BudujemyAI_

E-BOOK · LEKCJA 19 · MODUŁ 5

MODUŁ 5: TWOJE CENTRUM DOWODZENIA AI

Claude Code z telefonu 24/7 bez Maca mini: VPS, Ubuntu i Coolify

Własny serwer z Ubuntu, Remote Control i alarmami — Claude pracuje, gdy Ty jesteś w drodze

JEDNA PRACA, KTÓRĄ WYKONASZ

Postawisz własny serwer VPS z Claude Code, który działa 24/7 i którym sterujesz z telefonu.



Daniel Baranowski
BudujemyAI · wdrożenia AI w małych i średnich firmach
wiedza.budujemyai.pl · wydanie: listopad 2026

W skrócie

DLA KOGO	Dla właściciela firmy, który używa Claude Code i chce zlecać mu pracę z telefonu — także gdy komputer jest wyłączony.
JEDNA PRACA	**Postawisz własny serwer VPS z Claude Code, który działa 24/7 i którym sterujesz z telefonu.**
EFEKT	Masz bezpieczny serwer z Claude Code jako usługą 24/7, dostęp z telefonu, alarmy i listę testów odbioru.
CZAS	2–3 h
POZIOM	Zaawansowany
KOSZT	VPS od ok. 35 zł/mies. + plan Claude Pro lub Max (+ opcjonalnie Tailscale dla firm)
NARZĘDZIA	Claude Code, Aplikacja Claude, Hostinger VPS, Ubuntu 24.04 LTS, Tailscale, Termius, Coolify

Jak korzystać z tego e-booka

1. **Przeczytaj rozdziały 1–3** — zrozumiesz, po co to robisz i jak to działa.
2. **Zrób „Krok po kroku" z otwartym komputerem** — prompty skopiujesz z wersji online: wiedza.budujemyai.pl/ebooki/claude-code-z-telefonu/.
3. **Sprawdź wynik checklistą kontroli jakości** — to najważniejszy rozdział.
4. **Wracaj do „Zestawu do powtórzenia"**, kiedy robisz to następnym razem.

Spis treści

01 Zanim zaczniesz

02 Dlaczego to ważne dla Twojej firmy

03 Jak to działa — w prostych słowach

04 Ile to kosztuje — VPS czy Mac mini

05 Krok po kroku

06 Jak rozpoznać, że AI zrobiło dobrą robotę

07 Bezpieczeństwo i RODO

08 Jak to robię u siebie

09 Najczęstsze błędy

10 Zestaw do powtórzenia

11 Twój plan działania

12 Słowniczek

13 Źródła

14 Co dalej

ROZDZIAŁ 1

Zanim zaczniesz

Dla kogo: używasz już Claude Code (jeśli nie — zacznij od darmowego kursu Claude Code) i chcesz zlecać mu pracę z telefonu. Także wtedy, gdy laptop śpi w torbie, a Ty jesteś u klienta.

Jedna praca: postawisz własny serwer VPS z Claude Code, który działa 24/7 i którym sterujesz z telefonu.

Czego potrzebujesz:

- komputera z Windows lub macOS do konfiguracji (tylko na start),
- telefonu z aplikacją Claude (iOS lub Android),
- planu Claude Pro, Max, Team lub Enterprise — Remote Control nie działa na kluczu API,
- karty do zakupu serwera i menedżera haseł (lekcja o Bitwardenie).

Koszt: serwer od ok. 35 zł miesięcznie przy umowie na 24 miesiące (stan: październik 2026) plus Twój plan Claude. W firmie dolicz Tailscale Standard albo zostań przy publicznym SSH na klucze (szczegóły w części o kosztach); Coolify to drugi serwer, czyli drugi abonament. **Czas:** 2–3 h za pierwszym razem, Coolify to dodatkowa godzina. **Poziom:** zaawansowany, ale każde polecenie jest gotowe do wklejenia i opisane. Nie musisz znać Linuksa — musisz czytać, co wklejasz.

ROZDZIAŁ 2

Dlaczego to ważne dla Twojej firmy

Claude Code na laptopie ma jedną wadę: działa tylko wtedy, gdy laptop jest otwarty. Zamykasz klapę — praca staje. Wyjeżdżasz na dwa dni — agent czeka.

Wyobraź sobie właścicielkę małej agencji marketingowej. Poniedziałek, 7:40, korek. Klient pisze, że do 10:00 potrzebuje poprawionego cennika na stronie i zestawienia wyników kampanii. Laptop leży w biurze. Z serwerem pisze do Claude z telefonu: co zmienić, gdzie są pliki, po czym pozna, że jest dobrze. Gdy dojeżdża, w aplikacji czeka gotowa zmiana do przejrzenia. Ona decyduje i sprawdza, Claude wykonuje.

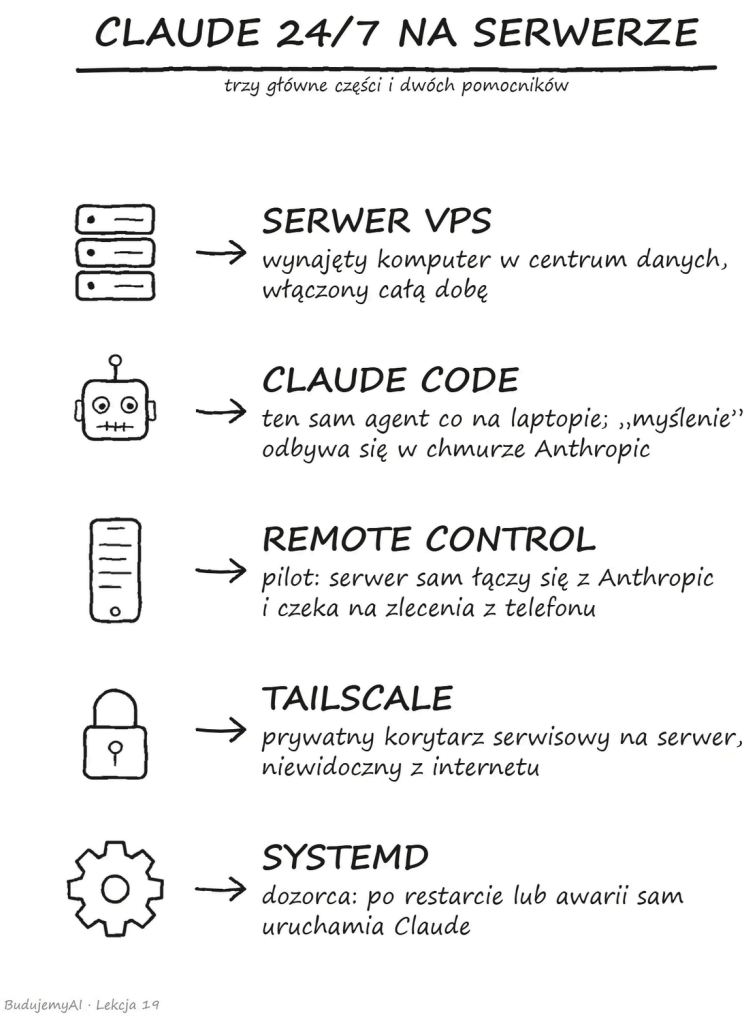
Typowe zastosowania w małej firmie:

- poprawki na stronie lub w aplikacji, które Claude przygotowuje w repozytorium,
- zestawienia i raporty z plików (oferty, cenniki, wyniki),
- długie zadania zlecane wieczorem i sprawdzane rano,
- dokumentacja i procedury pisane wtedy, gdy masz na nie głowę — także w drodze.

