# Technické informace a zabezpečení

Systém běží na serveru ve vaší firmě a data zůstávají u vás. Jak chrání přístup a data, jak se zálohuje a aktualizuje – a co zatím neumí. Stav k 19. 11. 2026.

## Zabezpečení

| OBLAST | JAK TO FACTORYPULSE ŘEŠÍ |
|---|---|
| **Přihlášení** | Hesla jen jako nevratný otisk (bcrypt, každé s vlastní solí); chybné přihlášení neprozradí, zda jméno existuje. 5 chybných pokusů na účet nebo 20 z jednoho počítače za 15 minut zamkne přihlášení na 15 minut. Přihlášení platí nejvýš 12 hodin; cookie nepřečte skript stránky (HttpOnly), zneužití z cizího webu omezuje SameSite a přes HTTPS se nepošle nešifrovaně (Secure). Odhlášení ho zruší i na serveru. Vyřazením zaměstnance se vypne i jeho účet. Volitelně dvoufázové přihlášení kódem z mobilu. |
| **Práva podle lidí** | Každá oblast i její záložky mají samostatné právo na čtení a na zápis. Role jsou jen výchozí šablony – správce každému přidá nebo odebere práva výjimkou. **Práva hlídá server:** bez práva uživatel data nedostane ani přímým dotazem (soulad nabídky a serveru hlídá automatický test). Role jen pro čtení (Vedení) nic nemění, správce má vždy vše. Plánek a sklad lze omezit po halách. Firmy jedné skupiny mají data oddělená. |
| **Citlivé údaje** | Ve sdílených seznamech (díly, materiály, zákazníci, zaměstnanci) vidí citlivé údaje jen ten, komu je správce dá: ceny materiálu a obalů a náklad na kus, hodnotu zásob v penězích, kontakty zákazníků, parametry receptur – vaše know-how (kontrolu receptury proti stroji počítá server a vrací jen výsledek) a osobní údaje zaměstnanců (jinde jen jméno a hala). |
| **Auditní stopa** | Kdo, kdy a co změnil (pole, původní a nová hodnota) v recepturách, zakázkách, kvalitě, skladu, obchodu, směnách, účtech, právech i zařízeních; hledání podle člověka, období a záznamu. Zůstane i po vyřazení účtu. Data ze strojů a skladové pohyby mají vlastní historii s časem. |
| **Zařízení u strojů** | Každý box a panel má vlastní přihlašovací údaje ze zavedení; server drží jen jejich nečitelný otisk a přístup jde kdykoli odebrat. Box zapisuje jen za svůj stroj, ani se zneužitými údaji ne za jiný. Panel přijme zápis jen s průkazem svého pracoviště, pracoviště bez panelu jen od přihlášeného s právem obsluhy. |
| **Šifrování** | Doporučujeme šifrované spojení (HTTPS) i ve vaší síti: reverzní proxy Caddy na serveru s certifikátem vaší firmy, nebo s vlastní certifikační autoritou; nešifrované spojení se přesměruje. Panel mimo síť serveru umí HTTPS s ověřením certifikátu. **Pobočky** přes VPN (WireGuard). **Podporu** zapíná váš správce nejvýš na 24 h – server se sám spojí ven tunelem SSH na ověřený servisní bod dodavatele, dovnitř se nic neotevírá. |
| **Ochrana aplikace** | Dotazy do databáze jen parametrizované (ochrana proti SQL injection), ochranné hlavičky (stránku nejde vložit do cizího webu), strop velikosti požadavků a souborů proti přetížení serveru. Kódy nejdou zdvojit podobnými znaky; souběžnou změnu téhož záznamu nikdo nepřepíše bez upozornění. |

## Infrastruktura

| ČÁST | CO DĚLÁ A JAK SE PŘIPOJUJE |
|---|---|
| **Server** | Webová aplikace (dva procesy), databáze PostgreSQL a zprostředkovatel zpráv boxů (MQTT); Linux, databáze a zprostředkovatel jako kontejnery (Docker). Běží i na Raspberry Pi 5; pro víc strojů a léta dat doporučujeme vlastní server, fyzický nebo virtuální. |
| **Panel pracoviště** | Dotykový displej: potvrzení kusů a beden, zmetky s vadou, balení, měření podle plánu; česky, anglicky, ukrajinsky a německy. Wi-Fi; bez spojení data uloží a odešle později. U ručních pracovišť i tablet. |
| **Modul stavu stroje** | Doplněk panelu: oddělené vstupy 24 V na RS-485 panelu – cykly, poruchy a nečinnost bez zásahu do řízení stroje. Dřív samostatný box (Wi-Fi, MQTT). |
| **Prohlížeče, kiosek** | Uživatelé v prohlížeči na počítači, tabletu i telefonu, česky, anglicky nebo německy. Kiosek na hale je bez přihlášení a ukazuje jen to, co správce zapne: směny lidí haly (jméno, osobní číslo), poruchy strojů, reklamace a blokace dílů (bez zákazníků), nové díly, oznámení – patří jen tam, kam chodí zaměstnanci haly. |

