SCIĄGA LARAVEL · SECURITY

Jak nie dać się zhakować: checklista na kwartał

dominik-dev.pl
pełny artykuł →

Serwer i sieć, aplikacja, CI/CD, dane, wykrywanie, pierwsze 72 godziny

TL;DR: kolejność, która zwraca się najszybciej

1	2	3	4	5	6
Skan z zewnątrz, zamknij wszystko poza 80/443	SSH tylko z kluczy, przez VPN	APP_DEBUG=false, root na public/, composer audit	Policies + testy 403 na każdym ID	Backup 3-2-1, test odtworzenia	Centralne logi, diff portów, alerty

DOCKER `ports: "6379:6379"` publikuje port na wszystkich interfejsach, a reguły iptables Dockera działają **przed UFW**. `ufw status` kłamie; prawdę mówi tylko `nmap -p-` z zewnątrz. Używaj `127.0.0.1:6379:6379` albo brak `ports` i sieć z `internal: true`.

SERWER I SIEĆ

- ☐ `nmap -Pn -p-` z zewnątrz pokazuje tylko 80 i 443
- ☐ Firewall domyślnie blokuje ruch przychodzący, także w panelu chmury
- ☐ Żaden `ports:` w Compose nie wystawia bazy, Redisa ani panelu na `0.0.0.0`
- ☐ SSH tylko z kluczy, root wyłączony, dostęp przez VPN lub bastion
- ☐ Automatyczne poprawki bezpieczeństwa, obrazy przebudowane w tym miesiącu
- ☐ phpMyAdmin, Horizon, Telescope, Grafana niepubliczne

APLIKACJA

- ☐ `APP_ENV=production`, `APP_DEBUG=false`
- ☐ Root na `public/`; `/.env`, `/.git/` zwracają 404
- ☐ Każdy endpoint z ID: Policy + test 403 dla obcego użytkownika
- ☐ Zapis tylko z `validated()`; modele mają `$fillable`
- ☐ Brak `whereRaw` / `DB::raw` z niezbindowanymi danymi
- ☐ Throttle na logowaniu, resecie, rejestracji, 2FA, API
- ☐ Uploady walidowane, dysk prywatny, bez wykonywania PHP
- ☐ HSTS, CSP, `nosniff`, `frame-ancestors`
- ☐ Cookies sesji `Secure`, `HttpOnly`, `SameSite`

CI/CD I ZALEŻNOŚCI

- ☐ `composer audit` + `npm audit` w każdym PR
- ☐ Dependabot lub Renovate włączony
- ☐ Skaner sekretów (gitleaks) blokuje commity z kluczami
- ☐ Pipeline blokuje deploy z `APP_DEBUG=true`

DANE I BACKUPY

- ☐ Kopie 3-2-1, jedna niezmienialna lub offline
- ☐ Pełne odtworzenie przetestowane w ostatnim kwartale
- ☐ Wrażliwe pola szyfrowane w bazie (cast `encrypted`)
- ☐ Lista sekretów i procedura rotacji spisane

WYKRYWANIE

- ☐ Logi aplikacji, serwera WWW i systemu w jednym miejscu
- ☐ Alerty: nieudane logowania, próby `/.env`, SSH spoza VPN, nowy port, skok ruchu wychodzącego
- ☐ Codzienny diff portów z zewnątrz względem wzorca
- ☐ Kontrola integralności plików (Wazuh / AIDE)

Codzienny diff portów (uruchamiany spoza sieci)

```
current="$(nmap -Pn -p- --min-rate 1000 -oG - "$host" | grep -oE '[0-9]+/open' | sort -u)"
baseline="$(cat ~/port-diff/$host.baseline)"
[[ "$current" == "$baseline" ]] || echo "$current" | mail -s "port-diff: $host" ops@example.com
```

Incydent: pierwsze 72 godziny

1. **Nie kasuj:** snapshot dysku, zachowaj logi. **Odizoluj** maszynę, nie wyłączaj jej, jeśli się da.
2. **Zamknij wejście**, potem **wymień wszystkie sekrety**: baza, klucze API, `APP_KEY`, tokeny CI, klucze SSH.
3. **Postaw serwer z czystego obrazu**, dane z kopii sprzed ataku. Oceń, co wyciekło, czyje i od kiedy.
4. **Zgłoś** (termin biegnie od chwili, gdy się dowiedziałeś), poinformuj użytkowników, napisz post-mortem bez szukania winnych.

Regulacja	Komu	Termin
RODO: dane osobowe z ryzykiem dla osób	Prezes UODO (+ osoby, gdy ryzyko wysokie)	72 h
NIS2 / KSC: podmiot kluczowy lub ważny, poważny incydent	CSIRT	24 h ostrzeżenie · 72 h zgłoszenie · miesiąc raport końcowy