Częsta rada w sieci brzmi: „kup Maca mini i zostaw go włączonego”. Tymczasem Claude myśli w chmurze Anthropic. Twój komputer tylko wykonuje polecenia i trzyma pliki, a do tego wystarczy mały, wynajęty serwer. Jedna uczciwa uwaga: serwer widzi tylko to, co mu dasz — repozytoria, pliki i narzędzia, które tam umieścisz.

ROZDZIAŁ 3

Jak to działa — w prostych słowach



Układ ma trzy główne części i dwóch pomocników.

```
TEKST

Telefon (aplikacja Claude) ──► Anthropic ◄── Serwer VPS: Claude Code 24/7
          (szyfrowane połączenie, serwer sam łączy się na zewnątrz)

Komputer / telefon ──► Tailscale (prywatna sieć) ──► SSH: administracja serwerem
```

1. **Serwer VPS** — wynajęty komputer w centrum danych, włączony całą dobę. Jak biuro w strzeżonym biurowcu: prąd, internet i kopie zapasowe są po stronie zarządcy.
2. **Claude Code na serwerze** — ten sam agent co na laptopie. Czyta i zmienia pliki, uruchamia polecenia. Samo „myślenie" odbywa się w chmurze Anthropic, dlatego serwer nie musi być mocny (wymaganie: od 4 GB RAM).

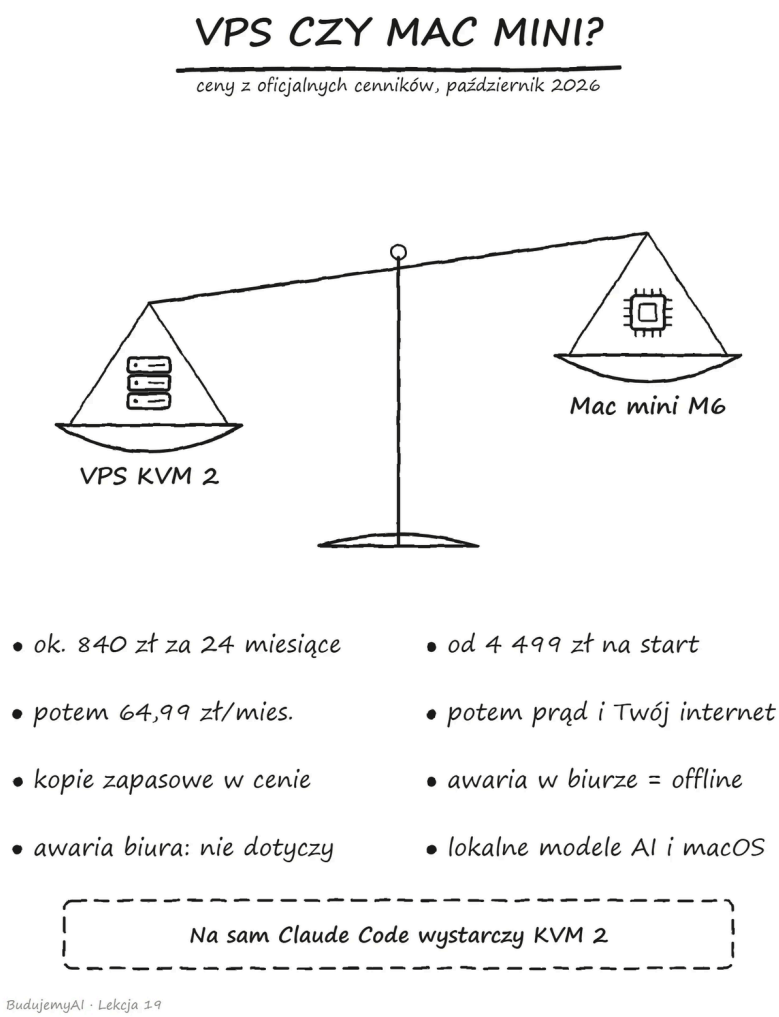
3. **Remote Control** — pilot. Serwer sam łączy się z Anthropic i czeka na zlecenia, jak taksówkarz, który zgłasza gotowość w aplikacji. Nikt nie musi się do niego dobijać, więc serwer nie otwiera żadnych portów. Telefon pokazuje rozmowę, wysyła polecenia i zdjęcia, a praca dzieje się na serwerze.

Pomocnicy: **Tailscale** to prywatny korytarz serwisowy, którym wchodzisz na serwer, niewidoczny z internetu. **systemd** to dozorca, który po restarcie lub awarii sam uruchamia Claude.

Opcjonalnie dochodzi **Coolify**: osobny serwer, który publikuje aplikacje i strony z GitHuba. Pierwszy serwer to warsztat, drugi — witryna sklepu. Awaria warsztatu nie zamyka sklepu.

ROZDZIAŁ 4

Ile to kosztuje — VPS czy Mac mini



Ceny z oficjalnych cenników (stan: październik 2026). Sprawdź aktualny cennik, w koszyku zobacz, czy doliczany jest VAT, i zapisz cenę odnowienia.

	VPS Hostinger KVM 2	Mac mini M6 (16 GB, 256 GB)
Parametry	2 vCPU, 8 GB RAM, 100 GB NVMe	12-rdzeniowy CPU, 16 GB pamięci
Na start	ok. 840 zł z góry za 24 mies. (34,99 zł/mies.)	od 4 499 zł
Później	64,99 zł/mies. po odnowieniu	prąd i Twój internet
Awaria prądu lub internetu w biurze	nie dotyczy	sesja offline

	VPS Hostinger KVM 2	Mac mini M6 (16 GB, 256 GB)
Kopie zapasowe	cotygodniowe w cenie planu	po Twojej stronie
Lokalne modele AI, aplikacje macOS	nie (brak GPU i macOS)	tak