**Síť a porty** – doporučené nastavení s HTTPS; pro provoz internet potřeba není

| PORT | KDO SE PŘIPOJUJE | K ČEMU |
|---|---|---|
| **443, 80 TCP** | prohlížeče uživatelů, kiosky | aplikace šifrovaně (HTTPS přes Caddy); 80 jen přesměruje |
| **8001 TCP** | panely u strojů | aplikace; na firewallu serveru povolit jen ze sítě strojů |
| **1883 TCP** | boxy u strojů | zprávy boxů (MQTT), vlastní účet každého boxu; jen ze sítě strojů |
| **51820 UDP** | pobočky | šifrovaná VPN (WireGuard), jen když ji používáte; port lze změnit |
| **9100, 631 TCP** | server → tiskárny v síti | štítky, doklady A4, stav; hledání tiskáren (SNMP, 161 UDP) na pokyn |
| **ven, volitelně** | server, panely | aktualizace, čas panelů, podpora (443 TCP, jen zapnutá), stav licence (tektavo.com 443 TCP, denně, po objednávce hodinově, lze vypnout); instalace: prohlížeč pro tisk (googlechromelabs.github.io, storage.googleapis.com). |

## Data a zálohy

- **Denní záloha** databáze i souborů ve 3:15 (nebo hned po spuštění serveru) na 30 dní; **měsíční archiv** se nemaže nikdy.
- **Řízená dokumentace** jako PDF ve složce jen pro aplikaci, s otiskem SHA-256.
- **Externí cíl** (externí disk nebo síťová složka) se připojí podle postupu z aplikace; každá záloha se tam zkopíruje sama. Bez něj zálohy nechrání proti ztrátě celého serveru.
- Aplikace ukazuje poslední zálohu, kopii na externí cíl a archivy.
- **Obnova:** postup k vybrané záloze vypíše aplikace; jeden příkaz na serveru vrátí databázi, přílohy, archiv i účty boxů (i na novém serveru).
- **Krok zpět:** smazané zařízení, forma, díl, pozice či zaměstnanec se jen vyřadí, historie zůstane; výrobní záznamy ani záznamy kvality aplikace nemaže.
- **Data nejsou uzamčená u dodavatele:** běžná databáze PostgreSQL na vašem serveru, čitelná standardními nástroji; hlavní seznamy stáhnete do tabulky pro Excel (CSV).

## Aktualizace a podpora

- **Postup:** čerstvá záloha → zkouška nové verze na kopii vašich dat → aktualizace → kontrola → při chybě návrat verze, dat i souborů. Způsob a četnost domluvíme při zavedení.
- **Aktualizace jen přidávají.** Vaše role, práva lidí, výjimky, nastavení ani záznamy nemění; role se nevracejí do výchozí podoby.
- Program panelů a boxů přichází s aktualizací; do zařízení ho nahrajete z aplikace přes USB kabel.
- **Licence:** na přesný počet pracovišť, vyřazené se nepočítá; objednáte ji přímo v aplikaci (převod s QR) a po platbě se stáhne sama (posílá se jen ID instalace, firma, číslo licence, počet a verze). 30 dní před koncem upozornění, po konci 30 dní lhůta, pak jen pro čtení – data i záznamy ze strojů zůstávají. Licenční podmínky na tektavo.com.
- **Podpora:** problém nahlásíte dohodnutým kanálem (e-mail, telefon). Garantované reakční doby nejsou obecným slibem – sjednají se ve smlouvě.
- **Ověřování změn:** přes 2 300 automatických testů při každé změně, průchod všemi stránkami pod každou rolí, kontroly bezpečnosti kódu; boxy a panely se na hardwaru ověřují ručně.

