)
0	Umfangreiche, nicht vollständig abschaltbare Übertragungen — auch bei deaktivierten Einstellungen

3. Bootloader entsperrbar

8% · Stufen: 0 / 3 / 5

Kann ich ein anderes Betriebssystem auf meinem Gerät installieren?
Ein gesperrter Bootloader macht dich dauerhaft abhängig vom Hersteller. Du kannst das vorinstallierte System nicht ersetzen — egal was er damit macht.

PUNKTE	BEDEUTUNG
5	Entsperrbar und danach wieder sicher verschließbar mit eigenem Schlüssel — volle Kontrolle (z.B. Pixel mit GrapheneOS)
3	Entsperrbar für alternatives OS, aber kein sicheres Re-Locking mit eigenem Schlüssel (z.B. Fairphone, OnePlus)
0	Nicht entsperrbar — Hersteller bestimmt, welches Betriebssystem läuft (z.B. iPhone, Samsung Knox)

4. Baseband / Modem

22%

Der Mobilfunk-Chip hat ein eigenes, verstecktes Betriebssystem und sendet Daten direkt ins Netz — an deinem Haupt-Betriebssystem vorbei. Das ist der größte blinde Fleck in jedem Smartphone. Kein Consumer-Gerät hat heute ein vollständig offenes Modem.

PUNKTE	BEDEUTUNG
5	Vollständig offenes Modem-System, unabhängig prüfbar — existiert derzeit in keinem Seriengerät
4	Physisch separater Modem-Chip, per Schalter vom Gerät trennbar (z.B. Librem 5 — Firmware noch proprietär)
3	Modem im Chip integriert, aber Abschirmung durch unabhängige Forscher bestätigt (z.B. Pixel, Fairphone mit Qualcomm)
2	Integriertes Modem, Abschirmung nicht unabhängig bestätigt, westlicher Hersteller ohne bekannte Kooperationen
1	Integriertes Modem mit bekannten Problemen oder dokumentierter staatlicher Einflussnahme auf den Hersteller
0	Dokumentierte Hintertüren oder nachgewiesene staatliche Kontrolle über Firmware-Updates

5. Hardware Kill-Switches

12% · Stufen: 0 / 3 / 5

Ein physischer Schalter trennt Kamera, Mikrofon oder WLAN direkt vom Strom — unabhängig vom Betriebssystem. Software kann umgangen werden. Ein physischer Schalter nicht. Heute sind solche Schalter nur in wenigen Spezialgeräten zu finden.

PUNKTE	BEDEUTUNG
5	3 oder mehr unabhängige Schalter (z.B. Librem 5: Kamera/Mikro, WLAN/BT, Modem)
3	1-2 physische Schalter (z.B. PinePhone)
0	Keine physischen Schalter — alle Abschaltungen nur per Software (alle gängigen Smartphones)

6. Firmware Blobs / Treiber

8%

Viele Chips im Smartphone — GPU, Kamera, Audio — benötigen geschlossene Steuerungsprogramme vom Hersteller. Dieser Code läuft auf deinem Gerät, kann aber von niemandem — nicht von dir, nicht vom Handyhersteller, nicht von Sicherheitsforschern — eingesehen werden.

PUNKTE	BEDEUTUNG
5	Keine geschlossenen Steuerungsprogramme für Kernfunktionen — in der Praxis kaum erreichbar
4	Minimale geschlossene Komponenten, alle sicherheitsrelevanten Treiber offen
3	Geschlossene GPU/Kamera-Treiber, aber WLAN offen und regelmäßige Sicherheitsupdates (z.B. Pixel, Fairphone)
2	Mehrere geschlossene Kernkomponenten, aktive Update-Politik (z.B. Samsung, OnePlus, Sony)
1	Umfangreiche geschlossene Komponenten, seltene oder keine Updates
0	Undokumentierte geschlossene Komponenten ohne jede Update-Politik

7. WLAN & Bluetooth Chip

7%

WLAN- und Bluetooth-Chips senden permanent Signale — auch wenn du nicht surfst. Ohne offene Firmware ist unklar, was dabei übertragen wird. Bewertet wird die Offenheit der Chip-Steuerung und die Update-Politik des Herstellers.