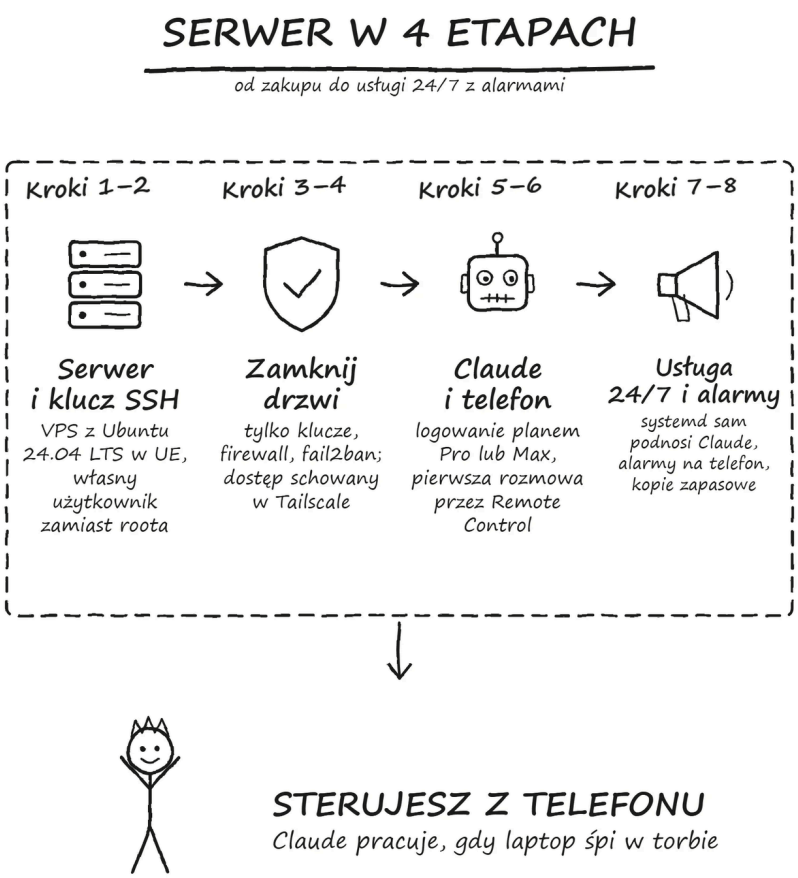
Rachunek przy niezmienionych cenach: za cenę bazowego Maca mini opłacisz KVM 2 przez prawie 7 lat (24 miesiące promocji, potem ok. 56 miesięcy po cenie odnowienia). Na sam Claude Code wystarczy KVM 2. KVM 1 (4 GB RAM) spełnia minimum, ale jest ciasny. KVM 4 lub KVM 8 wybierz, gdy obok działają Docker, kilka agentów albo renderowanie wideo.

Mac mini ma sens, gdy chcesz uruchamiać lokalne modele (lekcja o lokalnym LLM) albo potrzebujesz macOS. A jeśli masz już komputer włączony całą dobę, Remote Control zadziała i na nim.

Pozostałe koszty: Claude Pro 20 USD/mies. (17 USD przy płatności rocznej), Max od 100 USD/mies. Tailscale w planie Personal jest darmowy tylko do użytku niekomercyjnego — dla firmy właściwy jest Standard, 8 USD za użytkownika miesięcznie. Termius (Starter) i ntfy są darmowe.

ROZDZIAŁ 5

Krok po kroku



W poleceniach podmieniaj: `TWOJ_SERWER` — publiczny adres IP serwera z panelu dostawcy, `100.x.y.z` — adres serwera w Tailscale, `ania` — nazwę Twojego użytkownika. Każde polecenie, którego nie rozumiesz, wklej najpierw do Claude z promptem „Wyjaśnij, zanim wkleję" z sekcji Zestaw do powtórzenia.

Wklejaj po jednej linii i czekaj, aż poprzednia się skończy. Gdy program o coś pyta (hasło, `y/n`, kod logowania), najpierw odpowiedz — inaczej następna wklejona linia zostanie wzięta za odpowiedź. Wyjątek: blok z `<<'EOF'` … `EOF` w kroku 3 wklejasz w całości, a tuż przed nim wpisz `sudo -v`, żeby ewentualne pytanie o hasło padło wcześniej. Instalatory `curl … | bash` działają z prawami Twojego konta (a z `sudo` — z pełnymi prawami do serwera), dlatego bierz je tylko z oficjalnej dokumentacji programu (linki w Źródłach).

Krok 1: Kup serwer i przygotuj klucz SSH

Klucz SSH to para plików: kłódka (klucz publiczny) trafia na serwer, a klucz prywatny zostaje na Twoim komputerze. Logujesz się bez hasła, więc nie ma czego zgadywać ani podsłuchać. Na komputerze otwórz Terminal (macOS) lub PowerShell (Windows):

```
TERMINAL

ssh-keygen -t ed25519 -C "laptop-firma"
```

Na pytanie o plik naciśnij Enter (domyślne miejsce). Jeśli padnie `Overwrite (y/n)?`, wpisz `n` — masz już klucz i użyjesz go. Ustaw hasło do klucza i zapisz je w Bitwardenie. Klucz publiczny wyświetlisz poleceniem:

```
TERMINAL

cat ~/.ssh/id_ed25519.pub
```

W Hostingerze wybierz VPS (na start KVM 2), okres 24 miesiące, centrum danych w UE (dla VPS dostępne są m.in. Niemcy, Litwa i Francja) i system **Ubuntu 24.04 LTS** bez dodatkowych paneli. W kreatorze wklej klucz publiczny (linię zaczynającą się od `ssh-ed25519`). Włącz kopie zapasowe i wpisz do kalendarza przypomnienie przed końcem okresu — po promocji cena rośnie.

> **i Dlaczego Ubuntu 24.04 LTS**
>
> Wersja LTS dostaje poprawki bezpieczeństwa przez 5 lat (24.04 — do maja 2029). Nowsze 26.04 LTS też istnieje, ale dokumentacja Coolify wymienia 24.04 — dla spójności obu serwerów zostań przy 24.04.

Krok 2: Własny użytkownik zamiast roota

Root to konto „właściciela budynku” — może wszystko, więc nie pracujesz na nim na co dzień. Zaloguj się pierwszy raz z komputera:

```
TERMINAL

ssh root@TWOJ_SERWER
```

Przy pierwszym połączeniu potwierdź odcisk serwera, wpisując `yes`. Już na serwerze załóż swoje konto:

```
TERMINAL

adduser ania
```

`adduser` zapyta o hasło (zapisz je w Bitwardenie — przyda się do `sudo` i do konsoli awaryjnej w panelu dostawcy) i o dane, które pominiesz klawiszem Enter. Potem nadaj kontu uprawnienia i skopiuj klucz:

```
TERMINAL

usermod -aG sudo ania
mkdir -p /home/ania/.ssh
cp /root/.ssh/authorized_keys /home/ania/.ssh/
chown -R ania:ania /home/ania/.ssh
```

Nie zamykając tego okna, otwórz drugie i zaloguj się na nowe konto: `ssh ania@TWOJ_SERWER`. SSH może zapytać o hasło do klucza (`Enter passphrase for key`), ale nie o hasło konta (`ania@…'s password`) — to znak, że klucz nie działa i trzeba go poprawić w pierwszym oknie. Na nowym koncie:

```
TERMINAL

sudo apt update && sudo apt upgrade -y
sudo apt install -y git tmux mosh fail2ban curl
```

Jeśli `upgrade` pokaże niebieskie okno z pytaniem (np. o plik konfiguracyjny SSH), zostaw odpowiedź domyślną — przy pliku to `keep the local version currently installed` — i zatwierdź Enterem.

