ANLEITUNG · CLAUDE CODE

FILMT DICH JEMAND IM AIRBNB? SO FINDEST DU ES

Der Skill **Privacy Scanner** prüft das WLAN deiner Unterkunft auf Geräte, die wie Kameras aussehen. Du brauchst einen **Laptop mit Claude Code**, ein Handy reicht nicht. In meinem Test mit 35 Geräten dauerte die Suche knapp zwei Minuten.

Schritt 1: Einmal einrichten, am besten zu Hause

Kopiere diesen Text in Claude Code:

```
Installiere den Skill von https://github.com/maluta/privacy-scanner in meine
Claude-Code-Skills. Installiere auch alles, was er braucht: nmap, arp-scan und die
Python-Pakete aus requirements.txt. Prüf danach, ob alles läuft.
```

Claude fragt dich unterwegs nach Erlaubnis. Getestet habe ich das nur auf dem Mac. Auf Windows musst du nmap eventuell selbst von nmap.org installieren.

Schritt 2: In der Unterkunft benutzen

1. Verbinde deinen Laptop mit dem **WLAN der Unterkunft**.
2. Schreib Claude Code diesen Text:

   ```
   Prüf dieses WLAN auf Kameras. Erstelle den Bericht auf Englisch und erkläre mir
   das Ergebnis auf Deutsch.
   ```

3. Der Scan braucht Admin-Rechte. Das **Passwort deines Laptops** gibst du selbst im Terminal ein, nicht im Chat.
4. Warte auf den Bericht. Größere Netze dauern länger als zwei Minuten.

Der Zusatz mit Englisch ist nötig, weil der Bericht sonst auf Portugiesisch kommt. Deutsch kann das Tool selbst nicht.

Schritt 3: Ergebnis lesen

`CRITICAL`	Starker Hinweis auf eine Kamera oder einen Videostream
`HIGH`	Deutliche Hinweise, sieh dir das Gerät an
`MODERATE`	Unbekanntes oder verdächtiges Gerät, versuche es zu finden
`LOW / INFO`	Vermutlich harmlos, zum Beispiel Smart-Home-Geräte

Wichtig: Jeden Fund gegenprüfen

- Das Tool irrt sich auch. Bei mir standen 5 Geräte auf kritisch, 3 davon passten, **2 waren harmlose Smart-Schalter**.
- Bevor du jemanden beschuldigst, schreib Claude: **„Prüf jeden kritischen Fund noch mal. Warum soll das eine Kamera sein, und kann es ein Fehlalarm sein?“**

WENN WIRKLICH EINE KAMERA DA IST

1. **Nicht anfassen, nicht ausstecken.** Sonst zerstörst du Beweise.
2. **Foto machen:** vom Gerät und von der Stelle, an der es steht.
3. **Bericht speichern:** Der HTML-Bericht und die Ausgabe im Terminal sind dein Nachweis.
4. **Airbnb melden:** App öffnen, deine Reise wählen, Hilfe aufrufen und das Sicherheitsproblem melden. Die Menüs können je nach App-Version anders heißen.
5. **Fühlst du dich unsicher,** verlass die Unterkunft und wende dich an die Polizei.

Airbnb verbietet Kameras in Innenräumen, auch wenn sie ausgeschaltet sind. Die aktuellen Regeln stehen im Airbnb-Hilfeartikel 3061.

Was der Scan nicht findet

- **Ausgeschaltete Kameras** oder Geräte im Standby
- **Kameras ohne WLAN,** die nur auf eine Speicherkarte aufnehmen
- **Kameras mit Mobilfunk** (4G) oder in einem eigenen, getrennten Netz
- **Reine Abhörgeräte** ohne Kamera

Kein Fund heißt also nicht, dass sicher keine Kamera da ist. Sieh dir zusätzlich Rauchmelder, Ladegeräte, Wecker und alles an, was aufs Bett oder ins Bad zeigt.

Gut zu wissen

- **Hotels:** Viele Hotel-WLANs trennen die Geräte der Gäste voneinander. Der Scan sieht dort oft fast nichts.
- **Der Bericht** ist auf Airbnb ausgerichtet. Bei anderen Vermietern nutzt du die Hilfe der jeweiligen Plattform.
- **Andere Gäste:** Der Scan erreicht alle Geräte im Netz, also auch die anderer Gäste im selben WLAN.
- **Sicherheit:** Der Skill stammt von einem fremden Entwickler. Ich habe den Hauptteil des Codes vor dem Test durchsucht und keinen Datenversand nach außen und keine Passwortversuche gefunden. Das ist keine vollständige Prüfung.

Rechtlicher Hinweis

Nutze den Scan nur in WLANs, in die du als Gast darfst, und nur, um dich selbst zu schützen. Ob das Abtasten fremder Geräte in einem fremden WLAN erlaubt ist, ist nicht eindeutig geklärt. Ich bin kein Anwalt. Im Zweifel frag den Gastgeber vorher. Greife niemals auf gefundene Geräte zu und versuche nicht, Bilder abzurufen.