PUNKTE	BEDEUTUNG
5	Vollständig offene Firmware, unabhängig prüfbar — in aktuellen Smartphones nicht verfügbar
4	Geschlossene Firmware, aber Treiber im öffentlichen Linux-Kern, aktive Sicherheitspatches (z.B. Qualcomm in Pixel)
3	Geschlossene Firmware und Treiber, westlicher Hersteller ohne bekannte Hintertüren, aktive Updates
2	Geschlossene Firmware, eingeschränkte Update-Frequenz, bekannte frühere Schwachstellen (behoben)
1	Geschlossen ohne aktive Update-Politik, kein öffentliches Sicherheitsprogramm
0	Nachgewiesene Hintertüren oder staatlich kontrollierter Hersteller

8. TEE / Secure Enclave

6%

Ein isolierter Chip im Gerät verwahrt deine sensibelsten Daten: Fingerabdrücke, Passwörter, Zahlungsdaten. Wer diesen Chip kontrolliert, kontrolliert diese Daten. Die Frage ist, ob sein Innenleben offen und prüfbar ist.

PUNKTE	BEDEUTUNG
5	Vollständig offener Sicherheitschip, unabhängig auditierbar — derzeit in keinem Seriengerät
4	Separater, dokumentierter Sicherheitschip mit öffentlichem Sicherheitsbericht (z.B. Pixel Titan M2)
3	Industrie-Standard-Sicherheitsbereich, proprietär aber mit veröffentlichtem Sicherheits-Whitepaper
2	Proprietär, eingeschränkte Dokumentation, kein veröffentlichtes Sicherheits-Whitepaper
1	Bekannte ungepatchte Schwachstellen oder kein Programm zur Offenlegung von Sicherheitslücken
0	Dokumentierte Hintertür-Funktionalität

9. NFC-Chip

5% · Stufen: 0 / 3 / 5

NFC-Chips sind auf wenige Zentimeter Distanz aktiv — in U-Bahnen, Einkaufszentren, an Türen. Ohne die Möglichkeit, den Chip vollständig zu deaktivieren, ist dein Gerät im Umfeld solcher Lesegeräte potentiell erreichbar.

PUNKTE	BEDEUTUNG
5	Kein NFC verbaut (kein Angriffspunkt) oder Hardware-Schalter zum Abschalten
3	Per Software vollständig deaktivierbar, keine Hintergrundaktivität bei deaktiviertem NFC (Standard-Android)
0	Nicht vollständig deaktivierbar oder für Drittanbieter gesperrt (z.B. iPhone bis iOS 18.1)

10. Power Management IC

4% · Stufen: 0 / 3 / 5

Dieser Chip steuert, welche Komponenten wann Strom erhalten. Theoretisch könnte ein manipulierter Energiemanagement-Chip Teile des Geräts heimlich aktivieren — auch wenn das Betriebssystem sie "abgeschaltet" hat. Ein weitgehend unerforschtes Gebiet.

PUNKTE	BEDEUTUNG
5	Vollständig dokumentiert, Schaltpläne veröffentlicht (z.B. Librem 5, teilweise)
3	Chip von dokumentiertem westlichem Hersteller, Datenblatt verfügbar (z.B. Qualcomm PM in Pixel/Fairphone)
0	Hersteller unbekannt, Datenblatt nicht öffentlich oder staatlich beeinflusster Hersteller

11. Hardware-ID IMEI

3% · Stufen: 0 / 3 / 5

Die IMEI ist ein dauerhafter, unveränderlicher Fingerabdruck deines Geräts im Mobilfunknetz. Mit ihr lässt sich dein Gerät auch ohne SIM-Karte orten — solange es Empfang hat.

PUNKTE	BEDEUTUNG
5	Gerät lässt sich per Schalter vollständig vom Mobilfunknetz trennen — IMEI wird nicht gesendet (z.B. Librem 5)
3	Dual-SIM oder eSIM möglich, OS informiert transparent über IMEI-Verhalten (z.B. Pixel, Fairphone)
0	Keine Transparenz über IMEI-Weitergabe, kein Dual-SIM

12. Hardware-ID MAC / Bluetooth

2% · Stufen: 0 / 3 / 5

Die MAC-Adresse identifiziert dein Gerät in WLAN-Netzen eindeutig. Ohne Zufalls-Rotation können Einkaufszentren, Flughäfen und öffentliche Netze deine Bewegungen dauerhaft verfolgen — einfach weil dein Gerät nach bekannten WLANs sucht.

PUNKTE	BEDEUTUNG
5	Zufällige MAC bei jeder Verbindung — auch bei gespeicherten Netzen, standardmäßig aktiv (z.B. GrapheneOS)
3	Zufällige MAC für neue Netze standardmäßig aktiv (Android 10+, iOS 14+)
0	Keine MAC-Randomisierung, dauerhaft identifizierbar

13. IMU / Bewegungssensoren

1% · Stufen: 0 / 3 / 5

Gyroskop und Beschleunigungssensor sind eigentlich für Navigation gedacht. Studien zeigen jedoch, dass Tipp-Muster und Bewegungsprofile aus diesen Sensordaten zur eindeutigen Identifikation von Personen genutzt werden können.