Krok 3: Zamknij drzwi: tylko klucze, firewall, fail2ban

Wyłączasz logowanie hasłem i logowanie roota. Pułapka: obrazy serwerów potrafią mieć w katalogu `sshd_config.d` plik z ustawieniem `PasswordAuthentication yes`, a SSH bierze **pierwszą** znalezioną wartość. Dlatego Twój plik ma prefiks `00-`, a wynik sprawdzasz poleceniem `sshd -T`, które pokazuje ustawienia wynikające ze wszystkich plików naraz.

```
TERMINAL

sudo tee /etc/ssh/sshd_config.d/00-utwardzenie.conf > /dev/null <<'EOF'
PermitRootLogin no
PasswordAuthentication no
KbdInteractiveAuthentication no
EOF
sudo sshd -t && sudo systemctl restart ssh
sudo sshd -T | grep -Ei 'permitrootlogin|passwordauthentication|kbdinteractive'
```

Oczekiwany wynik: trzy linie zakończone słowem `no`. Dowód z zewnątrz: w nowym oknie na komputerze wpisz `ssh -o PubkeyAuthentication=no ania@TWOJ_SERWER` — ma od razu paść `Permission denied (publickey)`, bez pytania o hasło. Teraz firewall (ufw — bramkarz, który wpuszcza tylko z listy) i fail2ban (ochroniarz, który banuje adresy po kilku nieudanych próbach):

```
TERMINAL

sudo ufw allow OpenSSH
sudo ufw enable
sudo fail2ban-client status sshd
```

Na pytanie ufw odpowiedz `y`. Fail2ban powinien pokazać aktywną „celę" `sshd`. Automatyczne aktualizacje bezpieczeństwa Ubuntu ma włączone domyślnie — `systemctl is-enabled unattended-upgrades` powinno zwrócić `enabled`. Jeśli zamiast tego zobaczysz błąd, że takiej usługi nie ma, zainstaluj ją: `sudo apt install -y unattended-upgrades`.

Krok 4: Schowaj dostęp w prywatnej sieci Tailscale

```
TERMINAL

curl -fsSL https://tailscale.com/install.sh | sh
sudo tailscale up
tailscale ip -4
sudo ufw allow in on tailscale0
```

`tailscale up` wyświetli link — otwórz go i zaloguj się. Zainstaluj Tailscale na komputerze (na telefonie tylko wtedy, gdy chcesz terminal awaryjny — aplikacja Claude działa bez niego). `tailscale ip -4` pokaże adres `100.x.y.z`. Na komputerze utwórz w folderze `.ssh` (w katalogu użytkownika) plik tekstowy `config` bez rozszerzenia — w Notatniku „Zapisz jako", typ „Wszystkie pliki", inaczej powstanie `config.txt`, którego SSH nie czyta. Treść:

```
TEKST

Host serwer
    HostName 100.x.y.z
    User ania
```

Dopiero gdy `ssh serwer` działa w nowym oknie (odcisk serwera potwierdź jeszcze raz: `yes`), zrób punkt kontrolny: sprawdź z zewnątrz, że port 22 na publicznym adresie odpowiada (jak — w części „Testy odbioru serwera"). Potem zamknij publiczne SSH: `sudo ufw delete allow OpenSSH` i sprawdź `sudo ufw status` — na liście nie może być już OpenSSH ani 22, także z dopiskiem `(v6)`. W konsoli Tailscale wyłącz wygasanie klucza serwera (domyślnie 180 dni), inaczej po pół roku serwer wypadnie z sieci.

> ✓ **Terminal w telefonie na awarie**
>
> Zainstaluj Termius (plan Starter jest darmowy, także do użytku komercyjnego, obsługuje SSH i mosh). Dodaj host `100.x.y.z`, użytkownika `ania` i klucz wygenerowany w aplikacji. Jego część publiczną (linię `ssh-ed25519 …`) skopiuj z aplikacji i dopisz na serwerze, łącząc się z komputera: `echo 'ssh-ed25519 AAAA…' >> ~/.ssh/authorized_keys`. Mosh trzyma połączenie mimo zmiany sieci (Wi-Fi → LTE).

Jeśli nie chcesz płacić za Tailscale w firmie, możesz zostawić publiczne SSH — ale wyłącznie na klucze, z fail2ban. Remote Control i tak nie potrzebuje żadnego otwartego portu. W testach odbioru pomijasz wtedy zamknięty port 22 — dowodem jest odmowa logowania bez klucza z kroku 3.

Krok 5: Zainstaluj i zaloguj Claude Code

TERMINAL

```
curl -fsSL https://claude.ai/install.sh | bash
```

Wyloguj się (`exit`) i wejdź ponownie (`ssh serwer`), żeby system zobaczył nowy program. Sprawdź `claude --version` i `which claude` (ma pokazać `/home/ania/.local/bin/claude` — ta ścieżka wróci w kroku 7), a potem zaloguj się:

TERMINAL

```
claude auth login
```

Polecenie wyświetli link. Otwórz go na telefonie lub komputerze i zaloguj się kontem Claude z planem Pro lub Max, a kod z przeglądarki wklej w terminalu przy `Paste code here if prompted`. Nie używaj tu `claude setup-token` — taki token nie uruchomi Remote Control. Potem:

TERMINAL

```
claude doctor
mkdir -p ~/centrum && cd ~/centrum && git init
```

`claude doctor` pokaże, czy konto może używać Remote Control.

Folder `~/centrum` będzie miejscem pracy Claude. Repozytorium git sprawia, że każdą zmianę zobaczysz w aplikacji jako „diff" i cofniesz. Utwórz w nim plik zasad: `nano ~/centrum/CLAUDE.md`, wklej treść, zapisz `Ctrl+O` i Enter, wyjdź `Ctrl+X`.

```markdown
# Serwer firmy — zasady
- Pracujesz w ~/centrum. Poza nim tylko czytasz, chyba że poproszę inaczej.
- Nigdy nie wypisuj haseł, kluczy ani tokenów. Nie czytaj ~/.ssh.
- Przed usunięciem plików, wysyłką, publikacją lub zmianą firewalla — zapytaj.
- Każde zadanie kończ raportem: co zmieniłeś, gdzie, jak to sprawdzić.
```

Krok 6: Pierwsze połączenie z telefonu

```terminal
cd ~/centrum
claude remote-control --name serwer-firmy
```

Za pierwszym razem padną dwa pytania: `Trust /home/ania/centrum? [y/N]` i `Enable Remote Control? (y/n)` — oba razy `y`. Pojawi się link do sesji, a spacja pokaże kod QR. Zeskanuj go telefonem albo otwórz aplikację Claude → **Code**. Sesja „serwer-firmy" ma ikonę komputera i zieloną kropkę.