## Výkon v číslech

Zátěžový test v listopadu 2026 se skladbou běžné vstřikovny: 25 strojů posílajících data, 15 panelů (každý se ptá serveru po 4 s), obrazovky Hala, Běžící výroba a Kvalita, 40 otevřených oken se zprávami a otevření stránky každou 1,5 s pod různými rolemi. Data za **rok provozu**: 9 000 zakázek, 131 000 kontrolních záznamů, 185 000 beden, 157 000 skladových pohybů, 484 000 cyklů strojů. Měřicí server: notebook s procesorem Intel Core i5-10210U (4 jádra, 8 vláken, takt 1,6 GHz, pod zátěží až 4,2 GHz; úsporný procesor 15 W), dva procesy aplikace, měřeno 5. 11. 2026.

| SITUACE (ROK DAT) | POLOVINA STRÁNEK DO | 95 % STRÁNEK DO | VYTÍŽENÍ PROCESORU |
|---|---|---|---|
| zápis každých 15 s – kusy počítají stroje samy | **0,66 s** | **2,1 s** | **1,0 jádra** |
| zápis každé 2 s – 15 ručních pracovišť potvrzuje každý kus | **2,2 s** | **6,4 s** | **2,3 jádra** |

Omezení měření: test běžel nad databází SQLite, ve vašem provozu poběží PostgreSQL. Před nasazením ho proto zopakujeme na vašem serveru, s kopií vašich dat a s vaším počtem strojů, panelů a uživatelů. Doporučený server (fyzický nebo virtuální): aspoň 4 jádra x86-64, každé aspoň tak výkonné jako jádro měřicího notebooku, 8 GB paměti a databáze aspoň se 100 spojeními. Dlouhé seznamy se načítají po stránkách. Známá rezerva: po každém zápisu se náročnější přehledy počítají znovu.

## Osobní údaje (GDPR) v kostce

- **Data jen u vás.** Dodavatel k nim přistupuje jen při podpoře a aktualizacích na dálku (tunelem, který zapne váš správce) – proto se uzavírá zpracovatelská smlouva podle GDPR. Mimo to k datům přístup nemá.
- **Co aplikace eviduje:** účty; zaměstnance (jméno, osobní číslo, pozice, hala, směny, kvalifikace, kdo kdy obsluhoval který stroj a zabalil bednu); záznam změn; zprávy; kalendář; kontakty zákazníků; pokusy o přihlášení (mažou se po dni). Práci po lidech vidí jen vedení a manažer kvality.
- **Co neeviduje:** rodná čísla, adresy bydliště, mzdy ani bankovní spojení.
- **Pozor:** „důvod“ u výjimky ve směně je volný text. Zdravotní údaj (např. „nemoc“) je zvláštní kategorie – v pokynech pište jen „absence“.
- **Výmaz a přenositelnost:** kromě pokusů o přihlášení aplikace sama nic nemaže; účet i zaměstnance v ní vyřadíte, historie zůstane. Úplný výmaz na žádost je zásah technika v databázi. Zaměstnance, kvalifikace a záznam změn stáhnete do tabulky (CSV).

## Známá omezení

- **Bez přímého napojení na podnikový systém (ERP).** Data se vyměňují tabulkami (CSV, Excel, i ze složky): objednávky zákazníků a katalogy (díly, materiály, formy, obaly, zaměstnanci, zákazníci) z tabulky nahrajete s náhledem před zápisem, odjeté dodávky předáte do účetnictví (každou jen jednou) a hlavní seznamy stáhnete do tabulky.
- **Jeden server, bez automatického převzetí provozu.** Při závadě serveru aplikace nejede, dokud se neopraví nebo neobnoví ze zálohy. Dostupnost určuje váš hardware – počítejte s kvalitním serverem a záložním zdrojem napájení.
- **Upozornění jen v aplikaci** (Moje práce, počítadlo v liště), ne e-mailem ani SMS.
- **Obrazovky česky, anglicky a německy** (volí si každý), panely u strojů i ukrajinsky.
- **Boxy a panely v síti strojů komunikují nešifrovaně.** Riziko omezuje vlastní účet každého zařízení: box mluví jen za svůj stroj, panel se prokazuje průkazem svého pracoviště. Síť strojů proto oddělte (samostatná VLAN nebo segment) a porty 8001 a 1883 povolte jen z ní.

**Patrik Palouš**
patrik.palous@tektavo.com

Ukázka v prohlížeči:
demo.tektavo.com