PUNKTE	BEDEUTUNG
5	Sensor-Zugriff granular kontrollierbar, Messwerte werden durch Zufallsrauschen unkenntlich gemacht
3	Sensor-Zugriff per App-Berechtigung steuerbar, softwareseitige Einschränkung möglich
0	Keine Einschränkungen, jede App kann Sensordaten ohne Berechtigung auslesen

Zwei Beispiele im Vergleich

Hier siehst du, wie dieselbe Methodik auf zwei sehr unterschiedliche Geräte angewendet wird — einmal das Gerät mit dem derzeit besten erreichbaren Score in der Consumer-Klasse, einmal das weltweit meistgekaufte Smartphone.

Google Pixel 9 Pro mit GrapheneOS

~69% 

Das beste derzeit verfügbare Consumer-Gerät in dieser Bewertung.
GrapheneOS macht aus einem sehr guten Gerät ein außergewöhnliches —
aber die Hardware-Limitierungen (kein offenes Modem, keine physischen
Schalter) zeigen, wo die Industrie noch Hausaufgaben hat.

KRITERIUM	PUNKTE	GEWICHT	BEITRAG
OS-Quelloffenheit	5	12%	12,0%
Eingebaute Telemetrie	5	10%	10,0%
Bootloader entsperrbar	5	8%	8,0%
Baseband / Modem	3	22%	13,2%
Hardware Kill-Switches	0	12%	0,0%
Firmware Blobs / Treiber	3	8%	4,8%
WLAN & Bluetooth Chip	4	7%	5,6%
TEE / Secure Enclave	4	6%	4,8%
NFC-Chip	3	5%	3,0%
Power Management IC	3	4%	2,4%
Hardware-ID IMEI	3	3%	1,8%
Hardware-ID MAC / BT	5	2%	2,0%
IMU / Bewegungssensoren	5	1%	1,0%
Gesamtscore			~68,6% 

Apple iPhone 16 Pro

~17% 

Das weltweit meistgekaufte Smartphone — und eines der niedrigsten Ergebnisse in unserer Bewertung. Nicht weil Apple schlechte Hardware baut, sondern weil das Bewertungssystem Offenheit und Nutzerkontrolle misst. Beides ist beim iPhone grundsätzlich nicht vorgesehen.

KRITERIUM	PUNKTE	GEWICHT	BEITRAG
OS-Quelloffenheit	0	12%	0,0%
Eingebaute Telemetrie	0	10%	0,0%
Bootloader entsperrbar	0	8%	0,0%
Baseband / Modem	2	22%	8,8%
Hardware Kill-Switches	0	12%	0,0%
Firmware Blobs / Treiber	2	8%	3,2%
WLAN & Bluetooth Chip	3	7%	4,2%
TEE / Secure Enclave	3	6%	3,6%
NFC-Chip	0	5%	0,0%
Power Management IC	0	4%	0,0%
Hardware-ID IMEI	0	3%	0,0%
Hardware-ID MAC / BT	3	2%	1,2%
IMU / Bewegungssensoren	3	1%	0,6%
Gesamtscore			~21,6% 

Typische Score-Bereiche nach Gerätekategorie

GERÄTEKATEGORIE	TYPISCHER SCORE	FARBE
GrapheneOS auf Pixel (z.B. freifon-Geräte)	53–69%	
LineageOS + microG (z.B. freifon SKADI, ALRIK)	52–58%	

GERÄTEKATEGORIE	TYPISCHER SCORE	FARBE
Purism Librem 5 (mit physischen Kill-Switches)	~82%	
Google Pixel (Stock Android ohne GrapheneOS)	~43%	
Samsung Galaxy (One UI)	~36%	
OnePlus, Sony, Nokia (Stock Android)	38–42%	
Xiaomi, Oppo, Realme	28–35%	
Apple iPhone	~17–22%	
Huawei (HarmonyOS)	~12–18%	

Werte sind gerätespezifisch — die genauen Scores findest du für jedes Gerät einzeln auf checkmeinhandy.de.

Stand: August 2026 | checkmeinhandy.de

Dieses Dokument spiegelt den Stand der Technik zum Zeitpunkt der Erstellung wider. Bewertungen können sich durch OS-Updates, neue Erkenntnisse oder veränderte Geräteunterstützung ändern. Alle Scores auf checkmeinhandy.de werden bei Bedarf aktualisiert.

Check mein Handy wird betrieben von [Digital.Gemeinsam.Gestalten. e.V.](https://digital.gemeinsam.gestalten.de)