Napisz z telefonu: „Podaj wersję systemu, wolne miejsce na dysku i folder, w którym pracujesz. Nic nie zmieniaj". Porównaj odpowiedź z wynikiem `df -h /` w drugim oknie SSH — to Twój pierwszy test kontroli jakości. Zakończ `Ctrl+C`.

> **! Usługa potrzebuje własnego folderu**
>
> Usługa systemowa domyślnie startuje w katalogu głównym, a w katalogu domowym Claude Code nie zapisuje zgody na zaufanie folderu. W obu przypadkach pyta o zaufanie przy każdym starcie, a usługa bez klawiatury nie odpowie. Dlatego osobny folder `~/centrum`, raz potwierdzony ręcznie.

Krok 7: Usługa 24/7, która wstaje sama

Utwórz plik usługi: `sudo nano /etc/systemd/system/claude-rc.service`. Podmień `ania` we wszystkich pięciu miejscach, a ścieżka do `claude` ma się zgadzać z wynikiem `which claude`.

```ini
[Unit]
Description=Claude Code Remote Control
After=network-online.target
Wants=network-online.target

[Service]
Type=simple
User=ania
WorkingDirectory=/home/ania/centrum
Environment=HOME=/home/ania
Environment=PATH=/home/ania/.local/bin:/usr/local/bin:/usr/bin:/bin
Environment=TERM=xterm-256color
ExecStart=/usr/bin/script -qfc "/home/ania/.local/bin/claude remote-control --name serwer-firmy --
permission-mode default" /dev/null
Restart=always
RestartSec=5

[Install]
WantedBy=multi-user.target
```

`script` udaje terminal, bo Remote Control to program terminalowy, a usługa systemowa terminala nie ma. `Restart=always` podnosi usługę po awarii — ważne, bo przy dłuższym braku sieci (ok. 10 min) Remote Control sam się wyłącza. Uruchom:

```terminal
sudo systemctl daemon-reload
sudo systemctl enable --now claude-rc
sudo journalctl -u claude-rc -n 30 --no-pager
```

Nie uruchamiaj tego przez `tmux` z poziomu systemd — sesja tmux potrafi zniknąć, choć usługa wciąż świeci się na zielono. Do pracy w terminalu odpalaj osobne `claude` po SSH. Claude Code aktualizuje się w tle, ale nowa wersja działa dopiero po restarcie, więc raz w tygodniu, gdy nic nie pracuje, wykonaj `sudo systemctl restart claude-rc`.

Krok 8: Alarmy na telefon i kopie zapasowe

Zainstaluj na telefonie aplikację ntfy. Na serwerze utwórz tajny temat (każdy, kto go zna, czyta Twoje alarmy). W aplikacji dotknij +, wpisz temat wyświetlony przez `cat`, zostaw domyślny serwer ntfy.sh i zezwól na powiadomienia:

```terminal
mkdir -p ~/bin
openssl rand -hex 12 > ~/.ntfy-temat && chmod 600 ~/.ntfy-temat
cat ~/.ntfy-temat
nano ~/bin/alarm.sh
```

Treść skryptu `alarm.sh`:

```
TERMINAL

#!/bin/bash
curl -s -m 15 -H "Title: Serwer firmy" -H "Priority: high" -d "$1" "https://ntfy.sh/$(cat ~/.ntfy-temat)" > /dev/null
```

Potem `chmod +x ~/bin/alarm.sh` i próba: `~/bin/alarm.sh "Test alarmu"` — na telefonie powinno pojawić się powiadomienie. Serwery zwykle chodzą w czasie UTC, więc ustaw polski: `sudo timedatectl set-timezone Europe/Warsaw && sudo systemctl restart cron`. Następnie `crontab -e` (przy pierwszym razie wybierz edytor nano) i dopisz trzy linie:

```
TEKST

*/15 * * * * systemctl is-active --quiet claude-rc || ~/bin/alarm.sh "Usługa Claude nie działa"
0 8 * * * cd ~/centrum && timeout 300 ~/.local/bin/claude -p --no-session-persistence "Odpowiedz jednym słowem: OK" | grep -q OK || ~/bin/alarm.sh "Claude nie odpowiada - sprawdź logowanie i limit"
0 9 * * * [ $(df --output=pcent / | tail -1 | tr -dc 0-9) -lt 85 ] || ~/bin/alarm.sh "Dysk serwera prawie pełny"
```

Druga linia to codzienny, prawdziwy test logowania (`timeout` przerywa zawieszone wywołanie po 5 minutach). Sesja, której logowanie wygaśnie, przestaje pracować, a sama obecność pliku logowania niczego nie dowodzi. Gdy przyjdzie ten alarm: `ssh serwer` i sprawdź, czy to logowanie, czy wyczerpany limit planu. Po ponownym `claude auth login` wykonaj `sudo systemctl restart claude-rc`.

Powiadomienia od samego Claude: uruchom na serwerze `claude` w `~/centrum`, wpisz `/config` i włącz **Push when actions required** (prośby o zgodę) oraz **Push when Claude decides** (koniec zadania). Kopie zapasowe: cotygodniowe w cenie planu i ręczny snapshot w panelu przed większą zmianą. Kopia obejmuje cały dysk, razem z logowaniem Claude, więc konto u dostawcy zabezpiecz weryfikacją dwuetapową. Pracę z `~/centrum` wypychaj do prywatnego repozytorium przez token fine-grained z dostępem tylko do tego jednego repozytorium (lekcja o GitHubie, krok 8).

Krok 9: Opcjonalnie — Coolify na drugim serwerze

Coolify to darmowy (self-hosted) panel do publikowania aplikacji, stron i baz danych z repozytorium. Wymaga min. 2 rdzeni i 2 GB RAM, więc wybierz drugi KVM 2. Hostinger ma szablon „Ubuntu 24.04 with Coolify", a na czystym Ubuntu instalujesz go poleceniem z dokumentacji — dopiero po punktach 1 i 2 poniżej:

```
TERMINAL

sudo -i
curl -fsSL https://cdn.coollabs.io/coolify/install.sh | bash
```

Najważniejsze zasady, w tej kolejności:

1. **Najpierw zapora, potem instalacja.** Docker omija ufw: porty kontenerów są widoczne z internetu mimo reguł ufw. Dlatego tu użyj zapory w panelu dostawcy (w Hostingerze: Firewall w sekcji bezpieczeństwa VPS w hPanelu), która filtruje ruch, zanim dotrze do serwera. Publicznie zostaw 80 i 443 (i 22 do końca kroku 4). Porty panelu Coolify — 8000, 6001 i 6002 — zostają zamknięte dla internetu (dokumentacja portów Coolify).
2. Zrób kroki 2–4 także na tym serwerze. Dopiero potem uruchom instalator.
3. **Od razu załóż konto administratora**, otwierając panel przez Tailscale (`http://100.x.y.z:8000` — adres Tailscale tego serwera). Kto pierwszy wejdzie na stronę rejestracji, ten zostaje administratorem. Przy szablonie z gotowym Coolify panel działa od pierwszej minuty — konto załóż zaraz po utworzeniu serwera.
4. Połącz Coolify z GitHubem. Claude na serwerze-warsztacie wypycha zmiany do repozytorium, a Coolify publikuje je automatycznie.

