Zabezpieczenia do wdrożenia później

Zabezpieczenia do wdrożenia później

Decyzja użytkownika z 16.11: najpierw ma działać, zabezpieczenia po uruchomieniu całości. Ta lista jest przypomnieniem.

J-Tools i kanał hub → strona

- ☐ HMAC z czasem i treścią zamiast stałego klucza w nagłówku.
- ☐ Osobny klucz dla każdej strony, rotacja (lista dwóch kluczy), przechowywanie tylko w sejfie i na hubie.
- ☐ Lista IP huba i limit żądań na klucz.
- ☐ Podpis paczek z huba albo ograniczenie źródeł paczek.
- ☐ Podpis kokpitu albo drugi klucz dla zadań poziomu C (publikacja).
- ☐ Dziennik kanału wysyłany poza stronę.
- ☐ Przegląd Ochrony nowych zadań przed wydaniem na produkcję.

Hub i kokpit

- ☐ API kokpitu (port 8090) odpowiada bez klucza z całej sieci WireGuard 10.30.8.0/24. Dodać klucz.
- ☐ CT162 (agenci OpenBot) ma dostęp do kokpitu na porcie 8080, więc agent mógłby technicznie zatwierdzić kartę. Zawęzić do API.

☐ Kokpit nie ma własnego logowania, chroni go tylko Cloudflare Access.

☐ Hasło główne Vaultwarden leży w sejfie OpenBot. Rozważyć zmianę po zakończeniu prac.

☐ WGDashboard na slonce może nadpisać ręcznie dodany wpis klienta WireGuard (gate). Wyłączyć zapis z przeglądarki albo dodać wpis przez narzędzie.

Nadzór (mars)

☐ agent-nadzor (CT206): trzy agenty AI w jednym kontenerze, oddzielone użytkownikami i `BindPaths`. Izolacja jest słabsza niż przy osobnych kontenerach. Rozważyć osobne kontenery lub dodatkowe ograniczenia (np. `PrivateNetwork` per usługa z własnym wg0), jeśli ryzyko będzie nie do zaakceptowania.

☐ Klucze SSH agentów na hostach mają ograniczenie `from=` do adresu. Zmiana adresów agentów wymaga zmian na 7 hostach i w Wazuh.

Kopie i dane

☐ Kopie lokalne J-Tools leżą na tym samym koncie hostingu co strona.

☐ Kopia gminadobre (CT305): w katalogu WWW leży kopia `wp-config.php.przed-zadania-20261023` (prawa 640, właściciel www-data), którą Apache serwuje jako zwykły plik (HTTP 200 lokalnie, z internetu za Cloudflare Access). Zawiera dane dostępowe. Przenieść poza katalog WWW. Pozostałe kopie wp-config (np. `wp-config-przed-kluczB-*`, `wp-config.php.przed-klucz-huba`) są w `/root` kontenera, nie w katalogu WWW (sprawdzone 16.11 wieczorem; wcześniejszy zapis o katalogu WWW był błędny).

☐ Dane zgłoszeń zawierają dane osobowe: umowa powierzenia z gminami jest podpisana, pseudonimizacja do zrobienia.

Sekrety: gdzie leżą (audyt 16.11.2026 wieczorem)

Zasada: wartość działa tam, gdzie jest potrzebna (plik na hubie, wp-config, agent.env), a kopia zapasowa jest w Vaultwarden (sejf.grws.pl). W Vaultwarden są (9 pozycji): klucz Anthropic huba, token Cloudflare, klucz kanału J-Tools dla kopii gminadobre, hasło aplikacji hubredaktor, token BookStack, klucz REST Gravity Forms (kopia), konto bazy wpisy_czyt, token Proxmox agent-hub@pve!ro oraz pozycja testowa.

☐ **Poza Vaultwarden z założenia:** klucz API i hasło główne Vaultwarden (BW_CLIENTID, BW_CLIENTSECRET, BW_PASSWORD) są tylko w sejfie OpenBot. Hasło główne znasz Ty. Rozważyć jego zmianę po zakończeniu prac.

☐ **Klucze prywatne WireGuard** (hub CT163, gate CT200, agent-nadzor CT206): tylko na swoich kontenerach (nie kopiować). Po utracie kontenera trzeba wygenerować nowe i dodać klientów na slonce.

☐ **Sekrety systemu nadzoru na mars** (klucze Anthropic w agent.env agentów pve, backup i sec, tokeny gate, tokeny Proxmox i PBS, klucze SSH, dane Wazuh): leżą tylko w plikach w /etc/agent- (CT206) i CT200. Nie przeniesione do Vaultwarden, bo to osobny system z własnym modelem uprawnień. Ocenić, czy zapisać kopie.

☐ **Hasła aplikacji innych kont, token tunelu Cloudflare na CT134, hasła baz WordPress** na kopii i w formularzach: tylko w plikach konfiguracyjnych. Dopisać do Vaultwarden przy najbliższej zmianie.

☐ **Kopie `wp-config*` w /root kontenera CT305** (11 plików, w tym ze starym kluczem kanału i danymi bazy): to kopie zapasowe, nie miejsce robocze. Usunąć po zakończeniu testów.

☐ **Hasła SSH kont ug*** na dhostingu zostały wypisane 28.10 w transkrypcie i nie zostały zmienione.

Revision #4
Created 2026-11-16 16:37:30 UTC by Claude (dokumentacja)
Updated 2026-11-16 20:07:09 UTC by Claude (dokumentacja)