ROZDZIAŁ 6

Jak rozpoznać, że AI zrobiło dobrą robotę

AI pomaga tu w trzech miejscach: tłumaczy polecenia i błędy podczas konfiguracji, robi audyt serwera i wykonuje pracę, którą zlecasz z telefonu. Zasada jest jedna: „gotowe" od Claude to hipoteza. Dowodem jest wynik polecenia, który widzisz sam, albo zachowanie systemu w prawdziwym teście.

Przy konfiguracji dobre wyjaśnienie od AI (prompt 1) mówi, jak cofnąć zmianę i jaki wynik zobaczysz, gdy się uda. Jeśli po wklejeniu widzisz coś innego, zatrzymaj się. Nie wklejaj kolejnych „poprawek" na ślepo — wróć do ostatniego działającego stanu.

Testy odbioru serwera



Test	Jak	Dobry wynik
Restart	`sudo reboot`, odczekaj 2 min	sesja wraca z zieloną kropką; po 10 min `systemctl show claude-rc -p NRestarts` daje `NRestarts=0`
Telefon poza siecią	wyłącz komputer i Wi-Fi, pisz z danych komórkowych	Claude odpowiada i wykonuje zadanie
Drzwi zamknięte	test portu 22 z niezależnego miejsca przed i po zamknięciu	przed: otwarty (punkt kontrolny), po: brak odpowiedzi, przez Tailscale: działa
Logowanie	`sudo sshd -T` i próba `ssh -o PubkeyAuthentication=no`	`no` przy roocie i hasłach; próba kończy się `Permission denied`
Alarm	`sudo systemctl stop claude-rc`, odczekaj 15 min	powiadomienie w ntfy; potem `start`
Zgoda	poproś z telefonu o usunięcie pliku testowego	Claude prosi o zgodę, przychodzi push

Test portu wymaga punktu kontrolnego. Brak odpowiedzi wygląda tak samo, gdy port jest zablokowany i gdy test po prostu nie dochodzi do serwera. Dlatego sprawdź port, zanim go zamkniesz — tym samym narzędziem (np. Termius na danych komórkowych z wyłączonym Tailscale albo internetowy sprawdzacz portów). Jeśli przed zmianą test widział otwarty port, a po zmianie nie widzi — masz dowód.

Gdy Claude robi audyt swojego serwera

Użyj promptu audytu z Zestawu. Dobry raport ma przy każdym wniosku polecenie i fragment wyniku. Dwa wybrane polecenia uruchom sam i porównaj. Jeśli wyniki się różnią, raport traci wiarygodność w całości, nie tylko w jednym punkcie.

Sygnały ostrzegawcze: „wszystko jest bezpieczne" bez dowodów; propozycja wyłączenia firewalla „na chwilę"; `chmod 777`; `--dangerously-skip-permissions`; wklejanie skryptów z nieznanych stron; prośba o hasło w czacie; zmiany wprowadzone bez pytania.

Gdy zlecasz pracę z telefonu

Wpisz kryteria odbioru w samo polecenie. Sprawdź diff w aplikacji (dlatego `~/centrum` jest repozytorium git). Oceniaj efekt, nie raport: otwórz plik, przelicz jedną sumę, kliknij link.

✓ Odbiór serwera

- [ ] `sudo sshd -T` pokazuje `permitrootlogin no` i `passwordauthentication no`
- [ ] Port 22 z internetu nie odpowiada, a test kontrolny przed zmianą go widział (wariant z Tailscale)
- [ ] `ssh serwer` przez Tailscale działa, konsola awaryjna w panelu też
- [ ] Po `sudo reboot` sesja sama wraca w aplikacji, `NRestarts=0`
- [ ] Zadanie z telefonu wykonane przy wyłączonym komputerze i sprawdzone w diffie
- [ ] Testowy alarm dotarł, codzienny test logowania jest w crontabie
- [ ] Claude pyta o zgodę przed usunięciem pliku
- [ ] Data odnowienia VPS jest w kalendarzu

ROZDZIAŁ 7

Bezpieczeństwo i RODO

- **Kanał Remote Control** to wyłącznie połączenia wychodzące, szyfrowane TLS. W czasie połączenia zapis rozmowy jest przechowywany na serwerach Anthropic, żeby synchronizować urządzenia. Polecenia wykonują się na Twoim serwerze i tam leżą pliki, ale wszystko, co Claude przeczyta (treść plików, wyniki poleceń), trafia do Anthropic jako część rozmowy — centrum danych w UE tego nie zmienia.
- **Dane w planach Pro i Max:** w ustawieniach prywatności (claude.ai/settings/data-privacy-controls) sam decydujesz, czy rozmowy mogą trenować modele. Gdy nie — retencja wynosi 30 dni. To plany konsumenckie, bez umowy powierzenia, więc nie dawaj na nich Claude danych osobowych klientów. Plany Team i Enterprise działają na warunkach komercyjnych (z umową powierzenia, DPA), bez trenowania na Twoich danych — do takiej pracy wybierz jeden z nich i uzgodnij to z osobą od RODO.
- **Serwer w UE** — wybierz centrum danych w Unii i sprawdź umowę powierzenia u dostawcy.
- **Sekrety** trzymaj w Bitwardenie, nie w czacie — także hasło do `sudo`, bo wszystko, co wpiszesz, trafia do zapisu rozmowy. Dodaj w `~/.claude/settings.json` reguły blokujące odczyt kluczy i pliku logowania Claude. Gdy pliku nie ma, utwórz go z treścią poniżej; gdy jest, dopisz te wpisy do listy `deny` i pilnuj przecinków (błąd w pliku pokaże `claude doctor`). To pasek bezpieczeństwa, nie sejf — nie zatrzyma każdego programu uruchomionego przez agenta.

```JSON
{ "permissions": { "deny": ["Read(~/.ssh/**)", "Edit(~/.ssh/**)", "Read(~/.ntfy-temat)",
"Read(~/.claude/.credentials.json)"] } }
```

- **Zaufane urządzenia:** w planach Pro i Max możesz włączyć „Require trusted devices” — sterowanie sesją wymaga wtedy zarejestrowanego urządzenia i potwierdzenia biometrią (funkcja w wersji beta).
- **Prompt injection:** agent czytający maile lub strony może trafić na ukryte polecenia. Dlatego nic nie wysyła ani nie publikuje bez Twojej zgody (lekcja o MCP i uprawnieniach).

To nie jest porada prawna — przy danych osobowych skonsultuj umowy powierzenia z prawnikiem.

ROZDZIAŁ 8

Jak to robię u siebie

Mój serwer to Hostinger KVM 8 (8 vCPU, 32 GB RAM) z czystym Ubuntu 24.04. Jest większy, niż potrzebujesz na start, bo obok Claude Code działają u mnie inne narzędzia i agenci, w tym Codex i Grok jako drugie opinie (lekcja o radzie doradczej AI). SSH działa tylko przez Tailscale. Claude Code na planie Max chodzi jako usługa systemd, a w aplikacji Claude na telefonie mam zakładkę Code z sesją serwera.

Produkcja dla klientów (mój system do stron) działa na osobnym serwerze z Coolify, więc awaria serwera z Claude nie kładzie żadnej strony klienta. Co noc idzie szyfrowana kopia zapasowa, a rano health-check wysyła mi raport przez ntfy. Ten raport zawiera realny test, czy narzędzia AI są zalogowane. Dodałem go, gdy sesja jednego z narzędzi wygasła po ok. trzech tygodniach, choć plik logowania wciąż leżał na dysku.

Serwer nie zastąpił mi komputera: na co dzień pracuję lokalnie, a serwer przejmuje zadania 24/7 i pracę z telefonu. Pamiętaj, że wspólnym limitem jest plan Claude — sesje z komputera i serwera korzystają z tych samych limitów. Większość błędów poniżej to moje realne potknięcia z tego wdrożenia.

ROZDZIAŁ 9

Najczęstsze błędy

1. **Usługa bez właściwego folderu roboczego.** Skutek: systemd startuje program w katalogu głównym (albo w domowym, gdzie zaufanie nie jest zapisywane), Claude zgłasza „Workspace not trusted" i usługa kręci się w pętli restartów. Jak uniknąć: `WorkingDirectory` z osobnym folderem (`~/centrum`), raz potwierdzonym ręcznie.
2. **tmux uruchamiany przez systemd.** Skutek: sesja znika, a status wciąż mówi `active`. Jak uniknąć: `Type=simple` i `script -qfc`, a weryfikacja przez prawdziwy restart i połączenie z telefonu.
3. **Wyłączenie haseł tylko w głównym pliku SSH.** Skutek: plik z obrazu serwera wciąż pozwala logować się hasłem. Jak uniknąć: plik `00-utwardzenie.conf` i kontrola `sshd -T`.
4. **Zaufanie do ufw na serwerze z Dockerem.** Skutek: port kontenera widoczny z internetu. Jak uniknąć: zapora dostawcy przed serwerem i test z zewnątrz po każdej zmianie.
5. **Test portu bez punktu kontrolnego.** Skutek: fałszywe poczucie bezpieczeństwa. Jak uniknąć: ten sam test przed zmianą i po niej, z niezależnego miejsca.
6. **Zamknięcie publicznego SSH przed sprawdzeniem Tailscale.** Skutek: odcięcie od serwera. Jak uniknąć: najpierw `ssh serwer` w nowym oknie, a konsola awaryjna w panelu sprawdzona zawczasu.
7. **Tryb pomijania uprawnień „dla wygody".** Skutek: agent z dostępem do internetu i danych firmy robi wszystko bez pytania. Jak uniknąć: tryb domyślny z powiadomieniami. Gdy nabierzesz zaufania, `acceptEdits` — edytuje i usuwa pliki w `~/centrum` bez pytania, więc regularnie zapisuj stan w git, żeby każdą zmianę dało się cofnąć.
8. **Zapomniane daty.** Skutek: wyższa cena odnowienia VPS albo serwer wypadający z Tailscale po 180 dniach. Jak uniknąć: przypomnienie w kalendarzu i wyłączone wygasanie klucza serwera.

ROZDZIAŁ 10

Zestaw do powtórzenia

Prompt 1 — wyjaśnij, zanim wkleję (w aplikacji Claude lub w przeglądarce):

› PROMPT

```
Jesteś administratorem Linuksa i tłumaczysz osobie nietechnicznej.
Zanim wkleję poniższe polecenie na serwer z Ubuntu 24.04, wyjaśnij:
1. Co robi każda linia — prostymi słowami.
2. Co może pójść nie tak (np. odcięcie mnie od serwera) i jak się zabezpieczyć.
3. Jak cofnąć zmianę.
4. Jak sprawdzić, że zadziałało — podaj polecenie i oczekiwany wynik.
Jeśli czegoś nie jesteś pewien, napisz to wprost. Nie proponuj innych zmian.

Polecenie:
[WKLEJ POLECENIE]
```

Prompt 2 — audyt serwera tylko do odczytu (w sesji na serwerze, także z telefonu):

› PROMPT

```
Zrób audyt bezpieczeństwa tego serwera. Tryb: TYLKO ODCZYT — niczego nie zmieniaj, nie instaluj i nie restartuj.
Sprawdź: skuteczną konfigurację SSH (sshd -T), reguły ufw, nasłuchujące porty (ss -tulpn), fail2ban, automatyczne aktualizacje, użytkowników z sudo, porty publikowane przez Dockera (jeśli jest) i status usługi claude-rc.
Wynik podaj w tabeli: obszar | polecenie | fragment wyniku | ocena (OK / do poprawy) | proponowana poprawka.
Nie pisz „bezpieczne” bez dowodu z wyniku polecenia. Na końcu wypisz 3 najważniejsze poprawki według ryzyka i zapytaj, czy je wdrożyć.
```

Prompt 3 — zlecenie z telefonu z kryteriami odbioru:

› PROMPT

```
Zadanie: [CO MA POWSTAĆ, np. zestawienie ofert z folderu oferty/ w jednej tabeli].
Kontekst: [DLA KOGO, PO CO, SKĄD DANE].
Kryteria odbioru: [np. każda oferta ma kwotę netto i brutto; suma zgadza się z plikami; żadna oferta nie została pominięta].
Ograniczenia: pracuj tylko w folderze [FOLDER]; nic nie wysyłaj i nie publikuj; zapytaj przed usunięciem czegokolwiek.
Na koniec: lista zmienionych plików, jak sprawdziłeś każde kryterium i czego nie udało się sprawdzić.
```

Prompt 4 — diagnoza, gdy usługa nie wstaje:

› PROMPT

```
Usługa claude-rc na Ubuntu 24.04 nie działa po restarcie. Poniżej wynik poleceń systemctl status
claude-rc i sudo journalctl -u claude-rc -n 50.
Podaj 3 najbardziej prawdopodobne przyczyny, od najbardziej prawdopodobnej. Dla każdej: polecenie,
które ją potwierdzi lub wykluczy, i bezpieczną poprawkę.
Uwzględnij typowe pułapki: folder roboczy bez zaufania, wygasłe logowanie Claude, zła ścieżka do
programu, brak sieci przy starcie.
Nie zgaduj — jeśli danych jest za mało, napisz, czego jeszcze potrzebujesz.

[WKLEJ WYNIK]
```

Karta serwera (wypełnij i trzymaj w notatkach — bez haseł):

Pole	Twoja wartość
Dostawca, plan, centrum danych	
Koniec okresu i cena odnowienia	
System i użytkownik roboczy	
Gdzie są klucze i hasła	Bitwarden: nazwa wpisu
Folder roboczy i nazwa sesji	~/centrum, serwer-firmy
Kanał alarmów	ntfy (temat w Bitwardenie)
Ostatni test restartu i kopii	

Przegląd raz w miesiącu:

- [ ] Restart usługi (wejdzie nowa wersja Claude Code) i sesja wraca w aplikacji
- [ ] Testowy alarm dociera na telefon
- [ ] `sudo fail2ban-client status sshd` i `sudo ufw status` bez niespodzianek
- [ ] Przegląd urządzeń w Tailscale i zaufanych urządzeń w Claude — usuń nieużywane
- [ ] Prompt audytu uruchomiony, dwa wyniki sprawdzone ręcznie
- [ ] Test odtworzenia: sklonuj repozytorium z pracą na innym komputerze
- [ ] Data odnowienia VPS wciąż w kalendarzu

ROZDZIAŁ 11

Twój plan działania

- **Dziś (ok. 90 min):** kroki 1–4. Kończysz z serwerem zamkniętym na klucze i dostępnym przez Tailscale.
- **W tym tygodniu:** kroki 5–8 i wszystkie testy z checklisty odbioru. Zleć z telefonu trzy małe zadania z kryteriami odbioru (prompt 3) i sprawdź każde w diffie.
- **W tym miesiącu:** dopracuj `CLAUDE.md` na podstawie tego, co poszło nie tak, zrób pierwszy przegląd miesięczny i zdecyduj, czy potrzebujesz Coolify do publikowania aplikacji.

ROZDZIAŁ 12

Słowniczek

- **VPS** — wynajęty serwer wirtualny w centrum danych, działający całą dobę.
- **Ubuntu LTS** — wersja Linuksa z długim, 5-letnim wsparciem poprawkami bezpieczeństwa.
- **SSH** — szyfrowane połączenie, którym wydajesz polecenia serwerowi z daleka.
- **Klucz SSH** — para plików zamiast hasła: publiczna „kłódka" na serwerze, prywatny „klucz" u Ciebie.
- **Firewall (ufw)** — bramkarz, który wpuszcza ruch tylko na wskazane porty.
- **fail2ban** — program, który blokuje adresy po serii nieudanych logowań.
- **Tailscale** — prywatna sieć łącząca Twoje urządzenia, niewidoczna z internetu.
- **Remote Control** — funkcja Claude Code, która pozwala sterować sesją z telefonu lub przeglądarki.
- **Usługa systemd** — program uruchamiany przez system automatycznie, także po restarcie i awarii.
- **Docker** — „kontenery", czyli zamknięte pudełka z aplikacjami. Uwaga: omija ufw.
- **Coolify** — darmowy panel do publikowania aplikacji i stron z repozytorium na własnym serwerze.
- **mosh** — połączenie terminalowe, które przetrwa zmianę sieci w telefonie.

ROZDZIAŁ 13

Źródła

- Claude Code — Remote Control — działanie, wymagania, tryb serwera, ograniczenia
- Claude Code — instalacja — instalator i wymagania (Ubuntu 20.04+, 4 GB RAM)
- Claude Code — logowanie — logowanie przez SSH, ograniczenia setup-token
- Claude Code — wykorzystanie danych — trenowanie i retencja danych według planu
- Claude — cennik — plany Pro, Max i Team
- Hostinger — VPS — plany KVM, ceny i odnowienia
- iMagazine — polskie ceny Maca mini — Mac mini M6 od 4 499 zł
- Tailscale — serwer Ubuntu za UFW — zamknięcie SSH dla internetu
- Tailscale — FAQ cennika — Personal tylko niekomercyjnie, plany dla firm
- Coolify — instalacja — wymagania, instalacja, konto administratora
- Docker — zapory i ufw — dlaczego porty kontenerów omijają ufw
- Termius — cennik — darmowy Starter z SSH i mosh

Co dalej

NASTĘPNA LEKCJA · 20 z 21

Zbudowałem stronę z AI — dlaczego nie widzę jej w Google?

Zdiagnozujesz swoją stronę, podłączysz ją do Google Search Console i zgłosisz ją do indeksowania.

Obejrzyj wideo

Kanał BudujemyAI na YouTube

Dołącz do Klubu BudujemyAI

Pytania, Kawa z AI co tydzień i live konsultacyjny.

klub.budujemyai.pl

Konsultacja hybrydowa

Dwa spotkania online i e-book PDF z rozwiązaniami dla Twojej firmy — 499 zł. Na start: bezpłatne 15 min.

wiedza.budujemyai.pl/konsultacja/

Pozostałe e-booki — za darmo

21 lekcji ścieżki „Jedna praca" i mapa wiedzy.

wiedza.budujemyai.pl/ebooki/

ANKIETA · 1 MINUTA

Jak mógłbym dodatkowo rozwinąć według Ciebie ten wątek, bądź co jeszcze Cię ciekawi w tym temacie?

Odpowiedz tutaj: wiedza.budujemyai.pl/baza-wiedzy/claude-code-z-telefonu/#ankieta — czytam każdą odpowiedź, a najczęstsze prośby zamieniam w kolejne lekcje.

O autorze



Daniel Baranowski — prowadzi BudujemyAI. Wdraża AI i automatyzacje w małych i średnich firmach, buduje strony www z pomocą AI (także 3D) na własnym systemie, w którym klient sam edytuje stronę, pisząc do AI po polsku.

Na co dzień pracuje z Claude Code, Codexem i Grokiem jako „radą doradczą", a całą firmę prowadzi z vaulta w Obsidianie. W tej bazie pokazuje dokładnie to, czego sam używa — prosto i konkretnie.

ai@baranowski.consulting · budujemyai.pl · wiedza.budujemyai.pl

© 2026 BudujemyAI · Daniel Baranowski. Wydanie: listopad 2026. Możesz przesłać ten e-book dalej w niezmienionej formie.

Ceny, nazwy planów i funkcje narzędzi AI zmieniają się często — przed decyzją zakupową sprawdź aktualne informacje u producenta. Treść ma charakter edukacyjny i nie jest poradą prawną ani podatkową.